РОССИЙСКАЯ АКАДЕМИЯ НАУК
ИНСТИТУТ СИСТЕМНОГО ПРОГРАММИРОВАНИЯ

Поддержка мобильности в IPv6

RFC 3775 “Mobility Support in IPv6”
Перевод на русский язык

Москва 2004 г.

Список исполнителей

Исполнитель	Контактная информация	Примечания
Шнитман Виктор Зиновьевич, д.т.н.	vzs@ispras.ru	Перевод.

История документа

№ версии	Дата	Примечания
1.0	01.12.2004	Перевод опубликован.

Аннотация.

В данном документе представлен перевод на русский язык RFC 3775 “Mobility support in IPv6”, основополагающей спецификации Mobile IPv6, регламентирущей реализацию поддержки мобильности в сетях, построенных на протоколе IPv6.

Перевод выполнен в рамках проекта по гранту Российского фонда фундаментальных исследований № 04-07-90308 «Верификация функций безопасности и мобильности протоколов IP».

Network Working Group
Request for Comments: 3775
Category: Standards Track

D. Johnson
Rice University
C. Perkins
Nokia Research Center
J. Arkko
Ericsson

June 2004

Mobility Support in IPv6

Поддержка мобильности в IPv6

Статус данного меморандума

Данный документ специфицирует для сообщества Internet протокол, идущий по пути стандартизации Internet, и требует обсуждения и предложений по улучшению. Пожалуйста, обратитесь к текущей редакции документа "Internet Official Protocol Standards" (STD 1) для выяснения состояния стандартизации и статуса этого протокола. Распространение данного меморандума не ограничено.

Замечание относительно авторских прав

Резюме

Данный документ специфицирует протокол, который позволяет узлам оставаться достижимыми при перемещении по Internet. Каждый мобильный узел идентифицируется своим домашним адресом, независимо от своей текущей точки подсоединения к Internet. Когда мобильный узел находится за пределами своего дома, он ассоциируется также с временным адресом, который предоставляет информацию относительно текущего местоположения мобильного узла. Пакеты IPv6, адресованные на домашний адрес мобильного узла, прозрачно маршрутизируются на его временный адрес. Протокол позволяет узлам IPv6 кэшировать привязку домашнего адреса мобильного узла к его временному адресу и затем посылать любые предназначенные мобильному узлу пакеты на его временный адрес. Для поддержки такой работы мобильный IPv6 определяет новый IPv6-протокол и новую опцию места назначения. Все узлы IPv6, мобильные или стационарные, могут осуществлять обмен информацией с мобильными узлами.

Содержание

1. Введение

Данный документ определяет протокол, который дает возможность узлам оставаться достижимыми при перемещениях в IPv6 Internet. Без специальной поддержки мобильности в IPv6 [11] пакеты, отправленные мобильному узлу, не сумеют достичь его, пока мобильный узел находится вне своего домашнего линка. Чтобы несмотря на свои перемещения продолжить обмен информацией, мобильный узел может менять свой IP-адрес каждый раз, когда он перемещается на новый линк, но тогда при изменении местоположения он не сможет сохранить транспортные соединения, а также соединения протоколов более высоких уровней. Поддержка мобильности в IPv6 особенно важна, поскольку мобильные компьютеры, вероятно, составят большую, или, по крайней мере, значительную часть Internet в течение жизни IPv6.

Определенный в данном документе протокол, названный протоколом мобильного IPv6, дает возможность мобильному узлу перемещаться с одного линка на другой без изменения «домашнего адреса» мобильного узла. С помощью этого адреса пакеты могут маршрутизироваться на мобильный узел независимо от текущей точки подсоединения мобильного узла к Internet. После перемещения на новый линк мобильный узел может также продолжать обмен информацией с другими узлами (стационарными или мобильными). Таким образом, перемещение мобильного узла за пределы его домашнего линка является прозрачным для транспортного протокола, протоколов более высоких уровней и приложений.

Протокол мобильного IPv6 одинаково пригоден для обеспечения мобильности, как в гомогенной, так и в гетерогенной среде. Например, протокол мобильного IPv6 упрощает перемещение узла с одного сегмента Ethernet на другой, а также с сегмента Ethernet в ячейку беспроводной ЛВС, при этом, несмотря на такое перемещение, IP-адрес мобильного узла остается неизмененным.

Протокол мобильного IPv6 можно рассматривать как протокол, решающий проблему управления мобильностью на сетевом уровне. Некоторые приложения управления мобильностью (например, передача обслуживания между беспроводными приемопередатчиками, каждый из которых покрывает только очень небольшую географическую область) были решены с помощью техники канального уровня. Например, во многих существующих в настоящее время продуктах беспроводных ЛВС механизмы мобильности канального уровня дают возможность «передачи» мобильного узла из одной ячейки в другую, переустанавливая связность с узлом на канальном уровне в каждом новом местоположении.

Протокол мобильного IPv6 не пытается решить все общие проблемы, связанные с использованием мобильных компьютеров или беспроводных сетей. В частности, данный протокол не пытается решить:

- Управление линками с однонаправленной связностью или с частичной достижимостью, такими, например, как проблема скрытого терминала, в которой хост скрыт только от некоторых маршрутизаторов на линке.
- Управление доступом на линке, который посещает мобильный узел.
- Локальные или иерархические виды управления мобильностью (подобные многим существующим в настоящее время решениям по управлению мобильностью на канальном уровне).
- Поддержку адаптивных приложений.
- Мобильные маршрутизаторы.
- Определение служб.
- Различение между пакетами, потерянными в результате битовых ошибок, и потерянными в результате перегрузки сети.

2. Сравнение с протоколом мобильного IP для IPv4

Разработка поддержки мобильного IP в IPv6 (протокол мобильного IPv6) основывается как на опыте работы, полученным при разработке поддержки мобильного IP в IPv4 (протокол мобильного IPv4) [22, 23, 24], так и на возможностях, предоставляемых протоколом IPv6. Таким образом, протокол мобильного IPv6 имеет много общих свойств с протоколом мобильного IPv4, но интегрирован в IPv6 и предлагает много других улучшений. В данном разделе суммируются главные отличия между мобильным IPv4 и мобильным IPv6:

- Отсутствует необходимость, как в мобильном IPv4, развертывания специальных маршрутизаторов в качестве «внешних агентов». Мобильный IPv6 работает в любом месте без какой-либо специальной поддержки, требующейся от локального маршрутизатора.

- Поддержка оптимизации маршрутов является основной частью протокола, а не нестандартным набором расширений.

- Оптимизация маршрутов мобильного IPv6 может надежно работать даже без заранее организованных контекстов безопасности. Предполагается, что оптимизация маршрутов может быть развернута в глобальном масштабе между всеми мобильными узлами и узлами-корреспондентами.

- В мобильный IPv6 интегрирована также поддержка, предоставляющая возможность разумного сосуществования оптимизации маршрутов с маршрутизаторами, которые осуществляют «входную» фильтрацию [26].

- Механизм определения недостижимости соседей IPv6 гарантирует симметричную достижимость между мобильным узлом и его подразумеваемым маршрутизатором в текущем местоположении.

- В мобильном IPv6 большинство пакетов, посылаемых мобильному узлу, когда он находится вне дома, посылаются с помощью заголовка маршрутизации IPv6, а не с помощью IP-инкапсуляции, сокращая итоговые накладные расходы по сравнению с мобильным IPv4.

- Мобильный IPv6 отделен от какого-либо конкретного канального уровня, поскольку он вместо ARP использует протокол IPv6 Neighbor Discovery [12]. Это улучшает также устойчивость протокола.

- В мобильном IPv6 использование IPv6-инкапсуляции (и заголовка маршрутизации) устраняет необходимость управлять «мягким состоянием туннеля».

- В мобильном IPv6 механизм динамического определения адреса домашнего агента возвращает мобильному узлу одиночный ответ. Управляемый широковещательный подход, используемый в IPv4, возвращает отдельные ответы от каждого домашнего агента.

3. Терминология

В данном документе ключевые слова "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", и "OPTIONAL" интерпретируются так, как описано в BCP 14, RFC 2119 [2].

3.1. Общие термины

IP

Межсетевой протокол версии 6 (IPv6)

node (узел)

Устройство, которое реализует IP.

router (маршрутизатор)

Узел, который пересылает IP-пакеты, неявно адресованные к нему самому.

unicast routable address (индивидуальный маршрутизируемый адрес)

Идентификатор одиночного интерфейса такой, что пакет, посланный на него из другой подсети IPv6, доставляется на интерфейс, идентифицированный этим адресом. Таким образом, индивидуальный маршрутизируемый адрес должен иметь либо глобальную, либо «локальную для сайта» (но не «локальную для линка») область действия.

host (хост)

Любой узел, который не является маршрутизатором.

link (линк)

Средство связи или среда, через которые узлы могут общаться на канальном уровне, такие как Ethernet (простой или с мостами). Канальный уровень – это уровень, расположенный непосредственно ниже уровня IP.

interface (интерфейс)

Присоединение узла к линку.

subnet prefix (префикс подсети)

Битовая строка, состоящая из некоторого числа начальных битов IP-адреса.

interface identifier (идентификатор интерфейса)

Число, которое используется для идентификации интерфейса узла на линке. Идентификатор интерфейса представляет собой оставшиеся младшие биты IP-адреса узла, следующие за префиксом подсети.

link-layer address (адрес канального уровня, канальный адрес)

Идентификатор канального уровня для интерфейса, например, адреса IEEE 802 на линках Ethernet.

packet (пакет)

IP-заголовок плюс полезные данные.

security association (контекст безопасности)

Контекст безопасности IPsec представляет собой совместную связь, сформированную путем совместного использования криптографического ключевого материала и связанного контекста.

security policy database (база данных политики безопасности)

База данных, которая определяет, какие сервисы безопасности должны быть предложены IP-пакетам, и в какой форме.

destination option (опция места назначения)

Опции места назначения передаются с помощью заголовка расширения IPv6 Destination Options. Опции места назначения содержат дополнительную информацию, которая нуждается в проверке только IPv6-узлом, заданным адресом места назначения в IPv6-заголовке, но не маршрутизаторами в промежутках. Протокол мобильного IPv6 определяет одну новую опцию места назначения - Home Address (См. разд. 6.3).

routing header (заголовок маршрутизации)

Заголовок маршрутизации может быть представлен как расширение заголовка IPv6 и указывает на то, что полезные данные должны быть доставлены на IPv6-адрес места назначения некоторым способом, который отличается от того, что будет осуществляться стандартной маршрутизацией Internet. В данном документе использование термина «заголовок маршрутизации» обычно указывает на использование заголовка маршрутизации типа 2, как определено в разд. 6.4.

"|" (concatenation) конкатенация

Некоторые формулы в данной спецификации используют символ "|" для указания побайтовой конкатенации, как в A | B. Такая конкатенация требует, чтобы в результате все октеты элемента данных A появились первыми, а за ними следовали все октеты элемента данных B.

First (size, input)

Некоторые формулы в данной спецификации используют функциональную форму "First (size, input)" для указания усечения «input» (входных) данных таким образом, что остаются для использования только первые "size" (количество) бит.

3.2. Термины протокола мобильного IPv6

home address (домашний адрес)

Индивидуальный маршрутизируемый адрес, присвоенный мобильному узлу, используемый в качестве постоянного адреса мобильного узла. Этот адрес находится внутри домашнего линка мобильного узла. Стандартные механизмы IP-маршрутизации будут доставлять пакеты, отправляемые на домашний адрес мобильного узла, на его домашний линк. Мобильные узлы могут иметь несколько домашних адресов, например, когда на домашнем линке имеется несколько домашних префиксов.

home subnet prefix (префикс домашней подсети)

Префикс IP-подсети, соответствующий домашнему адресу мобильного узла.

home link (домашний линк)

Линк, на котором определяется префикс домашней подсети мобильного узла.

mobile node (мобильный узел)

Узел, который может изменить точку подсоединения с одного линка на другой, несмотря на то, что все еще остается достижимым с помощью своего домашнего адреса.

movement (перемещение)

Изменение точки соединения мобильного узла с Internet так, что он оказывается более не подсоединенным к тому же самому линку, как это было ранее. Если мобильный узел в текущий момент времени не подсоединен к своему домашнему линку, то говорят, что мобильный узел «находится вне дома».

L2 handover (передача обслуживания уровня 2)

Процесс, с помощью которого мобильный узел меняет одно соединение канального уровня на другое. Например, изменение беспроводной точки доступа представляет собой передачу обслуживания L2.

L3 handover (передача обслуживания уровня 3)

В результате передачи обслуживания L2 мобильный узел определяет изменение «линкового» префикса подсети, которое потребует изменения основного временного адреса. Например, изменение маршрутизатора доступа, являющееся результатом изменения беспроводной точки доступа, обычно приводит к передаче обслуживания L3.

correspondent node (узел-корреспондент)

Узел-партнер, с которым мобильный узел осуществляет обмен информацией. Узел-корреспондент может быть как мобильным, так и стационарным.

foreign subnet prefix (префикс внешней подсети)

Префикс IP-подсети, отличающийся от префикса домашней подсети мобильного узла.

foreign link (внешний линк)

Любой линк, отличный от домашнего линка мобильного узла.

care-of address (временный адрес)

Индивидуальный маршрутизируемый адрес, связанный с мобильным узлом на время посещения им внешнего линка; префикс подсети этого временного IP-адреса является префиксом внешней подсети. Среди нескольких временных адресов, которые мобильный узел может иметь в любой данный момент времени (например, с разными префиксами подсети), один временный адрес, зарегистрированный в домашнем агенте мобильного узла для данного домашнего адреса, называется его «основным» временным адресом.

home agent (домашний агент)

Маршрутизатор, находящийся на домашнем линке мобильного узла, в котором мобильный узел зарегистрировал свой текущий временный адрес. Пока мобильный узел находится вне дома, домашний агент перехватывает на домашнем линке пакеты, отправляемые на домашний адрес мобильного узла, инкапсулирует и туннелирует их на зарегистрированный временный адрес мобильного узла.

binding (привязка)

Ассоциация домашнего адреса мобильного узла с временным адресом этого мобильного узла вместе с оставшимся временем жизни этой ассоциации.

registration (регистрация)

Процесс, в течение которого мобильный узел посылает своему домашнему агенту или узлу-корреспонденту обновление привязки, которое является основанием для того, чтобы привязка мобильного узла была зарегистрирована.

mobility message (сообщение мобильности)

Сообщение, содержащее заголовок мобильности (см. разд. 6.1).

binding authorization (авторизация привязки)

Регистрация в узле-корреспонденте нуждается в авторизации, чтобы предоставить возможность получателю поверить в то, что отправитель имеет право определять новую привязку.

return routability procedure (процедура обратной маршрутизируемости)

Процедура обратной маршрутизируемости авторизует регистрацию с помощью обмена криптографическими маркерами.

correspondent registration (регистрация в узле-корреспонденте)

Процедура обратной маршрутизируемости, за которой следует регистрация, выполняется между мобильным узлом и узлом-корреспондентом.

home registration (регистрация в домашнем агенте)

Регистрация между мобильным узлом и его домашним агентом, авторизованная с помощью IPsec.

nonce (одноразовый номер)

Одноразовые номера представляют собой случайные числа, используемые внутри узла-корреспондента при создании маркеров keygen, связанных с процедурой обратной маршрутизируемости. Одноразовые номера не являются специфическими (индивидуальными) для некоторого мобильного узла и хранятся в секрете в узле-корреспонденте.

nonce index (индекс одноразового номера)

Индекс одноразового номера используется для указания того, какие одноразовые номера использовались при создании значений маркеров keygen, без раскрытия самих одноразовых номеров.

cookie (идентифицирующая цепочка)

Идентифицирующая цепочка представляет собой случайное число, используемое мобильным узлом для предотвращения спуфинга подложным узлом-корреспондентом в процедуре обратной маршрутизируемости.

care-of init cookie (идентифицирующая цепочка care-of init cookie)

Идентифицирующая цепочка, посылаемая узлу-корреспонденту в сообщении Care-of Test Init, которая должна быть возвращена в сообщении Care-of Test.

home init cookie (идентифицирующая цепочка home init cookie)

Идентифицирующая цепочка, посылаемая узлу-корреспонденту в сообщении Home Test Init, которая должна быть возвращена в сообщении Home Test.

keygen token (маркер keygen token)

Маркер keygen token представляет собой число, поставляемое узлом-корреспондентом в процедуре обратной маршрутизируемости для того, чтобы уполномочить мобильный узел вычислить необходимый ключ управления привязкой для авторизации обновления привязки.

care-of keygen token (маркер care-of keygen token)

Маркер keygen token, посылаемый узлом корреспондентом в сообщении Care-of Test.

home keygen token (маркер home keygen token)

Маркер keygen token, посылаемый узлом корреспондентом в сообщении Home Test.

binding management key (Kbm) (ключ управления привязкой).

Ключ управления привязкой (Kbm) представляет собой ключ, который используется для авторизации сообщения управления кэшем привязок (например, обновления привязки или подтверждения привязки). Процедура обратной маршрутизируемости предоставляет способ создания ключа управления привязкой.

4. Обзор протокола мобильного IPv6

4.1. Принципы работы

Предполагается, что мобильный узел всегда адресуем своим домашним адресом независимо от того, подключен ли он в текущий момент времени к своему домашнему линку, или находится вне дома. «Домашний адрес» - это IP-адрес, присвоенный мобильному узлу на его домашнем линке с точностью до префикса домашней подсети. Когда мобильный узел находится дома, пакеты, адресованные на его домашний адрес, маршрутизируются на домашний линк этого мобильного узла, используя традиционные механизмы маршрутизации Internet.

Когда мобильный узел подключен к какому-то внешнему линку вне дома, он адресуем также с помощью одного или нескольких временных адресов. Временный адрес – это IP-адрес, ассоциированный с мобильным узлом и имеющий префикс подсети конкретного внешнего линка. Мобильный узел может получить свой временный адрес с помощью традиционных механизмов IPv6, таких как бесконтекстная или контекстная автоконфигурация. До тех пор, пока мобильный узел остается в этом месте, пакеты, адресованные на этот временный адрес, будут маршрутизироваться к мобильному узлу. Мобильный узел может также принимать пакеты с нескольких временных адресов, например, когда он перемещается, но все еще достижим на предыдущем линке.

Ассоциация между домашним адресом и внешним адресом мобильного узла известна под названием «привязки» (binding) для мобильного узла. Находясь вне дома, мобильный узел регистрирует свой основной временный адрес в маршрутизаторе в своей домашней сети и просит этот маршрутизатор выполнять для мобильного узла функции «домашнего агента». Мобильный узел выполняет эту регистрацию привязки путем посылки домашнему агенту сообщения «Binding Update» (обновление привязки). Домашний агент отвечает мобильному узлу, возвращая сообщение «Binding Acknowledgement» (подтверждение привязки). Работа мобильного узла специфицируется в разд. 11, а работа домашнего агента – в разд.10.

Любой узел, осуществляющий обмен информацией с мобильным узлом, упоминается в данном документе как «узел-корреспондент» (correspondent node) мобильного узла, и может представлять собой либо стационарный, либо мобильный узел. Мобильные узлы могут предоставлять узлам-корреспондентам информацию о своем текущем местоположении. Это происходит посредством регистрации в узле-корреспонденте. Для того чтобы авторизовать установление привязки, как часть этой процедуры, выполняется проверка обратной маршрутизируемости (return routability test). Работа узла-корреспондента специфицируется в разд. 9.

Имеются два возможных режима обмена информацией между мобильным узлом и узлом-корреспондентом. Первый режим, двунаправленное туннелирование, не требует от узла-корреспондента поддержки протокола Mobile IPv6 и этот режим доступен даже в том случае, если мобильный узел не зарегистрировал своей текущей привязки в узле-корреспонденте. Пакеты от узла-корреспондента маршрутизируются домашнему агенту и затем туннелируются мобильному узлу. Пакеты от мобильного узла к узлу-корреспонденту сначала туннелируются («туннелируются в обратном направлении») домашнему агенту и затем обычным образом маршрутизируются из домашней сети узлу-корреспонденту. В этом режиме домашний агент для перехвата любых IPv6-пакетов, адресованных на домашний адрес (или домашние адреса) мобильного узла на домашнем линке, использует механизм proxy Neighbor Discovery. Каждый перехваченный пакет туннелируется на основной временный адрес мобильного узла. Это туннелирование осуществляется с помощью IPv6-инкапсуляции [15].

Второй режим, режим «оптимизации маршрута», требует, чтобы мобильный узел зарегистрировал свою текущую привязку в узле-корреспонденте. Пакеты от узла-корреспондента могут маршрутизироваться прямо на временный адрес мобильного узла. При посылке пакета на любое место назначения IPv6, узел-корреспондент проверяет свои кэшированные привязки на предмет наличия элемента с адресом места

назначения пакета. Если кэшированная привязка для этого адреса места назначения найдена, то узел использует новый тип заголовка маршрутизации IPv6 [11] (см. разд. 6.4) для маршрутизации пакета мобильному узлу по пути временного адреса, указанного в этой привязке.

Маршрутизация пакетов непосредственно на временный адрес мобильного узла позволяет использовать самый короткий путь обмена информацией. Она устраняет также перегрузку домашнего агента мобильного узла и домашнего линка. Кроме того, уменьшается влияние любой возможной ошибки домашнего агента или сетей, находящихся на пути к нему и от него.

При маршрутизации пакетов непосредственно мобильному узлу узел-корреспондент устанавливает поле Destination Address в заголовке IPv6 равным временному адресу мобильного узла. Для передачи требуемого домашнего адреса к пакету добавляется также новый тип заголовка маршрутизации IPv6 (см. разд. 6.4). Подобным образом, мобильный узел устанавливает поле Source Address в IPv6-заголовке пакета равным его текущему временному адресу. Для передачи своего домашнего адреса мобильный узел добавляет новую опцию места назначения IPv6 «Home Address» (см. разд. 6.3). Включение домашних адресов в эти пакеты делает использование временного адреса прозрачным выше сетевого уровня (например, на транспортном уровне).

Протокол Mobile IPv6 обеспечивает также поддержку нескольких домашних агентов, и, кроме того, ограниченную поддержку реконфигурации домашней сети. В этих случаях мобильный узел может не знать IP-адреса своего собственного домашнего агента, и префиксы домашней подсети могут даже меняться со временем. Механизм, известный под названием «dynamic home agent address discovery» (динамическое определение адреса домашнего агента) позволяет домашнему агенту динамически определить IP-адрес домашнего агента на его домашнем линке, даже когда мобильный узел находится вне дома. Мобильные узлы могут также узнать новую информацию относительно префиксов домашней подсети с помощью механизма «mobile prefix discovery» (определения мобильного префикса). Эти механизмы описываются начиная с разд. 6.5).

4.2. Новый IPv6-протокол

Протокол Mobile IPv6 определяет новый IPv6-протокол, используя Mobility Header (заголовок мобильности) (см. разд. 6.1). Этот заголовок используется для передачи следующих сообщений:

Home Test Init ( ) – (инициация проверки домашнего адреса)

Home Test ( ) – (проверка домашнего адреса)

Care-of Test Init ( ) – (инициация проверки временного адреса)

Care-of Test ( ) – (проверка временного адреса)

Эти четыре сообщения используются для выполнения процедуры обратной маршрутизируемости от мобильного узла к узлу-корреспонденту. Как описано в разд. 5.2.5, это гарантирует авторизацию последующих обновлений привязки.

Binding Update (обновление привязки)

Сообщение Binding Update используется мобильным узлом для уведомления узла-корреспондента или домашнего агента мобильного узла о его текущей привязке. Обновление привязки, посылаемое домашнему агенту мобильного узла помечается признаком «home registration» (регистрация в домашнем агенте).

Binding Acknowledgement (подтверждение привязки)

Сообщение Binding Acknowledgement используется для подтверждения получения обновления привязки, если подтверждение было запрошено в обновлении привязки, обновление привязки было послано домашнему агенту, или произошла ошибка.

Binding Refresh Request (запрос обновления привязки)

Сообщение Binding Refresh Request используется узлом-корреспондентом, чтобы потребовать от мобильного узла переустановить свою привязку с узлом-корреспондентом. Это сообщение обычно используется когда кэшированная привязка активно используется, но ее время жизни близко к исчерпанию. В качестве индикации активного использования узел-корреспондент может использовать, например, недавний трафик и открытые соединения транспортного уровня.

Binding Error (ошибка привязки)

Сообщение Binding Error используется узлом-корреспондентом для сигнализации ошибки, связанной с мобильностью, такой, например, как неуместная попытка использования опции места назначения Home Address без существующей привязки.

4.3. Новая опция места назначения IPv6

Протокол Mobile IPv6 определяет новую опцию места назначения IPv6 - Home Address destination option. Эта опция подробно описывается в разд. 6.3.

4.4. Новые сообщения ICMP IPv6

Протокол Mobile IPv6 вводит также четыре новых типа сообщений ICMP, два для использования в механизме динамического определения адреса домашнего агента, и два для механизмов перенумерации и мобильного конфигурирования. Как описывается в разд. 10.5 и 11.4.1, для определения адреса домашнего агента используются следующие два новых сообщения ICMP:

- Home Agent Address Discovery Request (запрос определения адреса домашнего агента), описанное в разд. 6.5.

- Home Agent Address Discovery Reply (ответ определения адреса домашнего агента), описанное в разд. 6.6.

Как описано в разд. 10.6, следующие два типа сообщений используются для перенумерации сетей и конфигурирования адресов на мобильном узле:

- Mobile Prefix Solicitation (запрос мобильного префикса), описанное в разд. 6.7.

- Mobile Prefix Advertisement (объявление мобильного префикса), описанное в разд. 6.8.

4.5. Терминология концептуальных структур данных

Данный документ описывает протокол Mobile IPv6 в терминах следующих концептуальных структур данных:

Binding Cache (кэш привязок)

Кэш привязок для других узлов. Этот кэш поддерживается домашними агентами и узлами-корреспондентами. Кэш содержит как элементы «регистрации в узле-корреспонденте» (см. разд. 9.1), так и элементы «регистрации в домашнем агенте» (см. разд. 10.1).

Binding Update List (список обновления привязок)

Этот список поддерживается каждым мобильным узлом. Список имеет отдельный элемент для каждой привязки, которую мобильный узел имеет или пытается установить с конкретным другим узлом. В этот список включаются как регистрации в узле-корреспонденте, так и регистрации в домашнем агенте. Элементы из этого списка удаляются при истечении времени жизни привязки. См. разд. 11.1.

Home Agents List (список домашних агентов)

Домашние агенты должны знать какие другие домашние агенты находятся на том же самом линке. Эта информация хранится в списке домашних агентов, как описано более подробно в разд. 10.1. Этот список используется для информирования мобильных узлов в процессе динамического определения адреса домашнего агента.

4.6. Возможность использования «локальных для сайта» адресов

Данная спецификация требует, чтобы домашний и временный адреса были индивидуальными (unicast) маршрутизируемыми адресами. «Локальные для сайта» адреса могут использоваться в сетях, которые не подсоединены к Internet, но данная спецификация не определяет, когда такое использование надежно, а когда нет. Мобильные узлы могут не знать, на каком сайте они находятся в данный момент времени, трудно предотвратить случайное подключение к другим сайтам, и неоднозначность «локальных для сайта» адресов может привести к проблемам, если домашняя и посещаемая сети используют одни и те же адреса. Поэтому «локальные для сайта» адреса не должны (SHOULD NOT) использоваться в качестве домашних и временных адресов.

5. Обзор средств безопасности Mobile IPv6

Данная спецификация предоставляет целый ряд функций безопасности. Они включают защиту передачи сообщений Binding Update (обновлений привязки) как домашним агентам, так и узлам-корреспондентам, защиту определения мобильного префикса и защиту механизмов, которые MIPv6 использует для транспортировки пакетов данных.

Сообщения Binding Update защищаются с помощью заголовков расширения IPsec, или с помощью опции Binding Authorization Data (данные для авторизации привязки). Эта опция применяет ключ управления привязкой Kbm (binding management key), который может быть определен с помощью процедуры обратной маршрутизруемости. Определение мобильного префикса защищается с помощью заголовков расширения IPsec. Механизмы, связанные с транспортировкой пакетов полезных данных, - например, опция места назначения Home Address и заголовок маршрутизации типа 2 – были специфицированы в такой манере, которая ограничивает их использование при реализации атак.

5.1. Обновления привязки, посылаемые домашним агентам

Для защиты целостности и аутентичности сообщений Binding Update и Binding Acknowledgement мобильный узел и домашний агент должны (MUST)использовать контекст безопасности (security association) IPsec. Для обеспечения аутентификации источника данных, целостности в режиме без установления соединения и дополнительной защиты от воспроизведения, как мобильные узлы, так и домашние агенты должны (MUST) поддерживать и должны (SHOULD) использовать заголовок ESP (Encapsulating Security Payload) [6] и должны (MUST) использовать ненулевой алгоритм аутентификации полезных данных. Заметим, что заголовок аутентификации AH (Authentication Header) [5] также возможен, но для краткости в данной спецификации не обсуждается.

Чтобы с помощью IPsec защитить сообщения, которыми обмениваются мобильный узел и домашний агент, должны быть созданы соответствующие элементы базы данных политики безопасности. Мобильный узел не должен допускать применение своего контекста безопасности для посылки сообщения Binding Update от лица другого мобильного узла, используя того же самого домашнего агента. Это должно (MUST) достигаться путем проверки домашним агентом того факта, что данный домашний адрес использовался с правильным контекстом безопасности. Такая проверка предусматривается обработкой IPsec в предположении, что элементы базы данных политики безопасности недвусмысленно определяют единственный контекст безопасности для защиты сообщений Binding Update между любым данным домашним адресом и домашним агентом. Чтобы это оказалось возможным, необходимо, чтобы домашний адрес мобильного узла был виден в сообщениях Binding Update и Binding Acknowledgement. В этих пакетах домашний адрес используется в качестве источника или места назначения, или в опции места назначения Home Address, или в заголовке маршрутизации типа 2.

Как и со всеми контекстами безопасности IPsec в данной спецификации, ручное конфигурирование контекстов безопасности должно (MUST) поддерживаться. Используемые общие секреты для разных мобильных узлов должны (MUST) быть случайными и уникальными и должны (MUST) раздаваться мобильным узлам автономно.

Автоматическое управление ключами IKE [9] может (MAY) поддерживаться. Когда используется IKE, либо элементы базы данных политики безопасности, либо обработка MIPv6 должны (MUST) недвусмысленно определять мандаты IKE фазы 1, которые могут использоваться для авторизации создания контекста безопасности для защиты сообщений Binding Update для конкретного домашнего адреса. Как реально такие отображения поддерживаются, находится вне рамок данной спецификации, но они могут поддерживаться, например, в виде локально администрируемой таблицы в домашнем агенте. Если идентификатор личности в фазе 1 определяется по полностью квалифицированному доменному имени FQDN (Fully Qualified Domain Name), то могут использоваться также безопасные разновидности DNS.

В разд. 11.3.2 обсуждается, насколько тщательная проверка адресов, используемых для транспортировки IKE, необходима для соединений IKE с домашним агентом. Такая тщательная проверка необходима для обеспечения того, чтобы сообщение Binding Update не потребовалось до обмена IKE, который необходим для защиты этого сообщения Binding Update.

Когда между мобильным узлом и домашним агентом используется IKE версии 1 с аутентификацией на основе предварительно распределенного секрета, должен (MUST) использоваться агрессивный режим.

В фазе 1 IKEv1 в качестве полезных данных идентификации личности (Identity Payload) не должен (MUST NOT) использоваться ID_IPV6_ADDR.

Ссылка [21] содержит более подробное описание и примеры использования IPsec для защиты обменов информацией между мобильным узлом и домашним агентом.

5.2. Обновления привязки, посылаемые узлу-корреспонденту

Защита сообщений Binding Update, посылаемых узлу-корреспонденту, не требует конфигурирования контекстов безопасности или существования инфраструктуры аутентификации между мобильными узлами и узлами-корреспондентами. Вместо этого, чтобы гарантировать, что сообщение посылает правильный мобильный узел, используется метод, называемый процедурой обратной маршрутизируемости (return routability procedure). Этот метод не защищает от злоумышленников, которые находятся на пути между домашней сетью и узлом-корреспондентом. Однако злоумышленники, находящиеся в таком месте способны осуществить те же самые атаки даже без Mobile IPv6. Основное преимущество процедуры обратной маршрутизируемости заключается в том, что она ограничивает круг потенциальных злоумышленников теми, кто имеет доступ к одному конкретному пути в Internet, и избегает подложных сообщений Binding Update из любого другого места в Internet. Более глубокое объяснение особенностей процедуры обратной маршрутизируемости см. в разд. 15.

Целостность и аутентичность сообщений Binding Update, посылаемых узлу-корреспонденту защищаются с помощью алгоритма ключевого хэша. С этой целью для задания ключа для алгоритма хэширования используется ключ управления привязкой Kbm (binding management key). Ключ Kbm порождается с помощью данных, обмен которыми производится во время процедуры обратной маршрутизируемости. Обмен данными выполняется с помощью ключей узла, одноразовых номеров, идентифицирующих цепочек, маркеров и известных криптографических функций. В разд. 5.2.5. описаны основные принципы процедуры обратной маршрутизируемости. В разд. 5.2.6 показано, как результаты этой процедуры используются для авторизации сообщения Binding Update, посылаемого узлу-корреспонденту.

5.2.1. Ключи узла

Каждый узел-корреспондент имеет секретный ключ Kcn, который называется «ключом узла» (node key) и используется для выработки маркеров keygen token, посылаемых мобильным узлам. Ключ узла должен (MUST) быть случайным числом длиною 20 октетов. Ключ узла позволяет узлу-корреспонденту проверить, что маркеры keygen token, используемые мобильным узлом для авторизации сообщения Binding Update, действительно являются его собственными. Этот ключ не должен (MUST NOT) разделяться ни с каким другим объектом.

Узел-корреспондент в любой момент времени может (MAY) сгенерировать новый ключ узла; это позволяет избежать необходимости организации защищенной постоянной памяти ключей. Процедуры для необязательного обновления ключа узла обсуждаются позже в разд. 5.2.7.

5.2.2. Одноразовые номера

Каждый узел-корреспондент должен также через регулярные интервалы времени генерировать одноразовые номера (nonces). Одноразовые номера должны генерироваться с помощью генератора случайных чисел, о котором известно, что он обладает хорошими свойствами случайности [1]. Узел-корреспондент может использовать тот же самый Kcn и одноразовый номер для всех мобильных узлов, с которыми он осуществляет обмен данными.

Каждый одноразовый номер (nonce) идентифицируется индексом одноразового номера (nonce index). Когда генерируется новый одноразовый номер, он должен быть связан с новым индексом одноразового номера; это можно сделать, например, путем инкрементирования предыдущего индекса одноразового номера, если индекс одноразового номера используется как указатель в линейном массиве одноразовых номеров. Однако отсутствуют требования, в соответствии с которыми одноразовые номера должны храниться этим способом, или чтобы значения последовательных индексов одноразовых номеров имели какую-либо конкретную связь друг с другом. Значение индекса предается в протоколе так, что если во время выполнения протокола одноразовый номер заменяется новым, узел-корреспондент может различить сообщения, которые должны быть проверены на соответствие новому одноразовому номеру. Строго говоря, индексы при аутентификации не обязательны, но позволяют узлу-корреспонденту эффективно находить значение одноразового номера, который он использует при создании маркера keygen token.

Узлы-корреспонденты хранят как текущий одноразовый номер, так и небольшой набор предыдущих годных одноразовых номеров, время жизни которых еще не истекло. Значения, устаревшие за истечением срока годности, должны (MUST) отбрасываться, а сообщения, использующие просроченные или неизвестные индексы, будут отвергаться.

Конкретные значения индексов одноразовых номеров не могут использоваться мобильными узлами для определения годности одноразового номера. Ожидаемые значения времени годности одноразовых номеров, и процедуры для их обновления обсуждаются позже в разд. 5.3.7.

Одноразовый номер представляет собой строку октетов произвольной длины. Рекомендованная длина одноразового номера составляет 64 бита.

5.2.3. Идентифицирующие цепочки и маркеры

Процедура проверки обратной маршрутизируемости адреса использует идентифицирующие цепочки (cookies) и маркеры keygen token в качестве трудных для понимания значений в сообщениях test init и test, соответственно.

- Идентифицирующие цепочки "home init cookie" и "care-of init cookie" представляют собой 64-битовые значения, посылаемые мобильным узлом узлу-корреспонденту, и возвращаемые позже мобильному узлу. Идентифицирующая цепочка home init cookie посылается в сообщении Home Test Init и возвращается в сообщении Home Test. Идентифицирующая цепочка care-of init cookie посылается в сообщении Care-of Test Init и возвращается в сообщении Care-of Test.

- Маркер "home keygen token" и маркер "care-of keygen token" представляют собой 64-битовые значения, посылаемые узлом-корреспондентом мобильному узлу через домашнего агента (в сообщении Home Test) и на временный адрес (в сообщении Care-of Test), соответственно.

В каждом посылаемом сообщении Home Test Init или Care-of Test Init мобильный узел должен устанавливать идентифицирующие цепочки home init cookie или care-of init cookie в значение вновь сгенерированного случайного числа. Идентифицирующие цепочки используются для проверки того, что сообщения Home Test или Care-of Test соответствуют сообщениям Home Test Init или Care-of Test Init, соответственно.

Маркеры home keygen token и care-of keygen token вырабатываются узлом-корреспондентом на основе его текущего активного секретного ключа (Kcn) и одноразовых номеров, а также домашнего или временного адресов, соответственно. Маркер keygen token является годным до тех пор, пока остаются годными секретный ключ (Kcn) и одноразовый номер, использованные для его создания.

5.2.4. Криптографические функции

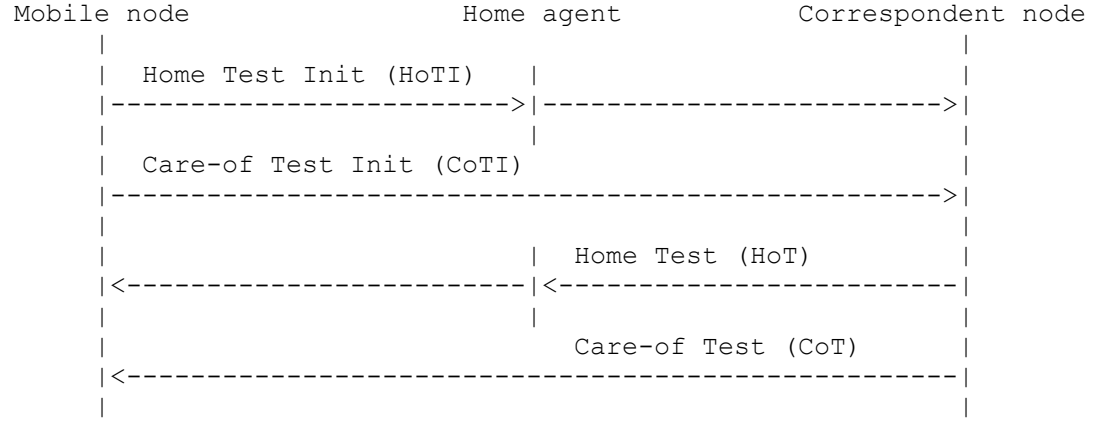
В данной спецификации для вычисления значений хэша используется функция SHA1 [20]. Коды аутентификации сообщений MAC (Message Authentication Code) вычисляются с помощью HMAC_SHA1 [25, 20]. HMAC_SHA1(K,m) обозначает такой MAC, который вычисляется над сообщением m с ключом K.

5.2.5. Процедура обратной маршрутизируемости

Процедура обратной маршрутизируемости позволяет узлу-корреспонденту получить некоторую разумную гарантию того, что мобильный узел в действительности адресуем по его заявленному временному адресу, а также по его домашнему адресу. Только при такой гарантии узел-корреспондент может считать приемлемыми сообщения Binding Update от мобильного узла, которые затем будут информировать узел-корреспондент о необходимости направлять трафик для данного мобильного узла на заявленный им временный адрес.

Это выполняется путем проверки того, что пакеты, адресованные на эти два объявленных адреса, маршрутизируются на мобильный узел. Мобильный узел может пройти эту проверку, только если он может представить доказательство того, что он получает определенные данные (маркеры keygen token), которые узел-корреспондент посылает по этим адресам. Эти данные объединяются мобильным узлом в ключ управления привязкой, обозначенный как Kbm.

На нижеприведенном рисунке показан поток сообщений для процедуры обратной маршрутизируемости.



Сообщения Home Test Init и Care-of Test Init посылаются одновременно. Процедура требует очень малой обработки в узле-корреспонденте, и сообщения Home Test и Care-of Test могут вернуться очень быстро, возможно почти одновременно. Эти четыре сообщения составляют процедуру обратной маршрутизируемости.

Сообщение Home Test Init

Мобильный узел посылает сообщения Home Test Init узлу-корреспонденту (через домашнего агента), чтобы получить маркер home keygen token. Содержимое сообщения можно обобщить следующим образом:

* Source Address = home address

* Destination Address = correspondent

* Parameters:

  + home init cookie

Сообщение Home Test Init передает узлу-корреспонденту домашний адрес мобильного узла. Мобильный узел посылает также вместе с ним идентифицирующую цепочку home init cookie, которую узел-корреспондент должен вернуть позже. Сообщение Home Test Init передается через домашнего агента посредством обратного туннелирования. (Заголовки и адреса, связанные с обратным туннелированием, в представленном выше обсуждении содержимого сообщения опущены). Мобильный узел запоминает эти значения идентифицирующей цепочки, чтобы получить некоторую гарантию того, что его протокольные сообщения обрабатывались требуемым узлом-корреспондентом.

Сообщение Care-of Test Init

Мобильный узел посылает сообщение Care-of Test Init узлу корреспонденту (прямо, а не через домашнего агента), чтобы получить маркер care-of keygen token. Содержимое этого сообщения можно обобщить следующим образом:

* Source Address = care-of address

* Destination Address = correspondent

* Parameters:
  + care-of init cookie

Сообщение Care-of Test Init передает узлу-корреспонденту временный адрес мобильного узла. Мобильный узел посылает также вместе с ним идентифицирующую цепочку care-of init cookie, которую узел-корреспондент должен позже вернуть. Сообщение Care-of Test Init посылается прямо узлу-корреспонденту.

Сообщение Home Test

Сообщение Home Test посылается в ответ на сообщение Home Test Init. Оно посылается через домашнего агента. Содержимое сообщения следующее:

* Source Address = correspondent

* Destination Address = home address

* Parameters:

  + home init cookie

  + home keygen token

  + home nonce index

Когда узел-корреспондент получает сообщение Home Test Init, он генерирует маркер home keygen token следующим образом:

```
home keygen token :=
   First (64, HMAC_SHA1 (Kcn, (home address | nonce | 0)))
```

где символ | обозначает конкатенацию. Последний "0" в функции HMAC_SHA1 представляет собой один нулевое октет, который используется для различения друг от друга идентифицирующих цепочек home cookie и care-of cookie.

Маркер home keygen token формируется из первых 64 бит кода MAC. Маркер home keygen token проверяет, что мобильный узел может получать сообщения, посылаемые по его домашнему адресу. При выработке маркера home keygen token используется ключ Kcn, чтобы позволить узлу-корреспонденту проверить, что он породил одноразовые номера home nonce и care-of nonce, не заставляя узел-корреспондент запоминать список всех маркеров, которые он выдал.

Сообщение Home Test посылается мобильному узлу через домашнюю сеть, из которой, как предполагается, домашний агент протуннелирует его мобильному узлу. Это означает, что мобильный узел должен был уже послать сообщение Binding Update домашнему агенту, так чтобы домашний агент мог получить и авторизовать новый временный адрес для мобильного узла до выполнения процедуры обратной маршрутизируемости. Для увеличения степени безопасности данные, передаваемые между домашним агентом и мобильным узлом, защищаются от просмотра и пассивных атак. Такая защита получается благодаря шифрованию маркера home keygen token, поскольку он туннелируется от домашнего агента к мобильному узлу как описано в разд. 10.4.6. Особенности системы безопасности с этой дополнительной защитой обсуждаются в разд. 15.4.1.

Идентифицирующая цепочка home init cookie от мобильного узла возвращается в сообщении Home Test, чтобы гарантировать, что сообщение пришло от узла, находящегося на пути между домашним агентом и узлом-корреспондентом.

Индекс одноразового номера home nonce index доставляется мобильному узлу, чтобы позже позволить узлу-корреспонденту эффективно найти значение одноразового номера, который использовался для создания маркера home keygen token.

Сообщение Care-of Test

Это сообщение посылается в ответ на сообщение Care-of Test Init. Данное сообщение не посылается через домашнего агента, оно посылается прямо мобильному узлу. Содержимое сообщения следующее:

* Source Address = correspondent

* Destination Address = care-of address

* Parameters:

  + care-of init cookie

  + care-of keygen token

  + care-of nonce index

Когда узел-корреспондент получает сообщение Care-of Test Init, он генерирует маркер care-of keygen token следующим образом:

```
care-of keygen token :=
   First (64, HMAC_SHA1 (Kcn, (care-of address | nonce | 1)))
```

Здесь последняя "1" в функции HMAC_SHA1 представляет собой один октет, содержащий шестнадцатеричное значение 0x01, и используется для различения друг от друга идентифицирующих цепочек home cookie и care-of cookie. Маркер keygen token формируется из первых 64 бит кода MAC и посылается прямо мобильному узлу по его временному адресу. Идентифицирующая цепочка care-of init cookie из сообщения Care-of Test Init возвращается, чтобы гарантировать, что сообщение приходит от узла, находящегося на пути к узлу-корреспонденту.

Индекс одноразового номера care-of nonce index служит для указания одноразового номера, использовавшегося для формирования маркера care-of key-

gen token. Индексы одноразовых номеров home nonce index и care-of nonce index в сообщениях Home Test и Care-of Test могут (MAY) быть одними и теми же, или различными.

Процедура обратной маршрутизируемости заканчивается, когда мобильный узел получит оба сообщения Home Test и Care-of Test. В результате процедуры мобильный узел имеет данные, которые ему необходимы для посылки обновления привязки узлу-корреспонденту. Мобильный узел хэширует маркеры вместе для формирования 20-октетного ключа привязки Kbm:

Kbm = SHA1 (home keygen token | care-of keygen token)

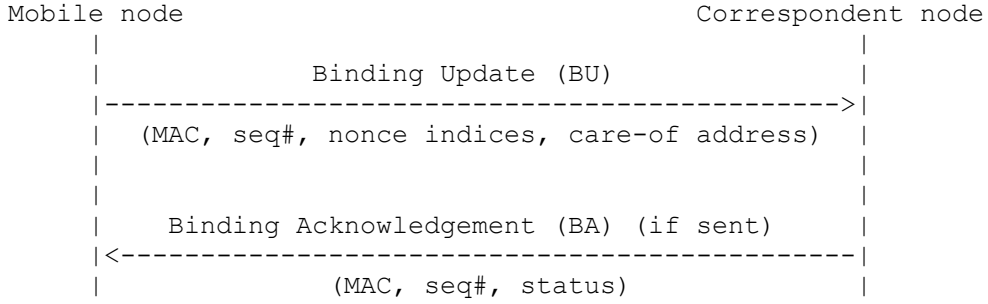
Сообщение Binding Update может также использоваться для удаления ранее установленной привязки (разд. 6.1.7). В этом случае маркер care-of keygen token не используется. Вместо этого, ключ управления привязкой генерируется следующим образом:

Kbm = SHA1(home keygen token)

Заметим, что узел-корреспондент не создает для мобильного узла никакого конкретного состояния до тех пор, пока он не получит от этого мобильного узла сообщение Binding Update. Узел-корреспондент не сохраняет значение ключа управления привязкой Kbm; он порождает Kbm когда поступают индексы одноразовых номеров и адреса мобильного узла.

5.2.6. Авторизация сообщений управления привязкой

После создания мобильным узлом ключа управления привязкой Kbm, он может поставить узлу-корреспонденту поддающееся проверке сообщение Binding Update. В этом разделе дается обзор такой регистрации. На приведенном ниже рисунке показан поток сообщений.



Сообщение Binding Update (обновление привязки)

Как описано в предыдущем разделе, для авторизации сообщения Binding Update мобильный узел создает ключ управления привязкой Kbm из маркеров keygen token. Содержимое сообщения Binding Update включает следующее:

* Source Address = care-of address

* Destination Address = correspondent

* Parameters:

  + home address (в опции места назначения Home Address, если он отличается от Source Address)

  + sequence number (в заголовке сообщения Binding Update)

  + home nonce index (в опции Nonce Indices)

+ care-of nonce index (в опции Nonce Indices)

+ First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BU)))

Сообщение Binding Update содержит опцию Nonce Indices, указывающую узлу-корреспонденту, какие одноразовые номера home nonce и care-of nonce использовать для повторного вычисления Kbm, ключа управления привязкой. Код MAC вычисляется, как описано в разд. 6.2.7, используя адрес узла-корреспондента в качестве адреса места назначения и самого сообщения Binding Update ("BU" выше) в качестве данных заголовка мобильности (MH).

После того, как узел-корреспондент проверил код MAC, он может создать для мобильного узла элемент кэша привязок.

Сообщение Binding Acknowledgement (подтверждение привязки)

В некоторых случаях сообщение Binding Update подтверждается узлом-корреспондентом. Содержимое этого сообщения следующее:

* Source Address = correspondent

* Destination Address = care-of address

* Parameters:

  + sequence number (в заголовке сообщения Binding Update)

  + First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BA)))

Сообщение Binding Acknowledgement содержит тот же самый порядковый номер, что и сообщение Binding Update. Код MAC вычисляется, как описано в разд. 6.2.7, используя адрес узла-корреспондента в качестве адреса места назначения и само сообщение ("BA" выше) в качестве данных заголовка мобильности (MH).

Время жизни привязок, устанавливаемых в узле-корреспонденте при помощи ключей, создаваемых при выполнении процедуры обратной маршрутизируемости, не должно (MUST NOT) превышать MAX_RR_BINDING_LIFETIME секунд (см. разд. 12).

Значение в поле Source Address в заголовке IPv6, переносящем сообщение Binding Update, обычно также представляет собой временный адрес, который используется в привязке. Однако путем включения в сообщение Binding Update опции мобильности Alternate Care-of Address (см. разд. 6.2.5), может быть (MAY) указан другой временный адрес. Когда такое сообщение посылается узлу-корреспонденту и в качестве метода авторизации используется процедура обратной маршрутизируемости, сообщения Care-of Test Init и Care-of Test должны (MUST) выполняться для адресов из опции Alternate Care-of Address(а не из поля Source Address). Индексы одноразовых номеров и значение кода MAC должны (MUST) основываться на информации, полученной при этой проверке.

Сообщения Binding Update могут также посылаться для уничтожения ранее установленной привязки. В этом случае формирование ключа управления привязкой зависит только от маркера home keygen token, а индекс одноразового номера care-of nonce index игнорируется.

5.2.7. Обновление ключей узла и одноразовых номеров

Узлы-корреспонденты генерируют одноразовые номера через регулярные интервалы времени. Рекомендуется каждый одноразовый номер (указываемый индексом одноразового номера) поддерживать годным в течение, по крайней мере, MAX_TOKEN_LIFETIME секунд (см. разд. 12) после того, как он впервые был использован при создании ответа на сообщение обратной маршрутизируемости. Однако узел-корреспондент не должен (MUST NOT) считать приемлемыми одноразовые номера

после MAX_NONCE_LIFETIME секунд (см. разд. 12) после первого использования. Поскольку разница между этими двумя константами составляет 30 секунд, удобным способом осуществления указанных выше времен жизни является генерация нового одноразового номера каждые 30 секунд. Тогда узел может продолжить принимать маркеры, которые были основаны на последних восьми (MAX_NONCE_LIFETIME/ 30) одноразовых номерах. Это приводит к тому, что маркеры оказываются годными в течение от MAX_TOKEN_LIFETIME до MAX_NONCE_LIFETIME секунд после того, как они были посланы мобильному узлу, в зависимости от того, был ли маркер послан в начале или в конце первого 30-секундного периода. Заметим, что узел-корреспондент может также попытаться генерировать новый одноразовый номер по запросу, или только если старые одноразовые номера были использованы. Это возможно до тех пор, пока узел-корреспондент отслеживает насколько давно одноразовые номера использовались впервые и не генерирует новых одноразовых номеров для каждого запроса обратной маршрутизируемости.

Из-за ограничений ресурсов, быстрого стирания обновлений или из-за перезагрузки узел-корреспондент может не всегда считать приемлемыми одноразовые номера, на которых основывались маркеры. Если индекс одноразового номера не признается годным, узел-корреспондент отвечает в подтверждении привязки кодом ошибки (136, 137, либо 138, как обсуждается в разд. 6.1.8). Тогда мобильный узел может повторить процедуру обратной маршрутизируемости.

Обновление Kcn должно (SHOULD) выполняться в то же время, что и обновление одноразового номера, так что индексы одноразовых номеров могут идентифицировать как одноразовый номер, так и ключ. Поэтому старые значения Kcn должны запоминаться до тех пор, пока хранятся старые значения одноразовых номеров.

Зная, что маркеры обычно предполагаются годными в течение MAX_TOKEN_LIFETIME секунд, мобильный узел может (MAY) их использовать после одного выполнения процедуры обратной маршрутизируемости до тех пор, пока не истечет время MAX_TOKEN_LIFETIME. После этого мобильный узел не должен (SHOULD NOT) использовать эти маркеры. Быстро перемещающийся мобильный узел может (MAY) повторно использовать последний маркер home keygen token от узла-корреспондента при переходе на новое местоположение, и непосредственно получить новый маркер care-of keygen token, чтобы продемонстрировать маршрутизируемость на новом местоположении.

Хотя в этом случае количество запросов и ответов из-за одновременной обработки проверок обратной маршрутизируемости не экономится, обмениваемых сообщений становится меньше, и потенциально длинный обмен запрос-ответ через домашнего агента аннулируется. Следовательно, такая оптимизация часто оказывается полезной. Мобильный узел, который имеет несколько домашних адресов, также может (MAY) использовать один и тот же маркер care-of keygen token для сообщений Binding Update, касающихся всех этих адресов.

5.2.8. Предотвращение атак повторного воспроизведения

Благодаря использованию порядковых номеров и кода MAC процедура обратной маршрутизируемости защищает также участников от повторно воспроизводимых сообщений Binding Update. Однако при удалении привязок в узле-корреспонденте необходимо соблюдать осторожность. Узел-корреспондент должен хранить привязки и связанную информацию о порядковых номерах, по крайней мере, до тех пор, пока еще остаются годными одноразовые номера, использовавшиеся при авторизации привязки. В качестве альтернативы, если память очень ограничена, узел-корреспондент может (MAY) признать недействительными одноразовые номера, которые использовались для удаляемой привязки (или некоторую группу одноразовых номеров большего размера, которой они принадлежат). Однако это может повлиять на способность принимать сообщения Binding Update от мобильных узлов, которые недавно получили маркеры keygen token. Поэтому эта альтернатива рекомендуется только как последняя возможность.

5.3. Динамическое определение адреса домашнего агента

Для динамического определения адреса домашнего агента не требуется никаких систем безопасности.

5.4. Определение мобильного префикса

Мобильный узел и домашний агент должны (SHOULD) использовать контекст безопасности IPsec для защиты целостности и аутентичности сообщений Mobile Prefix Solicitation и Mobile Prefix Advertisement. Как мобильные узлы, так и домашние агенты для обеспечения аутентификации первоисточника данных, целостности в режиме без установления соединений и дополнительной защиты от повторного воспроизведения должны (MUST) поддерживать и должны (SHOULD) использовать заголовок ESP (Encapsulating Security Payload) в транспортном режиме с ненулевым алгоритмом аутентификации полезных данных.

5.5. Пакеты полезных данных

Пакеты полезных данных, обмен которыми осуществляют мобильные узлы, могут защищаться обычным образом, тем же самым методом, которым их могут защитить стационарные хосты. Однако протокол мобильного IPv6 вводит в пакеты полезных данных опцию места назначения Home Address, заголовок маршрутизации и заголовки туннелирования. Ниже мы определяем меры безопасности, созданные для их защиты, а также для предотвращения их использования в атаках против других сторон.

Данная спецификация ограничивает использование опции места назначения Home Address ситуацией, когда узел-корреспондент уже имеет элемент кэша обновлений привязки для данного домашнего адреса. Это позволяет избежать использования опции Home Address в атаках, описанных в разд. 15.1.

Протокол мобильного IPv6 использует специальный тип заголовка маршрутизации. Этот тип заголовка обеспечивает необходимую функциональность, но не открывает слабые места в системе защиты, которые обсуждаются в разд. 15.1.

Туннели между мобильным узлом и домашним агентом защищаются путем обеспечения надлежащего использования адресов источника и дополнительной криптографической защиты. Мобильный узел проверяет, что внешний IP-адрес соответствует его домашнему агенту. Домашний агент проверяет, что внешний IP-адрес соответствует текущему местоположению мобильного узла (сообщения Binding Update, посылаемые домашнему агенту, защищены). Домашний агент идентифицирует мобильный узел по адресу источника, находящемуся во внутреннем пакете. (Обычно это домашний адрес мобильного узла, но это может быть и «локальный для линка» адрес, как обсуждается в разд. 10.4.2. Чтобы распознать последний тип адреса, домашний агент требует, чтобы в обновлении привязки был установлен флаг Link-Local Address Compatibility (L)). Эти меры защищают туннели от слабых мест, обсуждаемых в разд. 15.1.

Для трафика, туннелируемого через домашнего агента, может (MAY) поддерживаться и использоваться дополнительная инкапсуляция IPsec ESP. Если поддерживаются протоколы управления членством в мультикастовой группе или протоколы контекстного (с сохранением состояния) автоконфигурирования адресов, защита полезных данных должна (MUST) поддерживаться.

6. Новые IPv6-протокол, типы сообщений и опция места назначения

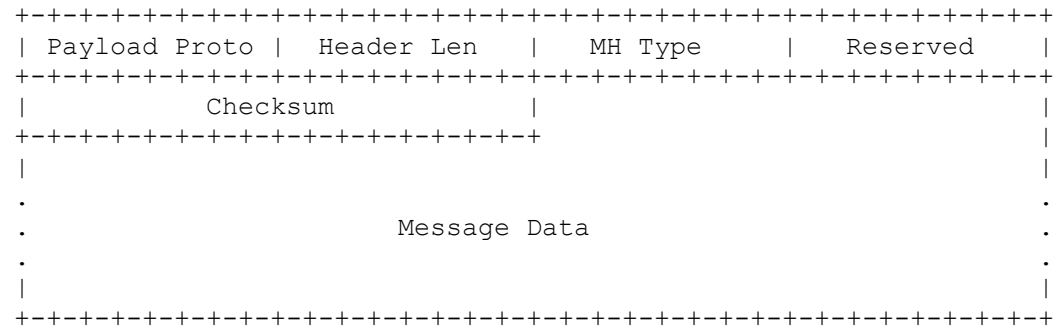
6.1. Заголовок мобильности

Заголовок мобильности (Mobility Header) представляет собой заголовок расширения, используемый мобильными узлами, узлами-корреспондентами и домашними агентами во всех обменах сообщениями, связанными с созданием привязок и управлением ими. В подразделах данного раздела описываются типы сообщений, которые могут посылаться с помощью заголовка мобильности.

Сообщения с заголовком мобильности не должны (MUST NOT) посылаться с заголовком маршрутизации типа 2, за исключением случая, описанного в разд. 9.5.4 для сообщения Binding Acknowledgement. Сообщения с заголовком мобильности также не должны (MUST NOT) использоваться с опцией места назначения Home Address, за исключением случаев, описанных в разд. 11.7.1 и 11.7.2 для сообщения Binding Update. Информация о месте назначения из списка обновлений привязки или кэша привязок (если таковая имеется) не должна (MUST NOT) использоваться при посылке сообщений с заголовком мобильности. А именно, сообщения с заголовком мобильности игнорируют (обходят) как проверку кэша привязок, описанную в разд. 9.3.2, так и проверку списка обновлений привязки, описанную в разд. 11.3.1, которые обычно выполняются для всех пакетов. Это правило применяется даже к сообщениям, посылаемым узлу-корреспонденту и принимаемым от узла-корреспондента, который сам является мобильным узлом.

6.1.1. Формат

Заголовок мобильности указывается в непосредственно предшествующем заголовке полем Next Header со значением 135 и имеет следующий формат:



Payload Proto (протокол полезных данных)

8-битовый селектор. Указывает тип заголовка, непосредственно следующего за заголовком мобильности. Использует те же самые значения, что и поле IPv6 Next Header [11].

Это поле предназначено для использования будущими расширениями (см. приложение B.1).

Реализации, соответствующие данной спецификации, должны (SHOULD) устанавливать тип протокола полезных данных в значение IPPROTO_NONE (59 десятичных).

Header Len (длина заголовка)

8-битовое целое без знака, представляющее длину заголовка мобильности в единицах по 8 октетов, исключая первые 8 октетов.

Длина заголовка мобильности должна (MUST) быть кратной 8 октетам.

MH Type (тип заголовка мобильности)

8-битовый селектор. Указывает в запросе конкретное сообщение мобильности. Текущие значения специфицированы в разд. 6.1.2 и далее. Нераспознанное поле MH Type вызывает посылку индикации ошибки.

Reserved (зарезервировано)

8-битовое поле, зарезервированное для будущего использования. Его значение должно (MUST) устанавливаться в ноль отправителем, и должно (MUST) игнорироваться получателем.

Checksum (контрольная сумма)

16-битовое целое без знака. Это поле содержит контрольную сумму заголовка мобильности. Контрольная сумма вычисляется из строки октетов, состоящей из «псевдо-заголовка», за которым следует весь заголовок мобильности, начиная с поля Payload Proto. Контрольная сумма представляет собой 16-битный обратный код суммы этой строки в обратном коде.

Псевдо-заголовок содержит поля заголовка IPv6, как специфицировано в разд. 8.1 RFC 2460 [11]. Значение поля Next Header, используемое в псевдо-заголовке равно 2. Используемые в псевдо-заголовке адреса представляют собой адреса, которые находятся в полях Source Address и Destination Address пакета IPv6, переносящего заголовок мобильности.

Заметим, что при нахождении вне дома процедуры вычисления контрольных сумм более высоких уровней, описанные в разд. 11.3.1, применяются даже к заголовку мобильности. Если сообщение мобильности имеет опцию места назначения Home Address, то вычисление контрольной суммы в качестве значения поля Source Address IPv6 использует домашний адрес из этой опции. Заголовок маршрутизации обрабатывается так, как объяснено в [11].

С целью вычисления псевдо-заголовка заголовок мобильности рассматривается как протокол более высокого уровня. Поле Upper-Layer Packet Length в псевдо-заголовке должно (MUST) быть установлено равным полной длине заголовка мобильности.

Для вычисления контрольной суммы поле контрольной суммы устанавливается в ноль.

Message Data (данные сообщения)

Поле переменной длины, содержащее данные, специфичные для указанного типа заголовка мобильности.

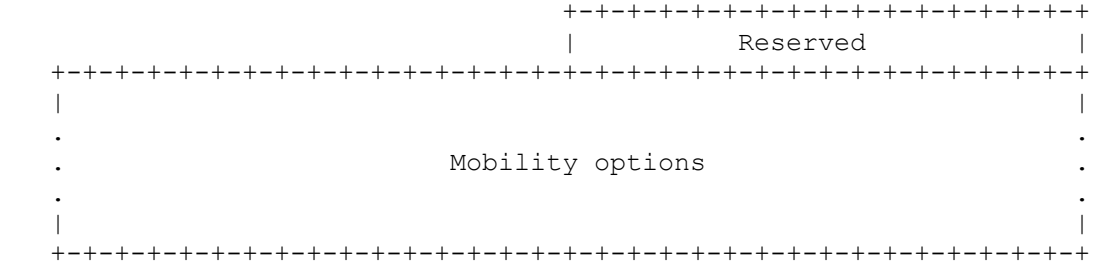
Для использования в этих сообщениях протокол мобильного IPv6 определяет целый ряд «опций мобильности» (mobility options); при включении в пакет, любая опция должна (MUST) появляться после фиксированной порции данных сообщения, указанной в данном документе. Наличие таких опций будет указываться в сообщении полем Header Len. Если значение поля Header Len больше длины, необходимой для специфицируемого здесь сообщения, то оставшиеся октеты интерпретируются как опции мобильности. Эти опции включают опции заполнителей, которые могут использоваться для того, чтобы гарантировать, что другие опции подобающим образом выровнены, и что общая длина сообщения кратна 8. Кодирование и формат определенных опций описывается в разд. 6.2.

Требования по выравниванию заголовка мобильности те же самые, что и для любого заголовка протокола IPv6. А именно, они должны быть выровнены по 8-октетной границе.

6.1.2. Сообщение Binding Refresh Request

Сообщение Binding Refresh Request (запрос обновления привязки) требует от мобильного узла обновления его привязки мобильности. Это сообщение посылается узлом-корреспондентом в соответствии с правилами разд. 9.5.5. Когда мобильный узел получает пакет, содержащий сообщение Binding Refresh Request, он обрабатывает это сообщение в соответствии с правилами разд. 11.7.4.

Сообщение Binding Refresh Request использует значение типа заголовка мобильности (MH Type) равное 0. Если это значение указывается в поле MH Type, то формат поля данных сообщения в заголовке мобильности имеет следующий вид:



Reserved (зарезервировано)

16-битовое поле, зарезервированное для будущего использования. Его значение должно (MUST) устанавливаться в ноль отправителем, и должно (MUST) игнорироваться получателем.

Mobility Options (опции мобильности)

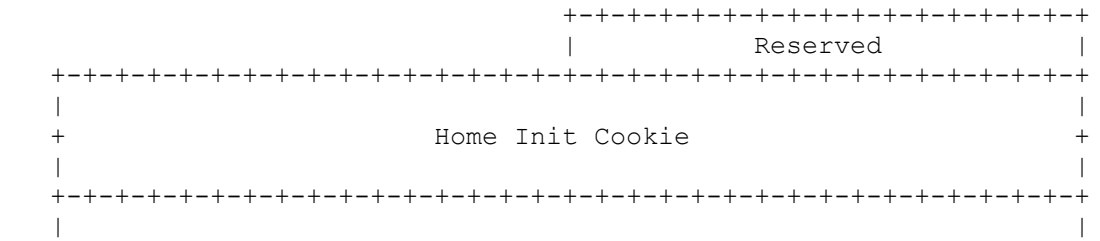
Поле переменной длины, которое имеет такую длину, что длина полного заголовока мобильности кратна 8 октетам. Это поле содержит ноль или несколько опций мобильности, закодированных в формате TLV. Кодирование и формат определенных опций описаны в разд. 6.2. Получатель должен (MUST) игнорировать и пропускать любые опции, которые он не понимает.

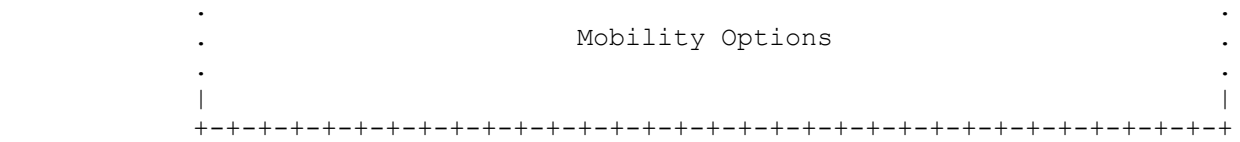
Может (MAY) существовать дополнительная информация, связанная с данным сообщением Binding Refresh Request, которая не требуется во всех посылаемых сообщениях Binding Refresh Request. Опции мобильности позволяют определить будущие расширения формата сообщения Binding Refresh Request. Данная спецификация не определяет ни одной опции, допустимой для сообщения Binding Refresh Request.

Если в данном сообщении реальные опции отсутствуют, то нет необходимости в заполнении, и поле Header Len будет установлено в 0.

6.1.3. Сообщение Home Test Init

Мобильный узел использует сообщение Home Test Init (HoTI) для инициализации процедуры обратной маршрутизируемости и запроса маркера home keygen token от узла-корреспондента (см. разд. 11.6.1). Сообщение Home Test Init использует значение типа заголовка мобильности (MH Type) равное 1. Если это значение указывается в поле MH Type, то формат поля данных сообщения в заголовке мобильности имеет следующий вид:





Reserved (зарезервировано)

16-битовое поле, зарезервированное для будущего использования. Его значение должно (MUST) устанавливаться в ноль отправителем, и должно (MUST) игнорироваться получателем.

Home Init Cookie (идентифицирующая цепочка Home Init Cookie)

64-битовое поле, которое содержит случайное значение – идентифицирующую цепочку Home Init Cookie.

Mobility Options (опции мобильности)

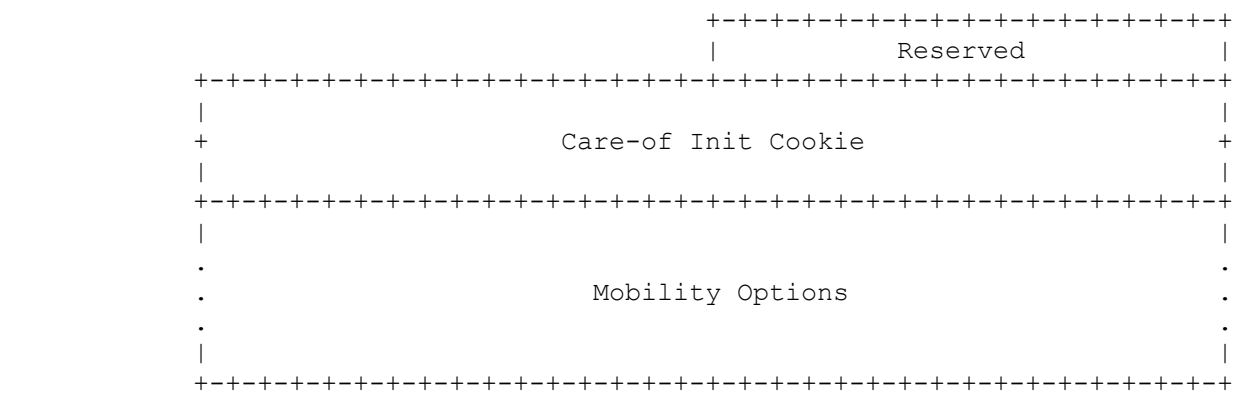
Поле переменной длины, которое имеет такую длину, что длина полного заголовока мобильности кратна 8 октетам. Это поле содержит ноль или несколько опций мобильности, закодированных в формате TLV. Получатель должен (MUST) игнорировать и пропускать любые опции, которые он не понимает. Данная спецификация не определяет ни одной опции, допустимой для сообщения Home Test Init.

Если в данном сообщении реальные опции отсутствуют, то нет необходимости в заполнении, и поле Header Len будет установлено в 1.

Это сообщение туннелируется через домашнего агента, когда мобильный узел находится вне дома. Такое туннелирование между домашним агентом и мобильным узлом должно (SHOULD) использовать IPsec ESP в туннельном режиме. Эта защита указывается базой данных политики безопасности IPsec. Защита сообщений Home Test Init не связана с требованием защиты обычного трафика полезных данных, которая также может (MAY) использовать такие туннели.

6.1.4. Сообщение Care-of Test Init

Мобильный узел использует сообщение Care-of Test Init (CoTI) для инициализации процедуры обратной маршрутизируемости и запроса маркера care-of keygen token от узла-корреспондента (см. разд. 11.6.1). Сообщение Care-of Test Init использует значение типа заголовка мобильности (MH Type) равное 2. Если это значение указывается в поле MH Type, то формат поля данных сообщения в заголовке мобильности имеет следующий вид:



Reserved (зарезервировано)

16-битовое поле, зарезервированное для будущего использования. Его значение должно (MUST) устанавливаться в ноль отправителем, и должно (MUST) игнорироваться получателем.

Care-of Init Cookie (идентифицирующая цепочка Care-of Init Cookie)

64-битовое поле, которое содержит случайное значение – идентифицирующую цепочку care-of init cookie.

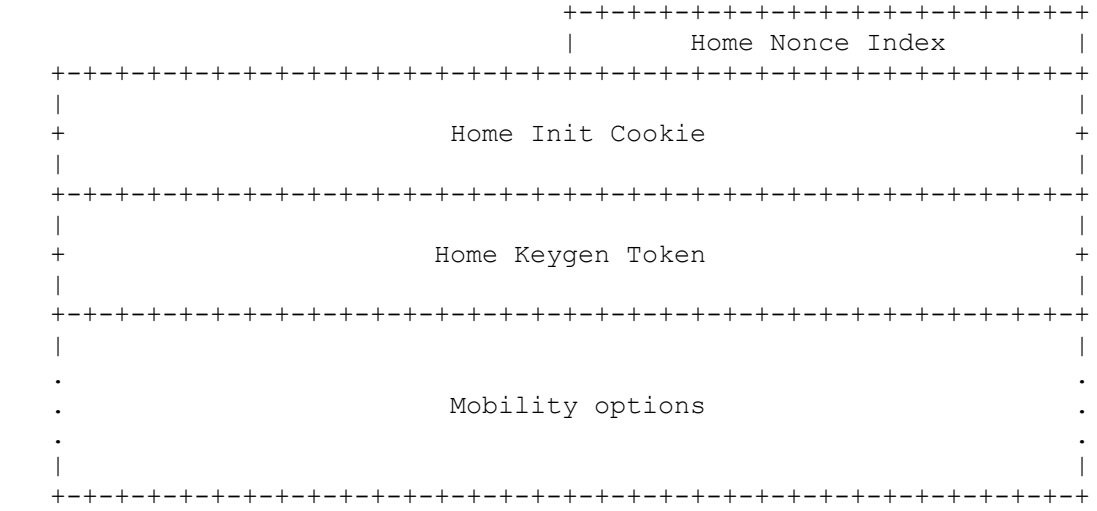
Mobility Options (опции мобильности)

Поле переменной длины, которое имеет такую длину, что длина полного заголовока мобильности кратна 8 октетам. Это поле содержит ноль или несколько опций мобильности, закодированных в формате TLV. Получатель должен (MUST) игнорировать и пропускать любые опции, которые он не понимает. Данная спецификация не определяет ни одной опции, допустимой для сообщения Care-of Test Init.

Если в данном сообщении реальные опции отсутствуют, то нет необходимости в заполнении, и поле Header Len будет установлено в 1.

6.1.5. Сообщение Home Test

Сообщение Home Test (HoT) представляет собой ответ на сообщение Home Test Init и посылается узлом-корреспондентом мобильному узлу (см. разд. 5.2.5). Сообщение Home Test использует значение типа заголовка мобильности (MH Type) равное 3. Если это значение указывается в поле MH Type, то формат поля данных сообщения в заголовке мобильности имеет следующий вид:



Home Nonce Index (индекс одноразового номера Home Nonce)

Это поле будет возвращено обратно узлу-корреспонденту мобильным узлом в последующем сообщении Binding Update.

Home Init Cookie (идентифицирующая цепочка Home Init Cookie)

64-битовое поле содержит идентифицирующую цепочку Home Init Cookie.

Home Keygen Token (маркер Home Keygen Token)

Это поле содержит 64 бита маркера home keygen token, используемого в процедуре обратной маршрутизируемости.

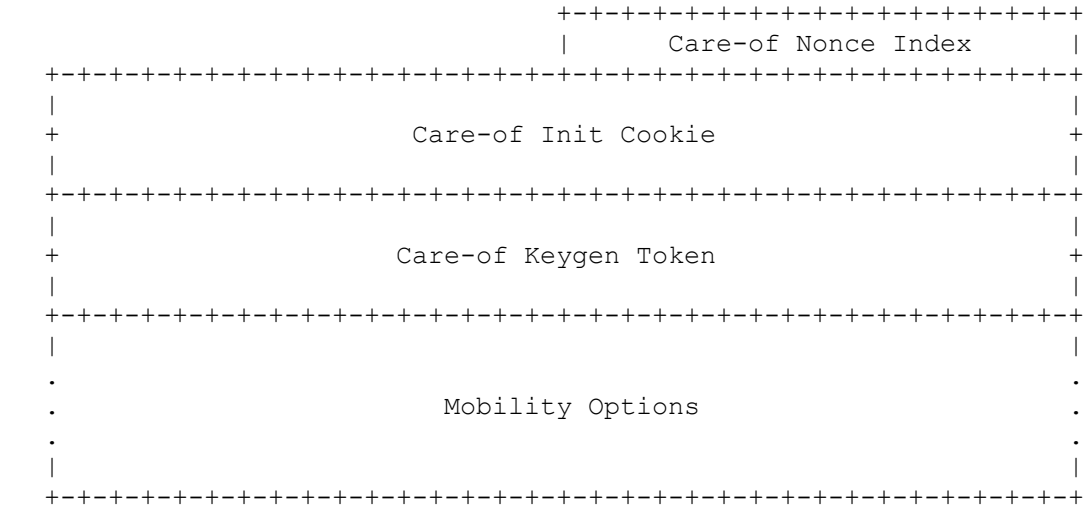
Mobility Options (опции мобильности)

Поле переменной длины, которое имеет такую длину, что длина полного заголовока мобильности кратна 8 октетам. Это поле содержит ноль или несколько опций мобильности, закодированных в формате TLV. Получатель должен (MUST) игнорировать и пропускать любые опции, которые он не понимает. Данная спецификация не определяет ни одной опции, допустимой для сообщения Home Test.

Если в данном сообщении реальные опции отсутствуют, то нет необходимости в заполнении, и поле Header Len будет установлено в 2.

6.1.6. Сообщение Care-of Test

Сообщение Care-of Test (CoT) представляет собой ответ на сообщение Care-of Test Init и посылается узлом-корреспондентом мобильному узлу (см. разд. 11.6.2). Сообщение Care-of Test использует значение типа заголовка мобильности (MH Type) равное 4. Если это значение указывается в поле MH Type, то формат поля данных сообщения в заголовке мобильности имеет следующий вид:



Care-of Nonce Index (индекс одноразового номера Care-of Nonce)

Это значение возвращается назад узлу-корреспонденту мобильным узлом в последующем сообщении Binding Update.

Care-of Init Cookie (идентифицирующая цепочка Care-of Init Cookie)

64-битовое поле, которое содержит идентифицирующую цепочку Care-of Init Cookie.

Care-of Keygen Token (маркер Care-of Keygen Token)

Это поле содержит 64 бита маркера care-of keygen token, используемого в процедуре обратной маршрутизируемости.

Mobility Options (опции мобильности)

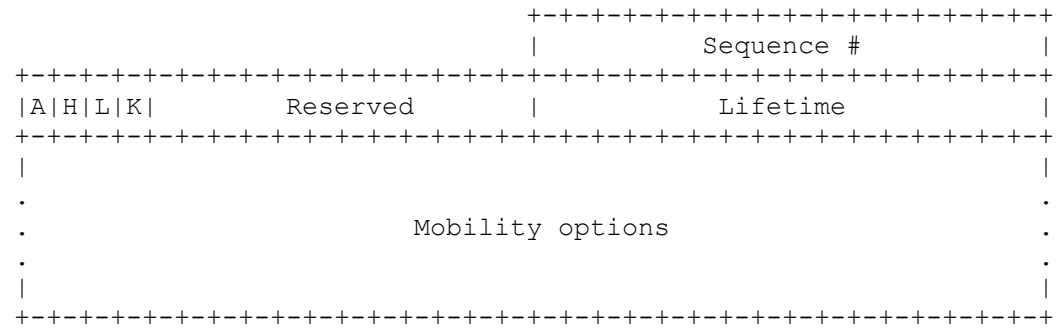
Поле переменной длины, которое имеет такую длину, что длина полного заголовока мобильности кратна 8 октетам. Это поле содержит ноль или несколько опций мобильности, закодированных в формате TLV. Получатель должен (MUST) игнорировать и пропускать любые опции, которые он не понимает. Данная спецификация не определяет ни одной опции, допустимой для сообщения Care-of Test.

Если в данном сообщении реальные опции отсутствуют, то нет необходимости в заполнении, и поле Header Len будет установлено в 2.

6.1.7. Сообщение Binding Update

Сообщение Binding Update (BU) используется мобильным узлом для уведомления других узлов о своем новом временном адресе. Сообщения Binding Update посылаются, как описано в разд. 11.7.1 и 11.7.2.

Сообщение Binding Update использует значение типа заголовка мобильности (MH Type) равное 5. Если это значение указывается в поле MH Type, то формат поля данных сообщения в заголовке мобильности имеет следующий вид:



Acknowledge (A) (подтверждение)

Бит подтверждения - Acknowledge (A) устанавливается посылающим мобильным узлом для того, чтобы потребовать возврата подтверждения привязки - Binding Acknowledgement (разд. 6.1.8) после получения обновления привязки.

Home Registration (H) (регистрация в домашнем агенте)

Бит регистрации в домашнем агенте - Home Registration (H) устанавливается посылающим мобильным узлом для того, чтобы потребовать, чтобы принимающий узел служил ему домашним агентом. Местом назначения пакета, переносящего это сообщение, должен (MUST) быть тот маршрутизатор, который имеет тот же самый префикс подсети, что и домашний адрес мобильного узла в привязке.

Link-Local Address Compatibility (L) (соответствие «локального для линка» адреса)

Бит соответствия «локального для линка» адреса - Link-Local Address Compatibility (L) устанавливается, когда домашний адрес, переданный мобильным узлом, имеет тот же самый идентификатор интерфейса, что и «локальный для линка» адрес мобильного узла.

Key Management Mobility Capability (K) (возможность мобильного управления ключами)

Если этот бит обнуляется, то протокол, используемый для установления контекстов безопасности IPsec между мобильным узлом и домашним агентом, не переносит перемещений. Тогда, вероятно, он должен быть запущен заново. (Заметим, что предполагается, что сами контексты безопасности IPsec переносят перемещения). Если используется ручное конфигурирование IPsec, то этот бит должен быть обнулен.

Этот бит является правомерным только в сообщениях Binding Update, посылаемых домашнему агенту, и должен (MUST) обнуляться в других сообщениях Binding Update. Узлы-корреспонденты должны (MUST) игнорировать этот бит.

Reserved (зарезервировано)

Эти поля не используются. Они должны (MUST) быть установлены в ноль отправителем и игнорироваться приемником.

Sequence # (порядковый номер)

16-битовое целое без знака используется принимающим узлом для упорядочивания сообщений Binding Update и узлом-отправителем для сопоставления сообщения Binding Acknowledgement с данным сообщением Binding Update.

Lifetime (время жизни)

16-битовое целое без знака. Количество единиц времени, оставшихся до того момента, когда привязка должна (MUST) считаться просроченной. Нулевое значение указывает на то, что элемент кэша привязок для мобильного узла должен (MUST) быть удален. (В этом случае указанный временный адрес также должен (MUST) быть установлен равным домашнему адресу). Единицей времени являются 4 секунды.

Mobility Options (опции мобильности)

Поле переменной длины, которое имеет такую длину, что длина полного заголовока мобильности кратна 8 октетам. Это поле содержит ноль или несколько опций мобильности, закодированных в формате TLV. Кодирование и формат определенных опций описываются в разд. 6.2. Получатель должен (MUST) игнорировать и пропускать любые опции, которые он не понимает.

В сообщении Binding Update допустимы следующие опции:

* Опция Binding Authorization Data (данные авторизации привязки) (эта опция является обязательной в сообщениях Binding Update, посылаемых узлу-корреспонденту)

* Опция Nonce Indices (индексы одноразовых номеров)

* Опция Alternate Care-of Address (альтернативный (запасной) временный адрес)

Если в данном сообщении опции отсутствуют, необходимы 4 октета заполнителя, и поле Header Len будет установлено в 1.

Временный адрес определяется либо полем Source Address в заголовке IPv6, либо опцией Alternate Care-of Address, если она присутствует. Временный адрес должен (MUST) быть индивидуальным маршрутизируемым адресом. Сообщения Binding Update для временного адреса, который не является индивидуальным маршрутизируемым адресом, должны (MUST) быть молча отброшены. Подобным образом, сообщение Binding Update должно (MUST) быть молча отброшено, если в существующем элементе кэша привязок временный адрес выступает как домашний адрес, создавая своим местоположением циклическую ссылку назад на домашний адрес, указанный в сообщении Binding Update (возможно через дополнительные элементы).

Удаление привязки может указываться путем установки в ноль поля Lifetime и установки временного адреса равным домашнему адресу. При удалении формирование ключа управления привязкой зависит только от маркера home keygen token, как пояснено в разд. 5.2.5. (Заметим, что в то время как от отправителей требуется установка как поля Lifetime в 0, так и временного адреса равным домашнему адресу, правила разд. 9.5.1 для получателей более либеральные, и интерпретируют любое из условий как удаление).

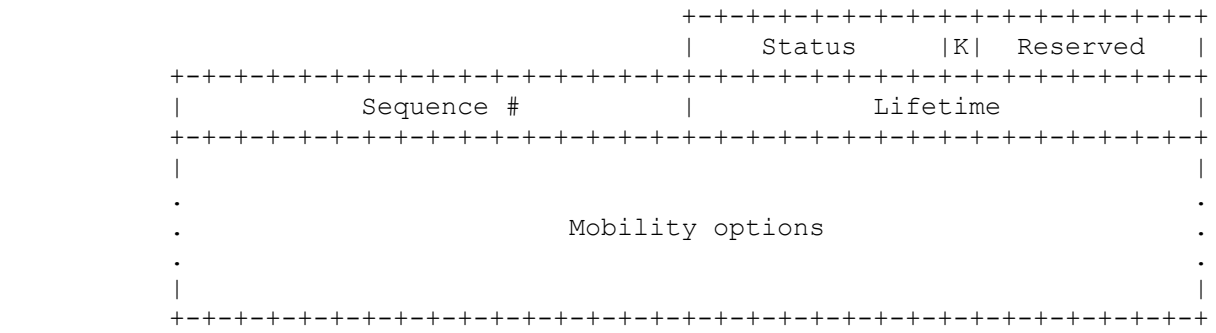
Узлы-корреспонденты не должны (SHOULD NOT) удалять элемент кэша привязок до истечения времени жизни, если имеется вероятность того, что любое приложение,

работающее на узле-корреспонденте, еще может потребовать обмена информацией с узлом-корреспондентом. Элемент кэша привязок, который освобождается преждевременно, может вызвать сброс последующих пакетов от мобильного узла, если они содержат опцию места назначения Home Address. Эта ситуация восстановима, поскольку мобильному узлу посылается сообщение Binding Error (см. разд. 6.1.9); однако она вызывает ненужную задержку обменов информацией.

6.1.8. Сообщение Binding Acknowledgement

Сообщение Binding Acknowledgement (подтверждение привязки) используется для подтверждения получения сообщения Binding Update (разд. 6.1.7). Этот пакет посылается, как описано в разд. 9.5.4 и 10.3.1.

Сообщение Binding Acknowledgement имеет значение типа заголовка мобильности (MH Type) равное 6. Если это значение указывается в поле MH Type, то формат поля данных сообщения в заголовке мобильности имеет следующий вид:



Key Management Mobility Capability (K) (возможность мобильного управления ключами)

Если этот бит обнуляется, то протокол, используемый домашним агентом для установления контекстов безопасности IPsec между мобильным узлом и домашним агентом, не переносит перемещений. Тогда, вероятно, он должен быть запущен заново. (Заметим, что предполагается, что сами контексты безопасности IPsec переносят перемещения).

Узлы-корреспонденты должны (MUST) устанавливать этот бит в 0.

Reserved (зарезервировано)

Эти поля не используются. Они должны (MUST) устанавливаться в ноль отправителем и должны (MUST) игнорироваться приемником.

Status (статус)

8-битовое целое без знака, указывающее решение, принятое при обработке сообщения Binding Update. Значения поля Status, меньшие 128, указывают на то, что сообщение Binding Update было признано годным принимающим узлом. Значения, большие или равные 128, указывают на то, что сообщение Binding Update было отклонено принимающим узлом. В настоящее время определены следующие значения поля Status:

0 Binding Update accepted (обновление привязки признано годным)

1 Accepted but prefix discovery necessary (признано годным, но требуется определение префиксов)

128 Reason unspecified (причина не специфицирована)

129 Administratively prohibited (запрещено административно)

130 Insufficient resources (недостаточно ресурсов)

131 Home registration not supported (регистрация в домашнем агенте не поддерживается)

132 Not home subnet (не домашняя сеть)

133 Not home agent for this mobile node (не является домашним агентом для этого мобильного узла)

134 Duplicate Address Detection failed (определение дублирования адреса закончилось неудачей)

135 Sequence number out of window (порядковый номер вне окна)

136 Expired home nonce index (просроченный индекс одноразового номера home nonce)

137 Expired care-of nonce index (просроченный индекс одноразового номера care-of nonce)

138 Expired nonces (просроченные одноразовые номера)

139 Registration type change disallowed (изменение типа регистрации не допускается)

Новые значения поля Status должны быть специфицированы в реестре присвоенных номеров IANA [19].

Sequence # (порядковый номер)

Порядковый номер в сообщении Binding Acknowledgement копируется из поля Sequence Number сообщения Binding Update. Оно используется мобильным узлом при сопоставлении данного сообщения Binding Acknowledgement с сообщением Binding Update, ожидающим завершения выполнения.

Lifetime (время жизни)

Предоставленное время жизни, в единицах времени по 4 секунды, для которого данный узел должен (SHOULD) сохранять элемент для этого мобильного узла в своем кэше привязок.

Значение этого поля не определено, если поле Status указывает на то, что обновление привязки было признано негодным.

Mobility Options (опции мобильности)

Поле переменной длины, которое имеет такую длину, что длина полного заголовка мобильности кратна 8 октетам. Это поле содержит ноль или несколько опций мобильности, закодированных в формате TLV. Кодирование и формат определенных опций описываются в разд. 6.2. Получатель должен (MUST) игнорировать и пропускать любые опции, которые он не понимает.

Может существовать дополнительная информация, связанная с данным подтверждением привязки, которая необязательно должна присутствовать во всех посылаемых подтверждениях привязки. Опции мобильности позволяют определить будущие расширения подтверждений привязки. Для подтверждения привязки следующие опции являются допустимыми:

* Опция Binding Authorization Data (данные авторизации привязки) (эта опция является обязательной в подтверждениях привязки, посылаемых узлом-корреспондентом, за исключением случаев, указанных в разд. 9.5.4)

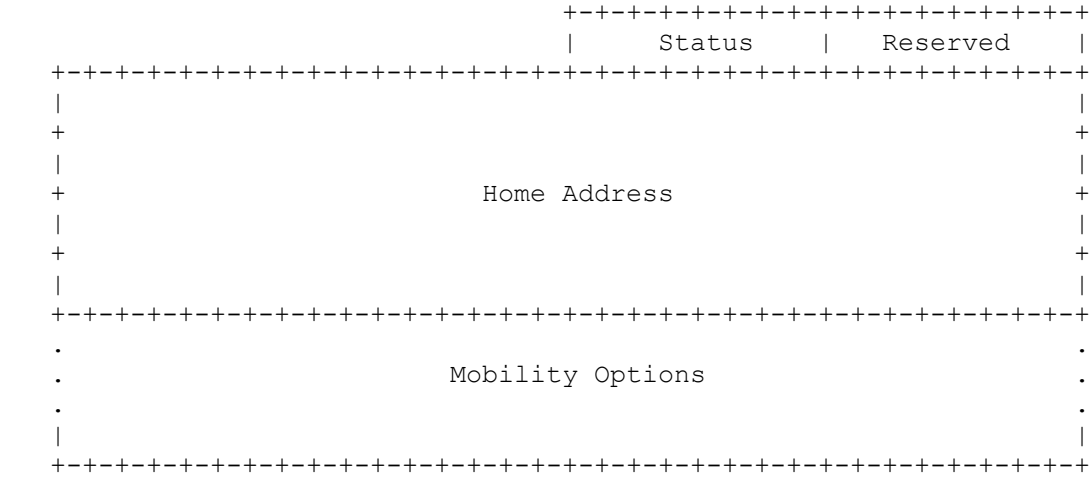
* Опция Binding Refresh Advice (совет обновить привязку)

Если в этом сообщении опции отсутствуют, то необходимы 4 октета заполнения, и поле Header Len будет установлено в 1.

6.1.9. Сообщение Binding Error

Сообщение Binding Error (BE) используется узлом-корреспондентом для сигнализации ошибки, связанной с мобильностью, такой, например, как неуместная попытка использования опции места назначения Home Address без существующей привязки; подробности см. в разд. 9.3.3.

Сообщение Binding Error имеет значение типа заголовка мобильности (MH Type) равное 7. Если это значение указывается в поле MH Type, то формат поля данных сообщения в заголовке мобильности имеет следующий вид:



Status (статус)

8-битовое целое без знака, указывающее причину этого сообщения. В настоящий момент определены следующие значения:

1 Unknown binding for Home Address destination option
(для опции места назначения Home Address привязка не известна)

2 Unrecognized MH Type value
(неопознанное значение типа заголовка мобильности)

Reserved (зарезервировано)

8-битовое поле, зарезервированное для будущего использования. Это значение должно (MUST) устанавливаться в ноль отправителем и должно (MUST) игнорироваться приемником.

Home Address (домашний адрес)

Домашний адрес, который находился в опции места назначения Home Address. В случаях, когда мобильный узел имеет несколько домашних адресов, он использует эту информацию для определения того, какая привязка не существует.

Mobility Options (опции мобильности)

Поле переменной длины, которое имеет такую длину, что длина полного заголовка мобильности кратна 8 октетам. Это поле содержит ноль или несколько опций мобильности, закодированных в формате TLV. Получатель должен (MUST) игнорировать и пропускать любые опции, которые он не понимает.

Может существовать дополнительная информация, связанная с данным сообщением Binding Error, которая необязательно должна присутствовать во всех посылаемых сообщениях Binding Error. Опции мобильности позволяют определить будущие расширения формата сообщений Binding Error. Кодирование и формат определенных опций описывается в разд. 6.2. Данная спецификация не определяет ни одной опции, допустимой для сообщений Binding Error.

Если в данном сообщении опции отсутствуют, то необходимость в заполнении отсутствует, и поле Header Len будет установлено в 2.

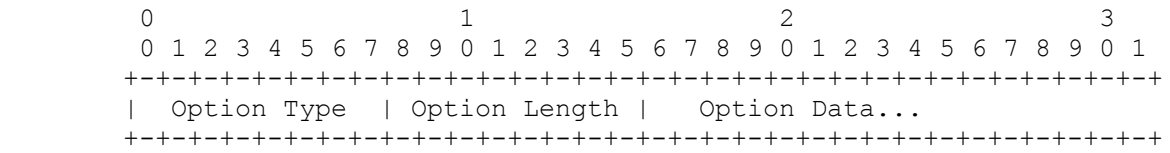
6.2. Опции мобильности

Сообщения мобильности могут включать ноль или несколько опций мобильности. Такая возможность предоставляет факультативные поля, которые необязательно должны присутствовать при каждом использовании конкретного заголовка мобильности, а также возможность будущих расширений формата сообщений. Такие опции включаются в поле Message Data самого сообщения после фиксированной части данных сообщения, специфицированных в подразделах сообщений раздела 6.1.

Наличие таких опций будет указываться полем Header Len заголовка мобильности. Если включается опция Binding Authorization Data (разд. 6.2.7), то она должна (MUST) быть последней опцией и не должна (MUST NOT) иметь завершающего заполнения. В противном случае, опции могут помещаться в любом порядке.

6.2.1. Формат

Опции мобильности кодируются в оставшемся пространстве поля Message Data сообщения мобильности с помощью формата тип – длина - значение (TLV) следующим образом:



Option Type (тип опции)

8-битовый идентификатор типа опции мобильности. При обработке заголовка мобильности, содержащего опцию, для которой приемник не распознает значения Option Type, приемник должен (MUST) тихо игнорировать и пропустить опцию, правильно обрабатывая любые оставшиеся в сообщении опции.

Option Length (длина опции)

8-битовое целое без знака, представляющее длину опции мобильности в октетах, не включая полей Option Type и Option Length.

Option Data (данные опции)

Поле переменной длины, которое содержит специфические для опции данные.

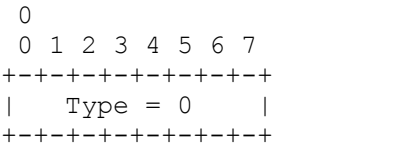
Следующие подразделы специфицируют типы опций, которые в текущий момент времени определяются для использования в заголовке мобильности.

Реализации должны (MUST) молча игнорировать любые опции мобильности, которые они не понимают.

Опции мобильности могут иметь требования по выравниванию. Следуя соглашениям IPv6, эти опции выровнены в пакете так, что многооктетные значения в пределах поля Option Data каждой опции завершаются на естественных границах (т.е., поля шириною n октетов размещаются на целое кратное n октетов от начала заголовка, для n = 1, 2, 4, or 8) [11].

6.2.2. Опция Pad1

Опция Pad1 не имеет никаких требований по выравниванию. Она имеет следующий формат:

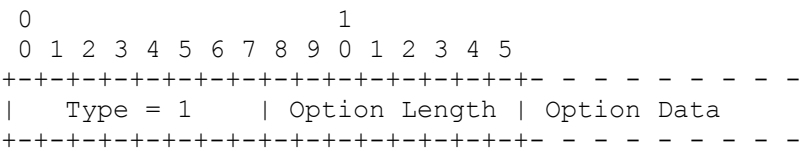


Примечание! Формат опции Pad1 представляет собой специальный случай – она не имеет ни поля Option Length, ни поля Option Data.

Опция Pad1 используется для вставки одного октета заполнения в область опций мобильности заголовка мобильности. Если требуется более одного октета заполнения, то должна использоваться описанная далее опция PadN, а не несколько опций Pad1.

6.2.3. Опция PadN

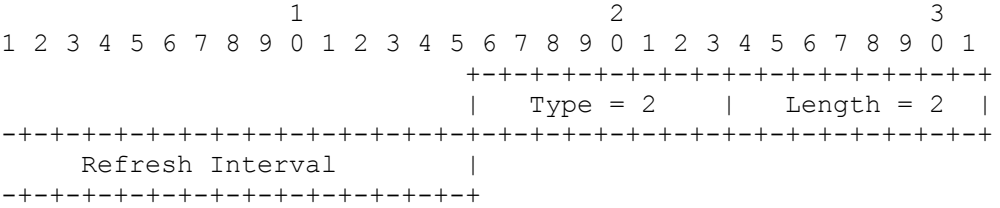
Опция PadN не имеет никаких требований по выравниванию. Она имеет следующий формат:



Опция PadN используется для вставки двух и более октетов заполнения в область опций мобильности сообщения мобильности. Для N октетов заполнения поле Option Length содержит значение N-2, а поле Option Data содержит N-2 октета с нулевым значением. Данные опции PadN должны (MUST) игнорироваться получателем.

6.2.4. Опция Binding Refresh Advice

Опция Binding Refresh Advice (совет обновить привязку) имеет требование по выравниванию 2n. Она имеет следующий формат:

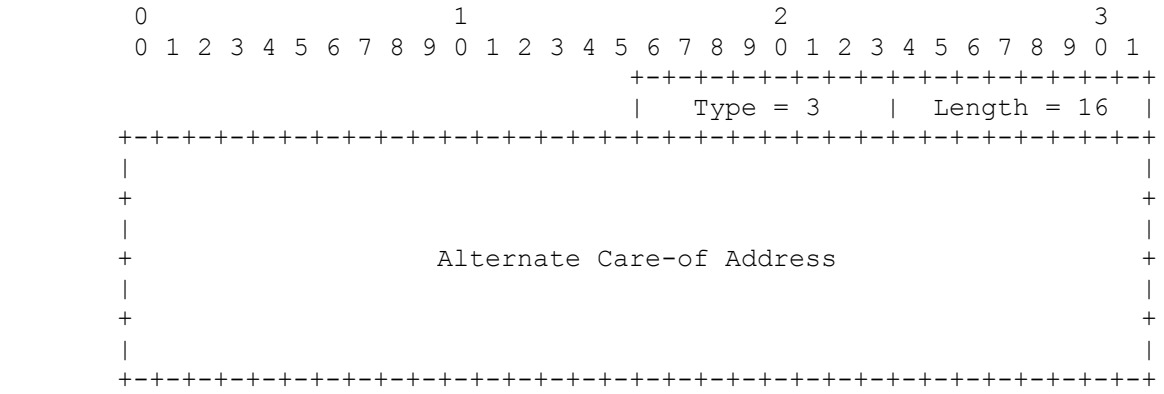


Опция Binding Refresh Advice допустима только в сообщениях Binding Acknowledgement, и только в тех сообщениях Binding Acknowledgement, которые посылаются от домашнего агента мобильного узла в ответ на регистрацию в домашнем агенте. Интервал обновления (Refresh Interval) измеряется в единицах по четыре секунды и указывает время, оставшееся до того момента, когда мобильный узел должен (SHOULD) послать домашнему агенту новую регистрацию в домашнем агенте. Поле Re-

fresh Interval должно (MUST) быть установлено для указания меньшего интервала времени, чем значение поля Lifetime сообщения Binding Acknowledgement.

6.2.5. Опция Alternate Care-of Address

Опция Alternate Care-of Address (альтернативный временный адрес) имеет требование по выравниванию 8n+6. Она имеет следующий формат:

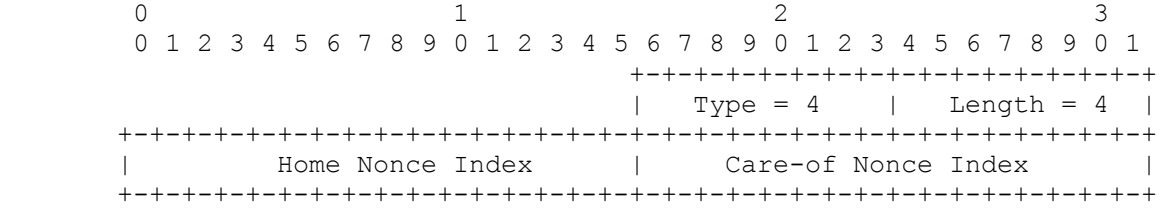


Обычно сообщение Binding Update указывает требуемый временный адрес в поле Source Address заголовка IPv6. Однако в некоторых случаях это невозможно, например, когда мобильный узел хочет указать временный адрес, который он не может использовать как типологически правильный адрес источника (разд. 6.1.7 и 11.7.2), или когда используемый механизм безопасности не защищает заголовок IPv6 (разд. 11.7.1).

Для таких ситуаций предоставляется опция Alternate Care-of Address. Эта опция допустима только в сообщении Binding Update. Поле Alternate Care-of Address содержит адрес, который должен использоваться для привязки в качестве временного адреса вместо использования для этих целей поля Source Address пакета.

6.2.6. Опция Nonce Indices

Опция Nonce Indices (индексы одноразовых номеров) имеет требование по выравниванию 2n. Она имеет следующий формат:



Опция Nonce Indices допустима только в сообщении Binding Update, посылаемом узлу-корреспонденту, и только когда она появляется вместе с опцией Binding Authorization Data. Когда узел-корреспондент авторизует сообщение Binding Update,

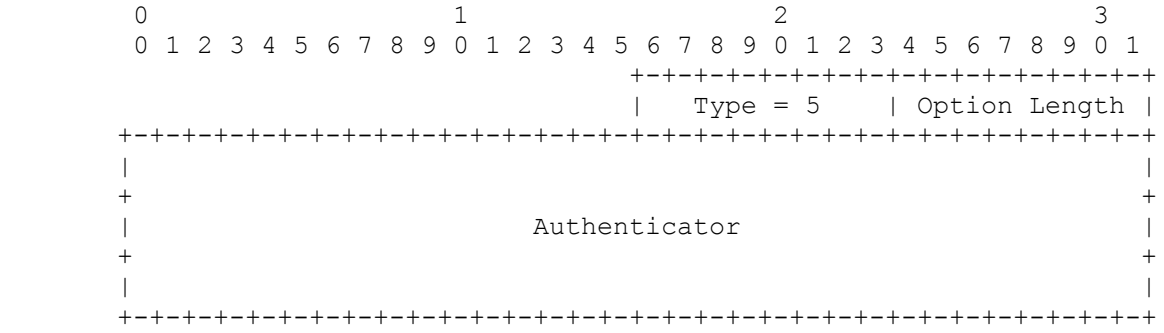
он должен сформировать из своих сохраненных случайных одноразовых номеров маркеры home keygen token и care-of keygen token.

Поле Home Nonce Index (индекс одноразового номера Home Nonce) указывает узлу-корреспонденту, какое значение одноразового номера он должен использовать для формирования маркера home keygen token.

Поле Care-of Nonce Index (индекс одноразового номера Care-of Nonce) указывает узлу-корреспонденту, какое значение одноразового номера он должен использовать для формирования маркера care-of keygen token.

6.2.7. Опция Binding Authorization Data

Опция Binding Authorization Data (данные авторизации привязки) по существу не имеет требований по выравниванию. Однако поскольку эта опция должна быть последней опцией мобильности, неявным требованием выравнивания является 8n + 2. Эта опция имеет следующий формат:



Опция Binding Authorization Data допустима только в сообщениях Binding Update и Binding Acknowledgement.

Поле Option Length содержит длину удостоверения (поля Authenticator) в октетах.

Поле Authenticator (удостоверение) содержит криптографическое значение, которое может использоваться для определения того, что сообщение в запросе приходит от правильного полномочного органа. Правила вычисления этого значения зависят от используемой процедуры авторизации.

Для процедуры обратной маршрутизируемости эта опция может появляться в сообщениях Binding Update и Binding Acknowledgement. Правила вычисления значения поля Authenticator следующие:

```
Mobility Data = care-of address | correspondent | MH Data
Authenticator = First (96, HMAC_SHA1 (Kbm, Mobility Data))
```

Где символ | означает конкатенацию. "care-of address" является временным адресом, который будет регистрироваться для мобильного узла, если сообщение Binding Update успешно проходит проверку, или домашним адресом мобильного узла, если эта опция используется для отмены регистрации. Заметим также, что этот адрес может отличаться от адреса источника сообщения Binding Update, если используется опция мобильности Alternative Care-of Address, или когда время жизни привязки устанавливается в ноль.

"correspondent" представляет собой IPv6-адрес узла-корреспондента. Заметим, что если сообщение посылается на место назначения, которое само по себе является мобильным, адрес "correspondent" может не совпадать с адресом, находящимся в

поле Destination Address заголовка IPv6; вместо этого должен использоваться домашний адрес из заголовка маршрутизации типа 2.

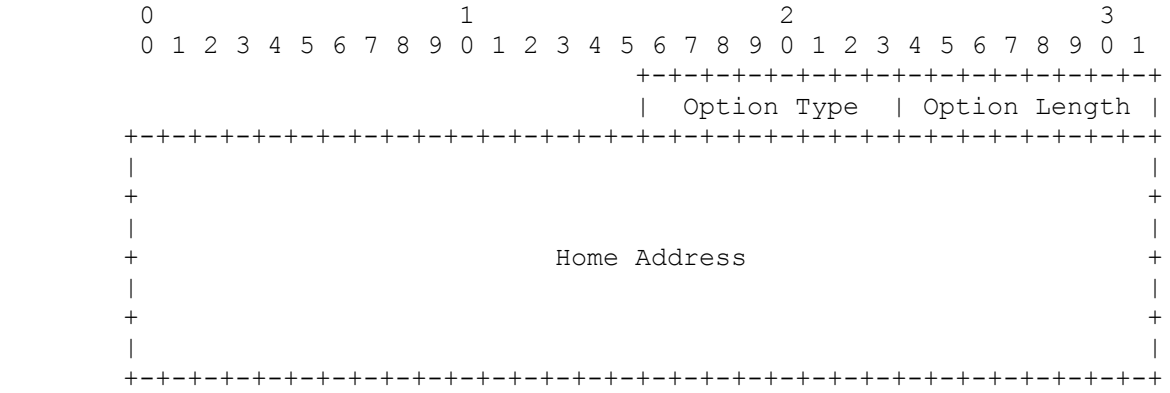
"MH Data" представляет собой содержимое заголовка мобильности, исключая само поле Authenticator. Значение поля Authenticator вычисляется, как если бы поле Checksum в заголовке мобильности было нулевым. Однако контрольная сумма в передаваемом пакете вычисляется обычным способом с вычисленным значением поля Authenticator, являющимся частью пакета, защищенного этой контрольной суммой. Kbm представляет собой ключ управления привязкой, который обычно создается с помощью одноразовых номеров, предоставляемых узлом-корреспондентом (см. разд.9.4). Заметим, что хотя содержимое потенциальной опции места назначения Home Address не покрыто в этой формуле, правила вычисления Kbm учитывают домашний адрес. Это гарантирует, что коды MAC для различных домашних адресов будут отличаться.

В качестве поля Authenticator используются первые 96 бит результата вычисления MAC.

6.3. Опция Home Address

Опция Home Address передается с помощью заголовка расширения Destination Option (значение Next Header = 60). Она используется в пакете, посылаемом мобильным узлом, находящимся вне дома, для информирования получателя о домашнем адресе мобильного узла.

Опция Home Address кодируется в формате тип-длина-значение (TLV) следующим образом:



Option Type (тип опции)

201 = 0xC9

Option Length (длина опции)

8-битовое целое без знака. Длина опции в октетах, исключая поля Option Type и Option Length. Это поле должно (MUST) устанавливаться в значение 16.

Home Address (домашний адрес)

Домашний адрес мобильного узла, посылающего пакет. Этот адрес должен (MUST) быть индивидуальным маршрутизируемым адресом.

Требованием выравнивания [11] для опции Home Address является 8n+6.

Три старших бита поля Option Type кодируются для указания особой обработки опции [11]; для опции Home Address эти три бита устанавливаются в значение 110. Это указывает на следующие требования к обработке:

- Любой узел IPv6, который не распознает поле Option Type, должен отбросить пакет и, если адрес места назначения пакета не представлял собой групповой адрес, вернуть на адрес источника пакета сообщение ICMP Parameter Problem, Code 2. Поле Pointer в сообщении ICMP должно (SHOULD) указывать на поле Option Type. В противном случае, для группового адреса сообщение ICMP посылаться не должно (MUST NOT).

- Данные внутри опции не могут изменяться по пути к конечному месту назначения пакета.

Опция Home Address должна (MUST) размещаться следующим образом:

- После заголовка маршрутизации, если этот заголовок имеется.

- До заголовка фрагментации, если этот заголовок имеется.

- До заголовка AH или заголовка ESP, если имеется любой один из этих заголовков.

Для каждого заголовка пакета IPv6 опция Home Address не должна (MUST NOT) появляться более одного раза. Однако инкапсулированный пакет [15] может (MAY) содержать отдельную опцию Home Address, связанную с каждым инкапсулирующим IP-заголовком.

Включение в пакет опции места назначения Home Address оказывает влияние на обработку принимающим узлом только одного данного пакета. В результате получения в пакете опции Home Address в принимающем узле не создается и не модифицируется никакое состояние. В частности, наличие опции Home Address в принятом пакете не должно (MUST NOT) менять содержимое кэша привязок получателя и не должно (MUST NOT) вызывать никаких изменений в маршрутизации последующих пакетов, посылаемых этим принимающим узлом.

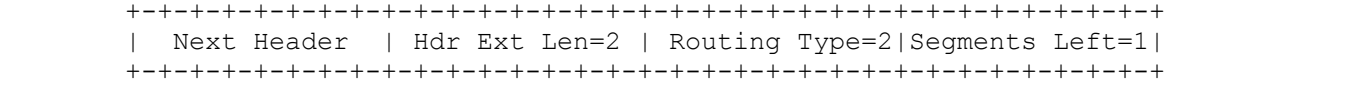
6.4. Заголовок маршрутизации типа 2

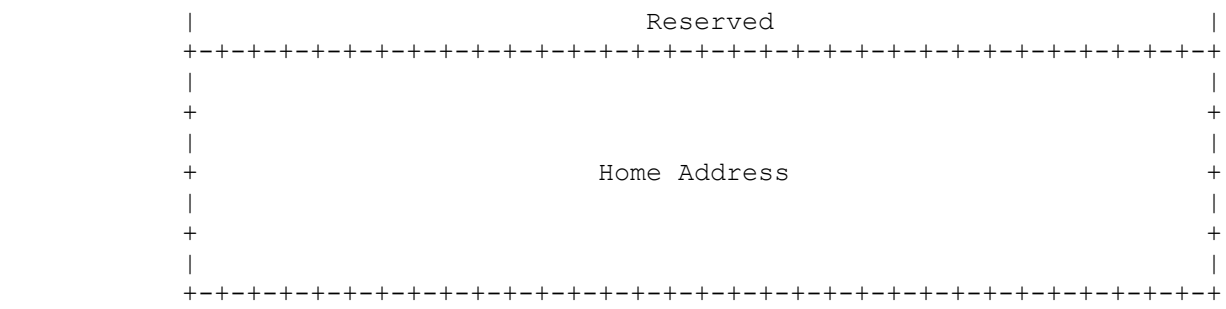
Чтобы позволить пакету маршрутизироваться непосредственно от узла-корреспондента на временный адрес мобильного узла, протокол мобильного IPv6 определяет новый вариант заголовка маршрутизации, заголовок маршрутизации типа 2. Временный адрес мобильного узла вставляется в поле Destination Address IPv6. Когда пакет прибывает на временный адрес, мобильный узел извлекает из заголовка маршрутизации свой домашний адрес, и этот адрес используется в качестве конечного адреса места назначения пакета.

Новый заголовок маршрутизации использует другой тип, отличный от определенного для «обычной» IPv6-маршрутизации от источника, позволяя межсетевым экранам применять к пакетам, маршрутизируемым от источника, другие правила по сравнению с пакетами мобильного IPv6. Этот тип заголовка маршрутизации (тип 2) ограничивается передачей только одного IPv6-адреса. Все узлы IPv6, которые обрабатывают этот заголовок маршрутизации, должны (MUST) проверить, что находящийся в нем адрес является собственным домашним адресом узла, чтобы не допустить пересылку пакетов за пределы узла. IP-адрес, находящийся в заголовке маршрутизации, должен (MUST) быть индивидуальным маршрутизируемым адресом, поскольку он является домашним адресом мобильного узла. Более того, если область действия домашнего адреса меньше, чем область действия временного адреса, то мобильный узел должен (MUST) отбросить пакет (см. разд. 4.6).

6.4.1. Формат

Заголовок маршрутизации типа 2 имеет следующий формат:





Next Header (следующий заголовок)

8-битовый селектор. Определяет тип заголовка, непосредственно следующего за заголовком маршрутизации. Использует те же самые значения, что и поле Next Header IPv6 [11].

Hdr Ext Len (длина заголовка расширения)

2 (8-битовое целое без знака); длина заголовка маршрутизации в единицах по 8 октетов, не включая первые 8 октетов.

Routing Type (тип маршрутизации)

2 (8-битовое целое без знака).

Segments Left (количество оставшихся сегментов)

1 (8-битовое целое без знака).

Reserved (зарезервировано)

32-битовое зарезервированное поле. Его значение должно (MUST) устанавливаться в ноль отправителем и должно (MUST) игнорироваться получателем.

Home Address (домашний адрес)

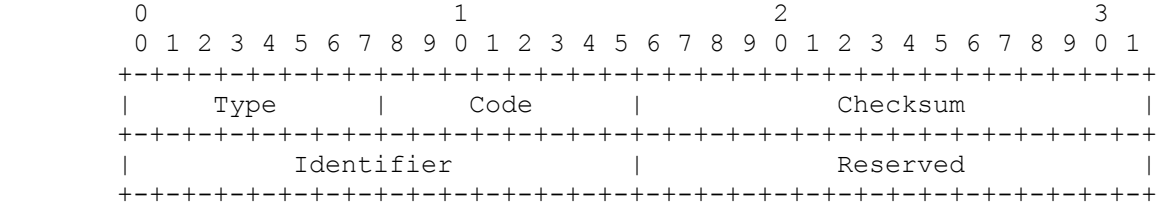
Домашний адрес мобильного узла назначения.

Для заголовка маршрутизации типа 2 значение Hdr Ext Len должно (MUST) быть равно 2. Значение Segments Left описывает количество оставшихся сегментов маршрута; т.е. количество явно перечисленных промежуточных узлов, которые еще должны быть посещены до достижения конечного места назначения. Значение Segments Left должно быть равно 1. Правила упорядочивания заголовков расширения в пакете IPv6 описываются в разд. 4.1 RFC 2460 [11]. Заголовок маршрутизации типа 2, определенный для протокола мобильного IPv6, следует тому же самому упорядочиванию, что и другие заголовки маршрутизации. Если (в пакете) присутствуют оба типа заголовков маршрутизации типа 0 и типа 2, то заголовок маршрутизации типа 2 должен следовать за другим заголовком маршрутизации. Пакет, содержащий такую вложенную инкапсуляцию, должен создаваться, как если бы внутренний заголовок маршрутизации (типа 2) был построен первым, а затем обрабатывался бы как первоначальный пакет процессом создания внешнего заголовка маршрутизации (типа 0).

Кроме того, общие процедуры, определенные IPv6 для заголовков маршрутизации, говорят о том, что принятый заголовок маршрутизации может (MAY) быть автоматически «перевернут» для создания заголовка маршрутизации для использования в любых ответных пакетах, посылаемых протоколами более высокого уровня, если полученный пакет аутентифицируется [6]. Для заголовков маршрутизации типа 2 это не должно (MUST NOT) делаться автоматически.

6.5. Сообщение ICMP Home Agent Address Discovery Request

Сообщение ICMP Home Agent Address Discovery Request (запрос для определения адреса домашнего агента) используется мобильным узлом для инициализации механизма динамического определения адреса домашнего агента, как описано в разд. 11.4.1. Мобильный узел посылает сообщение Home Agent Address Discovery Request на адрес «Mobile IPv6 Home-Agents anycast address» [16] для префикса своей собственной домашней подсети. (Заметим, что определенные в настоящее время адреса типа anycast не могут работать со всеми длинами префиксов, отличными от тех, которые определены в RFC 2373 [3, 35].)



Type (тип)

144

Code (код)

0

Checksum (контрольная сумма)

Контрольная сумма ICMP [14].

Identifier (идентификатор)

Идентификатор для поддержки сопоставления сообщений Home Agent Address Discovery Reply с данным сообщением Home Agent Address Discovery Request.

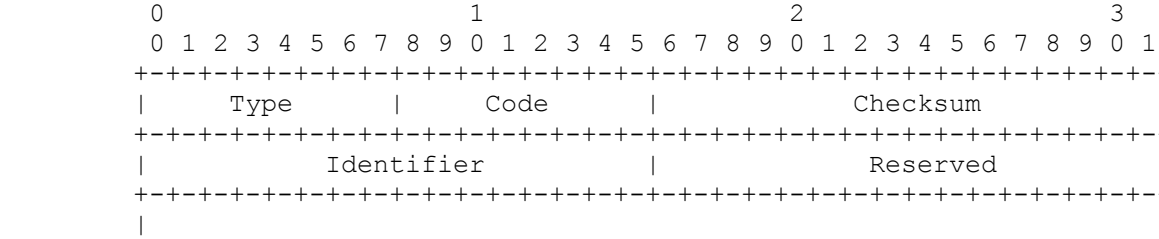
Reserved (зарезервировано)

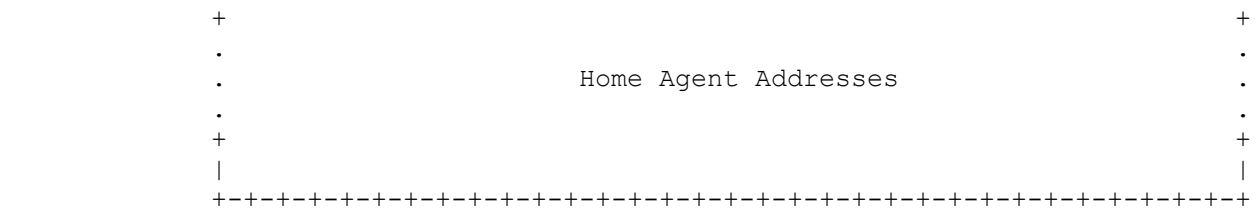
Это поле не используется. Оно должно (MUST) устанавливаться в ноль отправителем и должно (MUST) игнорироваться получателем.

Адресом источника сообщения Home Agent Address Discovery Request обычно является один из временных адресов мобильного узла. Во время выполнения этой процедуры динамического определения адреса домашнего агента, имеется вероятность того, что мобильный узел не зарегистрирован ни в одном домашнем агенте. Поэтому ни тип адреса, ни подлинность мобильного узла в это время не могут быть установлены. Тогда домашний агент должен (MUST) вернуть сообщение Home Agent Address Discovery Reply непосредственно на адрес источника, выбранный мобильным узлом.

6.6. Сообщение ICMP Home Agent Address Discovery Reply

Сообщение ICMP Home Agent Address Discovery Reply используется домашним агентом для ответа мобильному узлу, который использует механизм динамического определения адреса домашнего агента, как описано в разд. 10.5.





Type (тип)

145

Code (код)

0

Checksum (контрольная сумма)

Контрольная сумма ICMP [14].

Identifier (идентификатор)

Идентификатор из вызвавшего сообщения Home Agent Address Discovery Request.

Reserved (зарезервировано)

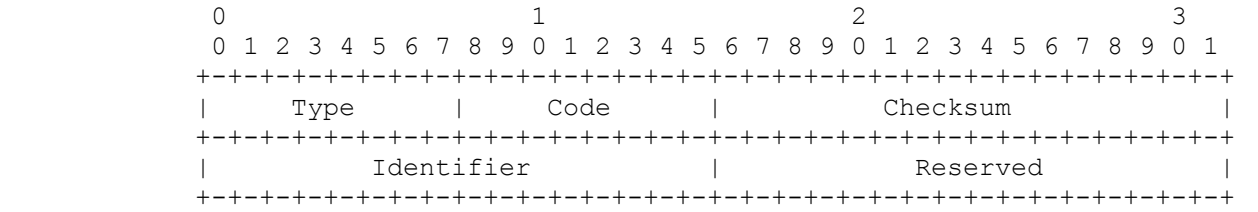
Это поле не используется. Оно должно (MUST) устанавливаться в ноль отправителем и должно (MUST) игнорироваться получателем.

Home Agent Addresses (адреса домашних агентов)

Список адресов домашних агентов мобильного узла на домашнем линке. Количество адресов, имеющихся в списке, указывается оставшейся длиной пакета IPv6, передающего сообщение Home Agent Address Discovery Reply.

6.7. Формат сообщения ICMP Mobile Prefix Solicitation

Сообщение ICMP Mobile Prefix Solicitation (запрос мобильного префикса) посылается мобильным узлом своему домашнему агенту, когда первый находится вне дома. Целью сообщения является запрос от домашнего агента сообщения Mobile Prefix Advertisement (объявление мобильного префикса), которое позволит мобильному узлу приобрести префиксную информацию относительно его домашней сети. Эта информация может использоваться для конфигурирования и обновления домашнего адреса (адресов) в соответствии с изменениями в префиксной информации, представленной домашним агентом.



Поля IP:

Source Address (адрес источника)

Временный адрес мобильного узла

Destination Address (адрес места назначения)

Адрес домашнего агента мобильного узла. Этот домашний агент должен быть на том линке, о котором мобильный узел хочет выяснить префиксную информацию.

Hop Limit (количество интервалов)

Подобно любому другому индивидуальному пакету, посылаемому мобильным узлом, устанавливается начальное значение количества интервалов.

Опция места назначения:

Опция места назначения Home Address должна (MUST) быть включена в пакет.

Заголовок ESP:

Заголовки IPsec должны (MUST) поддерживаться и должны (SHOULD) использоваться, как описано в разд. 5.4.

Поля ICMP:

Type (тип)

146

Code (код)

0

Checksum (контрольная сумма)

Контрольная сумма ICMP [14].

Identifier (идентификатор)

Идентификатор для поддержки сопоставления будущего сообщения Mobile Prefix Advertisement с данным сообщением Mobile Prefix Solicitation.

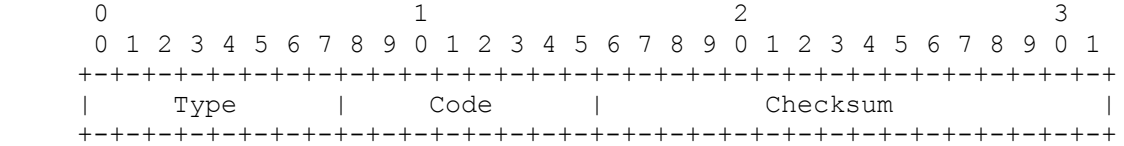
Reserved (зарезервировано)

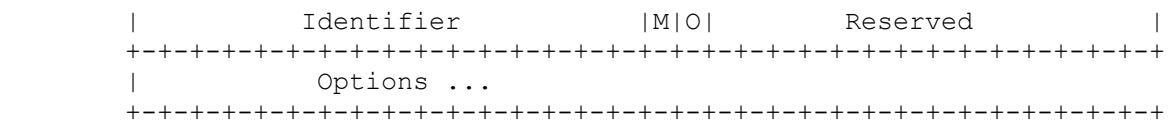
Это поле не используется. Оно должно (MUST) устанавливаться в ноль отправителем и должно (MUST) игнорироваться получателем.

Сообщения Mobile Prefix Solicitation могут иметь опции. Эти опции должны (MUST) использовать формат опций, определенный в RFC 2461 [12]. Данный документ не определяет ни одного типа опции для сообщения Mobile Prefix Solicitation, но будущие документы могут определить новые опции. Домашние агенты должны (MUST) молча игнорировать любые опции, которые они не распознают, и продолжать обработку сообщения.

6.8. Формат сообщения ICMP Mobile Prefix Advertisement

Пока мобильный узел перемещается вне домашней сети, домашний агент пошлет мобильному узлу сообщение Mobile Prefix Advertisement (объявление мобильного префикса) для распространения префиксной информации о домашнем линке. Это произойдет в виде объявления в ответ на запрос Mobile Prefix Solicitation, или в виде незапрошенного объявления, посылаемого в соответствии с правилами разд. 10.6.





Поля IP:

Source Address (адрес источника)

Адрес домашнего агента, поскольку мобильный узел предполагает его увидеть (т.е. тот же самый префикс сети).

Destination Address (адрес места назначения)

Если данное сообщение является ответом на сообщение Mobile Prefix Solicitation, то это поле содержит поле Source Address из того пакета. Для не запрошенных сообщений должен (SHOULD) использоваться временный адрес мобильного узла. Заметим, что незапрошенные сообщения могут посылаться, только если мобильный узел в настоящее время зарегистрирован в домашнем агенте.

Заголовок маршрутизации:

Заголовок маршрутизации типа 2 должен (MUST) быть включен (в пакет).

Заголовок ESP:

Заголовки IPsec должны (MUST) поддерживаться и должны (SHOULD) использоваться, как описано в разд. 5.4.

Поля ICMP:

Type (тип)

147

Code (код)

0

Checksum (контрольная сумма)

Контрольная сумма ICMP [14].

Identifier (идентификатор)

Идентификатор для поддержки сопоставления данного объявления Mobile Prefix Advertisement с предыдущим запросом Mobile Prefix Solicitation.

M

1-битовый флаг Managed Address Configuration (управляемое конфигурирование адресов). Если он установлен, хосты используют администрируемый (контекстный) протокол для автоконфигурирования адресов в дополнение ко всем адресам, автоматически сконфигурированным с помощью бесконтекстного автоконфигурирования адресов. Использование этого флага описано в [12, 13].

O

1-битовый флаг Other Stateful Configuration (другое контекстное конфигурирование). Если он установлен, то хосты используют администрируемый

(контекстный) протокол для автоконфигурирования другой (не адресной) информации. Использование этого флага описано в [12, 13].

Reserved (зарезервировано)

Это поле не используется. Оно должно (MUST) устанавливаться в ноль отправителем и должно (MUST) игнорироваться получателем.

Сообщения Mobile Prefix Advertisement могут иметь опции. Эти опции должны (MUST) использовать формат опций, определенный в RFC 2461 [12]. Данный документ не определяет ни одного типа опции для сообщения Mobile Prefix Advertisement, но будущие документы могут определить новые опции. Мобильные узлы должны (MUST) молча игнорировать любые опции, которые они не распознают, и продолжать обработку сообщения.

Prefix Information (префиксная информация)

Каждое сообщение содержит одну или несколько опций Prefix Information. Каждая опция передает префикс (префиксы), который мобильный узел должен использовать для конфигурирования своего домашнего адреса (домашних адресов). В разд. 10.6 описано, какие префиксы должны объявляться мобильному узлу.

Опция Prefix Information определена в разд. 4.6.2 RFC 2461 [12] с изменениями, определенными в разд. 7.2 настоящей спецификации. Домашний агент должен (MUST) использовать эту измененную опцию Prefix Information для посылки сетевых префиксов, как определено в разд. 10.6.1.

Если объявление посылается в ответ на запрос Mobile Prefix Solicitation, домашний агент должен (MUST) скопировать из этого сообщения значение поля Identifier в поле Identifier объявления.

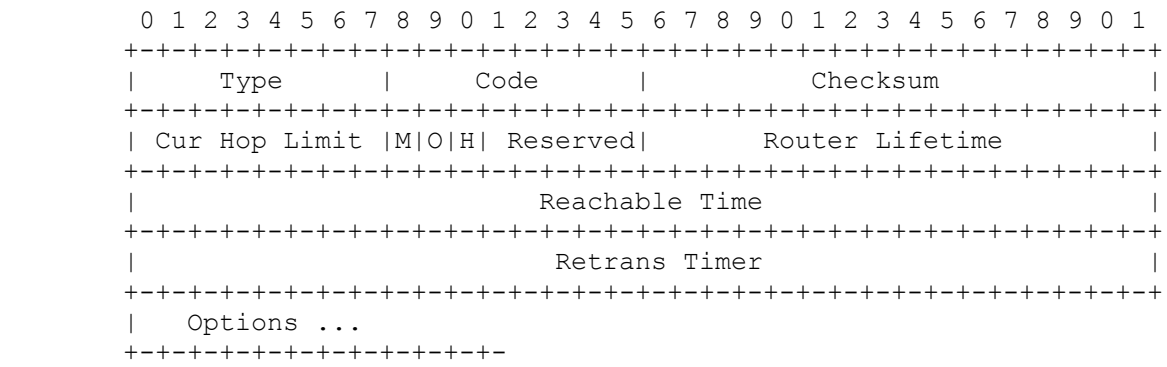
Домашний агент не должен (MUST NOT) посылать любому мобильному узлу более одного сообщения Mobile Prefix Advertisement в секунду.

Биты M и O должны быть (MUST) сброшены, если не обеспечивается поддержка домашнего агента DHCPv6. Если такая поддержка обеспечивается, то они устанавливаются во взаимодействии с административными установками домашней сети.

7. Изменения в протоколе IPv6 Neighbor Discovery

7.1. Модифицированный формат сообщения Router Advertisement

Протокол мобильного IPv6 изменяет формат сообщения Router Advertisement (объявление маршрутизатора) [12] путем добавления одного флагового бита для указания того, что маршрутизатор, посылающий сообщение-объявление служит домашним агентом на данном линке. Сообщение Router Advertisement имеет следующий формат:



Этот формат выражает следующие изменения по сравнению с форматом, первоначально специфицированном для протокола Neighbor Discovery [12]:

Home Agent (H) (домашний агент)

> Бит Home Agent (H) устанавливается в сообщении Router Advertisement для указания того, что маршрутизатор, посылающий это сообщение, функционирует также как домашний агент протокола мобильного IPv6 на данном линке.

Reserved (зарезервировано)

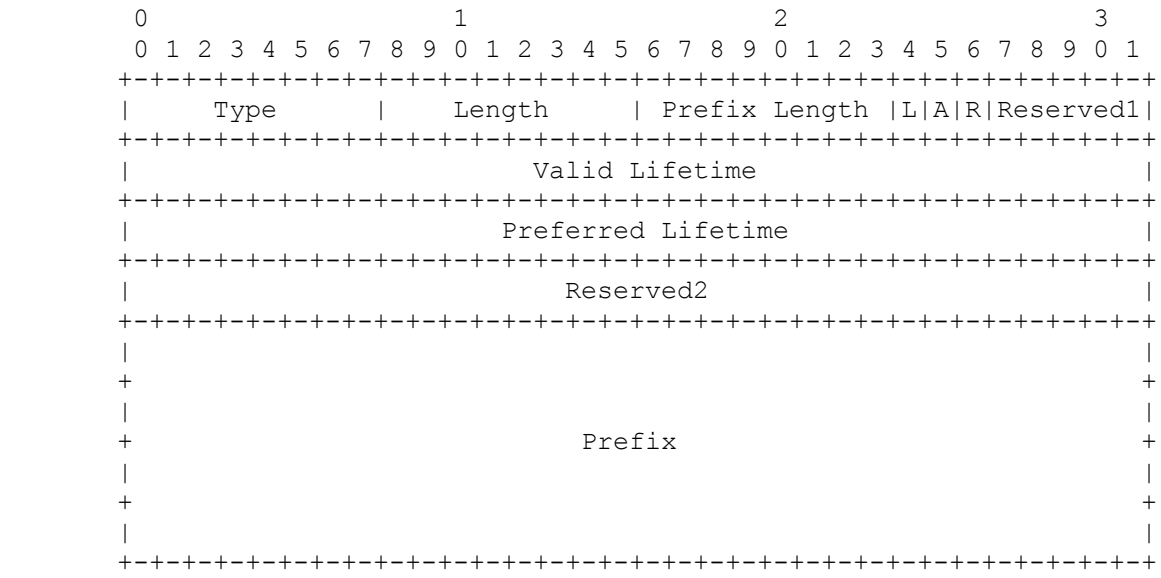
> Сокращенное с 6 до 5 бит поле, чтобы учесть добавление указанного выше бита.

7.2. Модифицированный формат опции Prefix Information

Протокол мобильного IPv6 требует знания глобального адреса маршрутизатора при построении списка домашних агентов как части механизма динамического определения адресов домашних агентов.

Однако протокол Neighbor Discovery [12] объявляет только «локальный для линка» адрес мршрутизатора, требуя использовать этот адрес в качестве адреса источника IP в каждом сообщении Router Advertisement.

Протокол мобильного IPv6 расширяет протокол Neighbor Discovery для того, чтобы позволить маршрутизатору объявить свой глобальный адрес путем добавления в формат опции Prefix Information (префиксная информация) одного флагового бита для использования в сообщениях Router Advertisement. Опция Prefix Information имеет следующий формат:



Этот формат выражает следующие изменения по сравнению с форматом, первоначально специфицированным для протокола Neighbor Discovery [12]:

Router Address (R) (адрес маршрутизатора)

1-битовый флаг «адрес маршрутизатора». Если установлен, указывает на то, что поле Prefix содержит полный IP-адрес, присвоенный посылающему маршрутизатору. Указанный префикс представляет собой первые биты поля Prefix, определяемые полем Prefix Length. IP-адрес маршрутизатора имеет ту же самую область действия и подчиняется тем же самым значениям времени жизни, что и объявляемый префикс. Такое использование поля Prefix соответствует его использованию при объявлении самого префикса, поскольку объявление префикса использует только первые биты. Таким образом, интерпретация этого флагового бита не зависит от обработки, которая требуется для обработки флаговых битов On-Link (L) и Autonomous Address-Configuration (A).

Reserved1 (зарезервировано1)

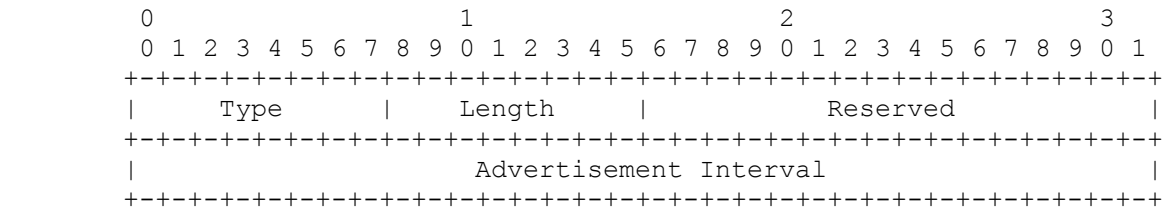
Сокращенное с 6 до 5 бит поле, чтобы учесть добавление указанного выше бита.

В объявление маршрутизатора домашний агент должен (MUST), а все другие маршрутизаторы могут (MAY), включить, по крайней мере, одну опцию Prefix Information с установленным флаговым битом Router Address (R). Протокол Neighbor Discovery определяет, что если включение в сообщение Router Advertisement всех опций увеличивает размер объявления так, что он превышает MTU линка, то могут посылаться несколько объявлений, каждое из которых содержит подмножество опций [12]. Кроме того, если не запрошенные групповые сообщения Router Advertisement посылаются чаще, чем определенное в RFC 2461 [12] предельное значение, то посылающий маршрутизатор не обязан включать в каждое такое объявление все опции. Однако в обоих этих случаях маршрутизатор должен (SHOULD) включить в каждое такое объявление, по крайней мере, одну опцию Prefix Information с установленным битом Router Address (R), если этот бит устанавливается в каком-либо объявлении, посылаемом маршрутизатором.

Кроме того, следующее требование может помочь мобильным узлам при определении перемещений. Кроме изменений префиксов на линке, маршрутизаторы, которые посылают несколько объявлений Router Advertisement с установленным в некоторых включенных опциях Prefix Information битом Router Address (R), должны (SHOULD) представить по крайней мере одну опцию и адрес маршрутизатора, который остается тем же самым во всех объявлениях.

7.3. Формат новой опции Advertisement Interval

Протокол мобильного IPv6 определяет новую опцию Advertisement Interval (период обновлений), которая используется в сообщениях Router Advertisement для объявления периода, с которым посылающий маршрутизатор посылает незапрошенные групповые объявления. Опция Advertisement Interval имеет следующий формат:



Type (тип)

7

Length (длина)

8-битовое целое без знака. Длина опции (включая поля Type и Length) в единицах по 8 октетов. Значение этого поля должно (MUST) быть равно 1.

Reserved (зарезервировано)

Это поле не используется. Оно должно (MUST) инициализироваться в ноль отправителем и должно (MUST) игнорироваться получателем.

Advertisement Interval (период объявлений)

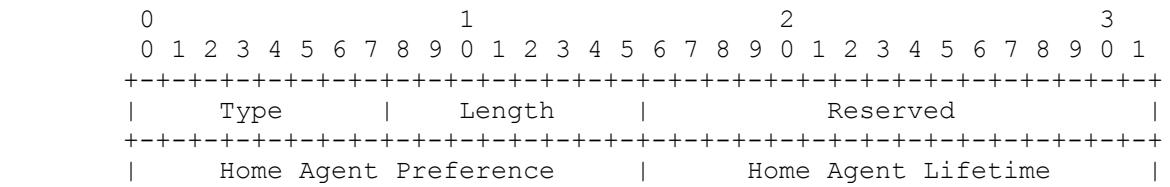
32-битовое целое без знака. Максимальное время в миллисекундах между последовательными незапрошенными сообщениями Router Advertisement, посылаемыми данным маршрутизатором по данному сетевому интерфейсу. Используя концептуальные переменные конфигурирования маршрутизатора, определенные в протоколе Neighbor Discovery [12], это поле должно (MUST) быть равно значению MaxRtrAdvInterval, выраженому в миллисекундах.

Маршрутизаторы могут (MAY) включать эту опцию в свои сообщения Router Advertisement. Мобильный узел, получающий объявление маршрутизатора, содержащее эту опцию, должен (SHOULD) использовать определенный для этого маршрутизатора период объявлений в своем алгоритме определения перемещений, как описано в разд. 11.5.1.

Эта опция должна (MUST) молча игнорироваться для других сообщений протокола Neighbor Discovery.

7.4. Формат новой опции Home Agent Information

Протокол мобильного IPv6 определяет новую опцию Home Agent Information (информация домашнего агента), которая используется в объявлениях маршрутизатора, посылаемых домашним агентом для объявления информации, специфической для функционирования данного маршрутизатора в качестве домашнего агента.



Type (тип)

8

Length (длина)

8-битовое целое без знака. Длина опции (включая поля Type и Length) в единицах по 8 октетов. Значение этого поля должно (MUST) быть равно 1.

Reserved (зарезервировано)

Это поле не используется. Оно должно (MUST) инициализироваться в ноль отправителем и должно (MUST) игнорироваться получателем.

Home Agent Preference (приоритет домашнего агента)

16-битовое целое без знака. Приоритет домашнего агента, посылающего данное объявление маршрутизатора, для использования в упорядочивании адресов, возвращаемых мобильному узлу в поле Home Agent Addresses сообщения Home Agent Address Discovery Reply. Большие значения означают больший приоритет. Если эта опция не включается в объявление маршрутизатора, в котором установлен бит Home Agent (H), то значение приоритета для этого домашнего агента должно (MUST) рассматриваться как нулевое. Большие значения указывают более приоритетного домашнего агента, чем меньшие значения.

Ручное конфигурирование значения Home Agent Preference описывается в разд. 8.4. Кроме того, посылающий домашний агент может (MAY) динамически устанавливать это значение, например, базируясь на количестве мобильных узлов, которые он в текущий момент времени обслуживает, или на своих ресурсах, оставшихся для обслуживания дополнительных мобильных узлов; подобные динамические установки выходят за рамки данного документа. Однако любая подобная динамическая установка приоритета домашнего агента должна (MUST) устанавливать приоритет соответствующе, относительно подразумеваемого нулевого значения приоритета домашнего агента, который может использоваться некоторыми домашними агентами на данном линке (т.е. домашний агент, не включающий опцию Home Agent Information в свои объявления маршрутизатора, будет рассматриваться как имеющий нулевое значение приоритета).

Home Agent Lifetime (время жизни домашнего агента)

16-битовое целое без знака. Время жизни в секундах, связанное с домашним агентом. Подразумеваемое значение совпадает со значением Router Lifetime, как определено в основном теле сообщения Router Advertisement. Максимальное время соответствует 18.2 часа. Нулевое значение не должно (MUST NOT) использоваться. Время жизни домашнего агента применяется только в контексте пригодности данного маршрутизатора для работы в качестве домашнего агента; оно не применяется к информации, содержащейся в других полях сообщения или опций.

Домашние агенты могут (MAY) включать эту опцию в свои объявления маршрутизатора. Данная опция не должна (MUST NOT) включаться в объявление маршрутизатора, в котором не установлен бит Home Agent (H) (см. разд. 7.1). Если данная опция не включена в объявление маршрутизатора, в котором бит Home Agent (H) установлен, то время жизни для данного домашнего агента должно (MUST) рассматриваться равным времени жизни маршрутизатора в объявлении маршрутизатора. Если вместо одного незапрошенного группового объявления большего размера посылается несколько объявлений, то эти все множественные объявления с установленным битом Router Address (R) должны (MUST) включать эту опцию с одним и тем же содержимым, в противном случае эта опция должна (MUST) опускаться во всех объявлениях.

Данная опция должна (MUST) молча игнорироваться для других сообщений протокола Neighbor Discovery.

Если приоритет домашнего агента и время жизни домашнего агента устанавливаются равными указанным выше подразумеваемым значениям, то эта опция не должна (SHOULD NOT) включаться в сообщения Router Advertisement, посылаемые данным домашним агентом.

7.5. Изменения в посылке сообщений Router Advertisement

Спецификация протокола Neighbor Discovery [12] ограничивает маршрутизаторы минимальным периодом в 3 секунды между посылками незапрошенных групповых сообщений Router Advertisement с любого заданного интерфейса (ограничивается значениями MinRtrAdvInterval и MaxRtrAdvInterval), устанавливая, что:

> «Маршрутизаторы формируют объявления маршрутизатора достаточно часто, чтобы хосты узнали об их присутствии в течение нескольких минут, но не настолько часто, чтобы полагаться на отсутствие объявлений для определения неисправности маршрутизатора; определение неисправности обеспечивает отдельный алгоритм Neighbor Unreachability Detection (алгоритм определения недостижимости соседей)».

Однако это ограничение не применимо для обеспечения периодического определения перемещений мобильными узлами. Мобильные узлы определяют свое собственное перемещение путем узнавания о наличии новых маршрутизаторов, как, например, мобильный узел перемещается в диапазоне передачи беспроводной сети (или физически подключается к новой проводной сети), и путем узнавания того, что предыдущие маршрутизаторы больше не достижимы. Мобильные узлы должны (MUST) быть способными быстро определить свое перемещение на линк, который обслуживается другим маршрутизатором так, чтобы они могли получить новый временный адрес и послать обновления привязки для регистрации этого временного адреса у своего домашнего агента и подобающим образом известить узлы-корреспонденты.

Один из методов, который может обеспечить быстрое определение перемещений, заключается в том, чтобы увеличить скорость посылки незапрошенных объявлений маршрутизатора. Протокол мобильного IPv6 смягчает это ограничение так, чтобы маршрутизаторы могли (MAY) чаще посылать незапрошенные групповые объявления. Этот метод может применяться там, где предполагается предоставление маршрутизатором услуг посещающим мобильным узлам (т.е. беспроводные сетевые интерфейсы), или там, где он служит домашним агентом одному или нескольким мобильным узлам (которые могут вернуться домой и должны услышать его объявления).

Машрутизаторы, поддерживающие мобильность, должны (SHOULD) иметь возможность конфигурирования с меньшими значениями MinRtrAdvInterval и MaxRtrAdvInterval, чтобы разрешить более частую посылку незапрошенных групповых объявлений. Допустимыми минимальными значениями являются:

- MinRtrAdvInterval 0.03 секунды
- MaxRtrAdvInterval 0.07 секунды

В случае, когда используются минимальные периоды и задержки, среднее время между незапрошенными групповыми объявлениями маршрутизатора составляют 50 мсек. Использование этих модифицированных ограничений должно быть (MUST) конфигурируемым (см. также переменную конфигурирования MinDelayBetweenRas в разд. 13, которая, возможно, также должна быть соответствующим образом изменена). Системы, в которых эти значения доступны, не должны (MUST NOT) по умолчанию переходить на них, а должны (SHOULD) по умолчанию использовать значения, определенные в RFC 2461. Для каждого сетевого интерфейса при конфигурировании этих ограничений должны (SHOULD) приниматься во внимание знания типа сетевого интерфейса и операционной среды. Это важно для некоторых

беспроводных линков, в которых увеличение частоты групповых сигналов может приводить к значительным накладным расходам. Маршрутизаторы должны (SHOULD) придерживаться периодов, определенных в RFC 2461 [12], если эти накладные расходы могут привести к деградации услуг.

Дополнительно, возможные малые значения MaxRtrAdvInterval могут в некоторых мобильных узлах создавать некоторые проблемы с определением перемещений. Чтобы гарантировать, что это не проблема, маршрутизаторы должны (SHOULD) добавлять 20 миллисекунд к любым периодам объявлений, посылаемых в объявлениях маршрутизатора, которые имеют значение менее 200 миллисекунд, чтобы учесть дисперсность планирования как на мобильном узле, так и на маршрутизаторе.

Заметим, что групповые объявления маршрутизатора в конкретных беспроводных сетях с ограниченной пропускной способностью требуются не всегда. Определение мобильности или изменения линка в таких сетях может быть сделано на более низких уровнях. Объявления маршрутизатора в таких сетях должны (SHOULD) посылаться только в случае запроса. В таких сетях должна (SHOULD) существовать возможность запрещения выдачи незапрошенных групповых объявлений маршрутизатора на конкретных интерфейсах. В этом случае значения MinRtrAdvInterval и MaxRtrAdvInterval могут быть установлены достаточно большими.

Домашние агенты должны (MUST) включать опцию Source Link-Layer Address во все объявления маршрутизатора, которые они посылают. Это упрощает процесс возвращения домой, как обсуждается в разд. 11.5.4.

Заметим, что в соответствии с RFC 2461 [12], по умолчанию значение AdvDefaultLifetime базируется на значении MaxRtrAdvInterval. Значение AdvDefaultLifetime используется в поле Router Lifetime объявлений маршрутизатора. Поскольку значение этого поля выражается в секундах, малое значение MaxRtrAdvInterval может привести к нулевому значению этого поля. Чтобы этого избежать, маршрутизаторы должны (SHOULD) сохранять значение AdvDefaultLifetime равным по крайней мере одной секунде, даже если использование значения MaxRtrAdvInterval приведет к меньшему значению.

8. Требования, предъявляемые к различным типам узлов IPv6

Протокол мобильного IPv6 предъявляет некоторые специальные требования к функциям, предоставляемым различными типами узлов IPv6. В этом разделе эти требования суммируются, и определяется функциональность, которая подразумевается необходимой для поддержки каждого требования.

Требования устанавливаются для следующих групп узлов:

- Все узлы IPv6.
- Все узлы IPv6 с поддержкой оптимизации маршрутов.
- Все маршрутизаторы IPv6.
- Все домашние агенты мобильного IPv6.
- Все мобильные узлы мобильного IPv6.

Определение того, какие из этих групп являются обязательными в IPv6, выходит за рамки настоящей спецификации. Мы описываем только то, что является обязательным для узла, который поддерживает, например, оптимизацию маршрутов. Предполагается, что рамки IPv6 должны определять другие спецификации.

8.1. Все узлы IPv6

Любой узел IPv6 может в любой момент времени быть узлом-корреспондентом мобильного узла либо посылая пакет мобильному узлу, либо принимая от него пакет. Для таких узлов отсутствуют специфические для мобильного IPv6 требования типа «MUST», и базовые средства IPv6 являются достаточными. Если мобильный узел пытается установить оптимизацию маршрута с узлом, реализующим только базовую поддержку, то сообщение об ошибке ICMP просигнализирует, что этот узел не поддерживает такую оптимизацию (разд. 11.3.5), и обмен информацией будет идти через домашнего агента.

Узел IPv6 не должен (MUST NOT) поддерживать опцию места назначения Home Address, заголовок маршрутизации типа 2 или заголовок мобильности (Mobility Header), если он полностью не поддерживает перечисленных в следующих разделах требований необходимой функциональности либо для оптимизации маршрутов, либо для мобильного узла, либо для домашнего агента.

8.2. Узлы IPv6 с поддержкой оптимизации маршрутов

Узлы, реализующие оптимизацию маршрутов, являются подмножеством всех узлов IPv6 в Internet. Способность узла-корреспондента участвовать в процессе оптимизации маршрутов является существенной для эффективной работы IPv6 Internet по следующим причинам:

- Предотвращение перегрузки в домашней сети и возможность использования в качестве домашнего агента оборудования меньшей производительности даже для поддержки тысяч мобильных узлов.
- Уменьшенная нагрузка на всю сеть Internet, поскольку мобильные устройства начинают в ней преобладать.
- Сокращение разброса и задержки обмена информацией.
- Повышенная вероятность успешной сигнализации QoS, поскольку исключается туннелирование и, повторим, уменьшается количество источников перегрузки.

- Повышенная устойчивость к расчленению сети, перегрузке и другим проблемам, поскольку по пути маршрута проходится меньшее количество сегментов.

Эти результаты объединяются и обеспечивают гораздо лучшую производительность и надежность обменов информацией между мобильными узлами и узлами-корреспондентами IPv6. Оптимизация маршрутов приводит к необходимости сохранения партнерами небольшого объема дополнительной информации о состоянии, некоторому дополнительному обмену сообщениями и к полуторным задержкам туда и обратно до того, как она может быть введена в действие. Однако имеется уверенность в том, что общий полезный результат в большинстве случаев намного перевесит издержки. В разд. 11.3.1 обсуждается вопрос о том, как мобильные узлы могут избежать оптимизации маршрутов в некоторых оставшихся ситуациях таких, например, как очень краткосрочные обмены информацией.

Следующие требования применяются ко всем узлам-корреспондентам, которые поддерживают оптимизацию маршрутов:

- Узел должен быть способным (MUST) признать действительной опцию Home Address используя существующий элемент кэша привязок, как описано в разд. 9.3.1.

- Узел должен быть способным (MUST) вставлять в пакеты, которые должны посылаться мобильному узлу, заголовок маршрутизации типа 2, как описано в разд. 9.3.2.

- Узел-корреспондент должен (MUST) игнорировать заголовки маршрутизации типа 2 и молча отбрасывать все пакеты, которые он получил с такими заголовками, если только он сам не действует как мобильный узел.

- Узел должен быть способным (SHOULD) интерпретировать сообщения ICMP, как описано в разд. 9.3.4.

- Узел должен быть способным (MUST) посылать сообщения Binding Error, как описано в разд. 9.3.3.

- Узел должен быть способным (MUST) обрабатывать заголовки мобильности, как описано в разд. 9.2.

- Узел должен быть способным (MUST) участвовать в процедуре обратной маршрутизируемости (разд. 9.4).

- Узел должен быть способным (MUST) обрабатывать сообщения Binding Update (разд. 9.5).

- Узел должен быть способным (MUST) возвращать сообщения Binding Acknowledgement (разд. 9.5.4).

- Узел должен быть способным (MUST) поддерживать кэш привязок для привязок, полученных в признанных годными сообщениях Binding Update, как описано в разд. 9.1 и 9.6.

- Узел должен (SHOULD) позволять административно разрешать и запрещать оптимизацию маршрутов. По умолчанию такая оптимизация должна быть (SHOULD) разрешена.

8.3. Все маршрутизаторы IPv6

Все маршрутизаторы IPv6, даже те, которые не работают в качестве домашних агентов для мобильного IPv6, влияют на то, насколько хорошо мобильные узлы могут обмениваться информацией:

- Каждый маршрутизатор IPv6 должен быть (SHOULD) способным посылать опцию Advertisement Interval (разд. 7.3) в каждом своем сообщении Router Advertisement [12], чтобы поддержать алгоритм определения перемещения мобильными узлами (как описано в разд. 11.5.1). Использование этой опции в сообщениях Router Advertisement должно быть (SHOULD) конфигурируемым.

- Каждый маршрутизатор IPv6 должен быть (SHOULD) способным поддерживать посылку не запрошенных групповых (multicast) сообщений Router Advertisement с повышенной скоростью, описанной в разд. 7.5. Если маршрутизатор поддерживает повышенную скорость, используемая скорость должна быть (MUST) конфигурируемой.

- Каждый маршрутизатор IPv6 должен (SHOULD) включать в свои сообщения Router Advertisement, по крайней мере, один префикс с установленным битом Router Address (R) и со своим полным IP-адресом (как описано в разд. 7.2).

- Маршрутизаторы, поддерживающие фильтрацию пакетов с заголовками маршрутизации, должны (SHOULD) поддерживать различные правила для заголовков маршрутизации типа 0 и типа 2 (см. разд. 6.4) так, чтобы фильтрация маршрутизируемых от источника пакетов (тип 0) не обязательно приводила к ограничению трафика мобильного IPv6, который доставляется с помощью заголовков маршрутизации типа 2.

8.4. Домашние агенты IPv6

Для того чтобы мобильный узел, находясь вне дома, работал правильно, по крайней мере, один маршрутизатор IPv6 на домашнем линке мобильного узла должен функционировать как его домашний агент. Следующие дополнительные правила применяются ко всем маршрутизаторам IPv6, которые служат в качестве домашних агентов:

- Каждый домашний агент должен быть способным (MUST) поддерживать в своем кэше привязок элемент для каждого мобильного узла, для которого он служит домашним агентом (разд. 10.1 и 10.3.1).

- Каждый домашний агент (с помощью агента-посредника proxy Neighbor Discovery [12]) должен быть способным (MUST) перехватывать на домашнем линке пакеты, адресованные мобильному узлу, для которого в текущий момент времени он служит домашним агентом, в то время, когда мобильный узел находится вне дома (разд. 10.4.1).

- Каждый домашний агент должен быть способным (MUST) инкапсулировать [15] эти перехваченные пакеты, чтобы туннелировать их на основной временный адрес мобильного узла, указанный в его привязке, хранящейся в кэше привязок домашнего агента (разд. 10.4.2).

- Каждый домашний агент должен (MUST) поддерживать декапсуляцию [15] туннелируемых в обратном направлении пакетов, посланных ему с домашнего адреса мобильного узла. Каждый домашний агент должен (MUST) также проверять, что адрес источника в туннелируемых пакетах соответствует зарегистрированному в текущий момент времени местоположению мобильного узла (разд. 10.4.5).

- Узел должен быть способным (MUST) обрабатывать заголовки мобильности, как описано в разд. 10.2.

- Каждый домашний агент должен быть способным (MUST) возвращать сообщение Binding Acknowledgement в ответ на сообщение Binding Update (разд. 10.3.1).

- Каждый домашний агент должен (MUST) поддерживать отдельный список домашних агентов для каждого линка, на котором он служит в качестве домашнего агента, как описано в разд. 10.1 и 10.5.1.

- Каждый домашний агент должен быть способным (MUST) принимать пакеты, адресованные на адрес типа «Mobile IPv6 Home-Agents anycast address» [16] для подсети, на которой он служит в качестве домашнего агента, и должен быть способным (MUST) участвовать в процессе динамического определения адреса домашнего агента (разд. 10.5).

- Каждый домашний агент должен (SHOULD) поддерживать механизм конфигурирования, чтобы позволить системному администратору вручную установить значение, которое должно посылаться этим домашним агентом в поле Home Agent Preference опции Home Agent Information Option в сообщениях Router Advertisement, которые он посылает (разд. 7.4).

- Каждый домашний агент должен (SHOULD) поддерживать посылку сообщений ICMP Mobile Prefix Advertisement (разд. 6.8), и должен (SHOULD) отвечать на сообщения Mobile Prefix Solicitation (разд. 6.7). Если такая поддержка обеспечивается, то поведение домашнего агента должно быть (MUST) конфигурируемым так, чтобы в соответствии с потребностями администрирования сети в домашнем домене была возможность избежать посылки таких сообщений Prefix Advertisement.

- Каждый домашний агент должен (MUST) поддерживать IPsec ESP для защиты пакетов, являющихся частью процедуры обратной маршрутизируемости (разд. 10.4.6).

- Каждый домашний агент должен (SHOULD) поддерживать протоколы управления участием в мультикастовых группах, как описано в разд. 10.4.3. Если такая поддержка обеспечивается, то домашний агент должен быть способным (MUST) использовать ее для определения того, какие групповые пакеты данных пересылать через туннель мобильному узлу.

- Домашние агенты могут (MAY) поддерживать контекстное автоконфигурирование адресов для мобильных узлов, как описано в разд. 10.4.4.

8.5. Мобильные узлы IPv6

Наконец, следующие требования предъявляются ко всем узлам IPv6, способным функционировать в качестве мобильных узлов:

- Узел должен (MUST) поддерживать список обновлений привязок (разд. 11.1).

- Узел должен (MUST) поддерживать посылку пакетов, содержащих опцию Home Address (разд. 11.3.1), и следовать требуемым взаимодействиям IPsec (разд. 11.3.2).

- Узел должен быть способным (MUST) выполнять IPv6-инкапсуляцию и IPv6-декапсуляцию [15].

- Узел должен быть способным (MUST) обрабатывать заголовок маршрутизации типа 2, как определено в разд. 6.4 и 11.3.3.

- Узел должен (MUST) поддерживать прием сообщения Binding Error (разд. 11.3.6).

- Узел должен (MUST) поддерживать прием сообщений об ошибках ICMP (разд.1.3.5).

- Узел должен (MUST) поддерживать алгоритм определения перемещений, механизмы формирования временного адреса и возвращения домой (11.5).

- Узел должен быть способным (MUST) обрабатывать заголовки маршрутизации, как описано в разд. 11.2.

- Узел должен (MUST) поддерживать процедуру обратной маршрутизируемости (разд. 11.6).

- Узел должен быть способным (MUST) посылать сообщения Binding Update, как специфицировано в разд. 11.7.1 и 11.7.2.

- Узел должен быть способным (MUST) принимать и обрабатывать сообщения Binding Acknowledgement, как определено в разд. 11.7.3.

- Узел должен (MUST) поддерживать прием сообщения Binding Refresh Request (разд. 6.1.2), и отвечать сообщением Binding Update.

- Узел должен (MUST) поддерживать прием сообщений Mobile Prefix Advertisement (разд. 11.4.3) и реконфигурировать свой домашний адрес в соответствии с содержащейся в них префиксной информацией.

- Узел должен (SHOULD) поддерживать использование механизма динамического определения адреса домашнего агента, как описано в разд. 11.4.1.

- Узел должен (MUST) допускать административное разрешение и запрещение динамической оптимизации маршрутов. По умолчанию она должна быть (SHOULD) разрешена.

- Узел может (MAY) поддерживать «часть слушателя группового адреса» протокола управления членством в мультикастовой группе, как описано в разд. 11.3.4. Если такая поддержка обеспечивается, мобильный узел должен (MUST) быть способным получать туннелируемые групповые пакеты от домашнего агента.

- Узел может (MAY) поддерживать механизмы контекстного автоконфигурирования адресов, такие как DHCPv6 [29], на интерфейсе, представляемым туннелем к домашнему агенту.

9. Работа узла-корреспондента

9.1. Концептуальные структуры данных

Узлы IPv6 с поддержкой оптимизации маршрутов содержат кэш привязок (Binding Cache) для других узлов. Каждым узлом IPv6 для каждого из его индивидуальных маршрутизируемых адресов должен (SHOULD) поддерживаться отдельный кэш привязок. Кэш привязок может быть (MAY) реализован любым способом, согласующимся с внешним поведением, описанным в данном документе, например, объединенным с кэшем мест назначения узла (Destination Cache), который поддерживается протоколом Neighbor Discovery [12]. При посылке пакета поиск в кэше привязок осуществляется до поиска в концептуальном кэше мест назначения Neighbor Discovery [12].

Концептуально каждый элемент кэша привязок содержит следующие поля:

- Домашний адрес мобильного узла, для которого создается элемент кэша привязок. Это поле используется в качестве ключа для поиска в кэше привязок адреса места назначения посылаемого пакета.

- Временный адрес для мобильного узла, указанного полем домашнего адреса в данном элементе кэша привязок.

- Значение времени жизни, указывающее оставшееся время жизни данного элемента кэша привязок. Значение времени жизни инициализируется из поля Lifetime в сообщении Binding Update, которое создало или в последний раз модифицировало этот элемент кэша привязок.

- Флаг, указывающий является или не является этот элемент кэша привязок элементом регистрации в домашнем агенте (применим только в узлах, которые поддерживают функциональность домашнего агента).

- Максимальное значение поля Sequence Number, полученного в предыдущих сообщениях Binding Update для этого домашнего адреса. Поле Sequence Number имеет длину 16 бит. Значения Sequence Number должны (MUST) сравниваться по модулю 2**16, как объяснено в разд. 9.5.1.

- Информация об использовании данного элемента кэша привязок. Она требуется для реализации применяемой политики замещения в кэше привязок. Недавнее использование элемента кэша служит также в качестве указания того, что должно быть послано сообщение Binding Refresh Request, когда время жизни этого элемента приближается к исчерпанию.

Элементы кэша привязок, не помеченные признаком регистрации в домашнем агенте, в любой момент времени могут (MAY) быть замещены с использованием любой подходящей политики замещения локального кэша, но не обязательно должны (SHOULD NOT) удаляться. Кэш привязок для любого из адресов узла может содержать не более одного элемента для каждого домашнего адреса мобильного узла. Содержимое кэша привязок не должно (MUST NOT) меняться в ответ на опцию Home Address в полученном пакете.

9.2. Обработка заголовков мобильности

При обработке заголовков мобильности должны (MUST) соблюдать следующие правила:

- Контрольная сумма должна быть подтверждена, как указано в разд. 6.1. В противном случае узел должен (MUST) молча отбросить сообщение.

- Поле MH Type должно (MUST) иметь известное значение (разд. 6.1.1). В противном случае узел должен (MUST) отбросить сообщение и выдать сообщение Binding Error, как описано в разд. 9.3.3, с полем Status, установленным в значение 2 (unrecognized MH Type value).

- Поле Payload Proto должно (MUST) быть равным IPPROTO_NONE (59 десятичное). В противном случае узел должен (MUST) отбросить сообщение и должен (SHOULD) послать сообщение ICMP Parameter Problem, Code 0, непосредственно на адрес источника (Source Address) пакета, как описано в RFC 2463 [14]. Таким образом, при посылке сообщения ICMP никакая информация из кэша привязок не используется. Поле Pointer в сообщении ICMP должно (SHOULD) указывать на поле Payload Proto.

- Поле Header Len в заголовке мобильности не должно (MUST NOT) быть меньше, чем длина, специфицированная для данного конкретного типа сообщения в разд. 6.1. В противном случае узел должен (MUST) отбросить сообщение и должен (SHOULD) послать сообщение ICMP Parameter Problem, Code 0, непосредственно на адрес источника (Source Address) пакета, как описано в RFC 2463 [14]. (Информация из кэша привязок снова не используется). Поле Pointer в сообщении ICMP должно (SHOULD) указывать на поле Header Len.

  Последующие проверки зависят от конкретного заголовка мобильности.

9.3. Обработка пакетов

В данном разделе описано, как узел-корреспондент посылает пакеты мобильному узлу и принимает от него пакеты.

9.3.1. Прием пакетов с опцией Home Address

Пакеты, содержащие опцию Home Address должны (MUST) отбрасываться, если данный домашний адрес не является индивидуальным маршрутизируемым адресом.

Мобильные узлы могут включать в пакет опцию места наазначения Home Address, если они уверены в том, что узел-корреспрондент имеет элемент кэша привязок для домашнего адреса мобильного узла. Пакеты, содержащие опцию Home Address должны (MUST) отбрасываться, если отсутствует соответствующий элемент в кэше привязок. Соответствующий элемент в кэше привязок должен (MUST) иметь тот же самый домашний адрес, который появляется в опции места назначения Home Address, а зарегистрированный в текущий момент времени временный адрес должен (MUST) быть равен адресу источника пакета. Эти проверки не должны (MUST NOT) выполняться для пакетов, которые содержат опцию Home Address и сообщение Binding Update.

Если пакет отброшен по причине указанных выше проверок, узел-корреспондент должен (MUST) послать сообщение Binding Error, как описано в разд. 9.3.3. Поле Status в этом сообщении должно быть установлено в 1 (unknown binding for Home Address destination option).

Узел-корреспондент должен (MUST) обрабатывать опцию способом, согласованным со способом передачи поля Home Address из опции Home Address в заголовок IPv6, и замены в нем оригинального значения поля Source Address. После обработки всех опций IPv6 верхние уровни должны (MUST) иметь возможность обрабатывать пакет не зная, что первоначально он пришел с временного адреса, или что использовалась опция Home Address.

Использование заголовка аутентификации AH IPsec для опции Home Address не требуется, за исключением случая, когда IPv6-заголовок пакета охвачен AH, тогда аутентификация должна (MUST) также охватывать опцию Home Address; этот охват достигается автоматически путем определения кода Option Type для опции Home Address, поскольку он указывает на то, что данные в опции не могут измениться по пути к конечному месту назначения пакета, и, таким образом, опция включается в процесс вычисления AH. Благодаря требованию того, что любая аутентификация заголовка IPv6 охватывает также опцию Home Address, наличие опции Home Address не подрывает безопасность поля Source Address в заголовке IPv6.

При попытке проверить аутентификационные данные AH в пакете, который содержит опцию Home Address, принимающий узел должен (MUST) вычислить аутентификационные данные AH, как если бы было истинно следующее: опция Home Address содержит временный адрес, а поле IPv6-адреса источника в заголовке IPv6 содержит домашний адрес. Это соответствует вычислениям, специфицированным в разд. 11.3.2.

9.3.2. Посылка пакетов мобильному узлу

Перед посылкой любого пакета узел-отправитель должен (SHOULD) проверить свой кэш привязок на наличие элемента для адреса места назначения, на который этот пакет посылается. Если узел-отправитель имеет элемент кэша привязок для этого адреса, он должен (SHOULD) использовать заголовок маршрутизации типа 2 для пересылки пакета этому мобильному узлу (узлу места назначения) по пути его временного адреса. Однако узел-отправитель не должен (MUST) делать этого в следующих случаях:

- При посылке пакета IPv6 Neighbor Discovery [12].

- При условии, отмеченном в разд. 6.1.

При вычислении аутентификационных данных в пакете, который содержит заголовок маршрутизации типа 2, узел-корреспондент должен (MUST) вычислить аутентификационные данные AH, как если бы было истинным следующее: заголовок маршрутизации содержит временный адрес, поле IPv6-адреса места назначения заголовка IPv6 содержит домашний адрес, и поле Segments Left равно нулю. Поиск в базе данных политики безопасности IPsec должен (MUST) базироваться на домашнем адресе мобильного узла.

Например, предполагая, что в данном пакете отсутствуют дополнительные заголовки маршрутизации, помимо необходимых для протокола мобильного IPv6, узел-корреспондент может установить поля в IPv6-заголовке пакета и заголовке маршрутизации следующим образом:

- Поле Destination Address в IPv6-заголовке пакета устанавливается равным домашнему адресу мобильного узла (первоначальный адрес места назначения, на который посылался пакет).

- Заголовок маршрутизации инициализируется так, чтобы он включал один маршрутный сегмент, содержащий временный адрес мобильного узла, скопированный из элемента кэша привязок. Однако поле Segments Left временно устанавливается в 0.

Уровень IP вставит заголовок маршрутизации перед выполнением любой необходимой обработки IPsec. Когда вся обработка IPsec выполнена, узел осуществляет обмен поля места назначения IPv6 с полем Home Address в заголовке маршрутизации, устанавливает поле Segments Left в единицу и посылает пакет. Это гарантирует, что вычисление AH выполняется над пакетом в такой форме, которую оно будет иметь в приемнике после прохода заголовка маршрутизации.

Следуя определению заголовка маршрутизации типа 2 в разд. 6.4, этот пакет будет маршрутизирован на временный адрес мобильного узла, где он будет доставлен мобильному узлу (мобильный узел имеет временный адрес, ассоциированный с его сетевым интерфейсом).

Заметим, что следование описанной выше концептуальной модели в реализации создает некоторые дополнительные требования для определения MTU пути, поскольку уровень, который принимает решение о размере пакета (например, TCP и приложения, использующие UDP) должен быть осведомлен о размере заголовков, добавляемых уровнем IP на узле-отправителе.

Если, вместо этого, узел-отправитель не имеет элемента кэша привязок для адреса места назначения, на который посылается пакет, то он просто посылает пакет

обычным образом без заголовка маршрутизации. Если узел назначения не является мобильным узлом (или является мобильным узлом, который в текущий момент времени находится дома), пакет будет доставлен непосредственно этому узлу и обычным образом им обработан. Однако если узел назначения является мобильным узлом, который в текущий момент времени находится вне дома, то пакет будет перехвачен домашним агентом мобильного узла и туннелирован на текущий основной временный адрес мобильного узла.

9.3.3. Посылка сообщений Binding Error

В разд. 9.2 и 9.3.1 описываются ошибочные ситуации, которые приводят к необходимости посылки сообщения Binding Error.

Сообщение Binding Error посылается непосредственно на тот адрес, который находился в поле IPv6 Source Address пакета, нарушевшего нормальную работу. Если поле Source Address не содержит индивидуального адреса, то сообщение Binding Error не должно (MUST NOT) посылаться.

Поле Home Address в сообщении Binding Error должно (MUST) копироваться из поля Home Address опции места назначения Home Address пакета, нарушившего нормальную работу, или установлено в значение неспецифицированного адреса, если в пакете такая опция отсутствует.

Заметим, что значения полей IPv6 Source Address и Home Address, обсуждавшиеся выше, являются значениями, полученными с «линии», т.е. до каких-либо возможно выполнявшихся модификаций, как специфицировано в разд. 9.3.1.

Скорость отправки сообщений Binding Error должна (SHOULD) быть ограничена тем же самым способом, как и для сообщений ICMPv6 [14].

9.3.4. Прием сообщений об ошибках ICMP

Когда узел-корреспондент имеет элемент кэша привязок для мобильного узла, весь трафик, предназначенный мобильному узлу, при помощи заголовка маршрутизации направляется непосредственно на текущий временный адрес мобильного узла. Любое сообщение ICMP, вызванное пакетами на их пути к временному адресу, будет возвращено узлу-корреспонденту обычным способом.

С другой стороны, если узел-корреспондент не имеет элемента кэша привязок для мобильного узла, пакет будет маршрутизироваться через домашний линк мобильного узла. Любое сообщение об ошибках ICMP, вызванное находящимся в туннеле пакетом на его пути к мобильному узлу, будет передано домашнему агенту мобильного узла. По определению IPv6-инкапсуляции [15], домашний агент должен (MUST) ретранслировать определенные сообщения об ошибках ICMP назад первоначальному отправителю пакета, которым в данном случае является узел-корреспондент.

Таким образом, во всех случаях любые существенные сообщения об ошибках ICMP, вызванные пакетами от узла-корреспондента к мобильному узлу, будут возвращаться узлу-корреспонденту. Если узел-корреспондент после посылки мобильному узлу пакетов, сформированных на базе элемента в своем кэше привязок, получает устойчивые сообщения ICMP Destination Unreachable, то он должен (SHOULD) уничтожить этот элемент кэша привязок. Заметим, что если мобильный узел продолжает посылать этому узлу-корреспонденту пакеты с опцией места назначения Home Address, то они будут отбрасываться из-за отсутствия привязки. По этой причине важно, чтобы только устойчивые сообщения ICMP приводили к уничтожению элемента кэша привязок.

9.4. Процедура обратной маршрутизируемости

В данном подразделе специфицируются действия, выполняемые узлом-корреспондентом во время процедуры обратной маршрутизируемости.

9.4.1. Прием сообщений Home Test Init

При получении сообщения Home Test Init узел-корреспондент осуществляет проверку следующего:

- Пакет не должен (MUST NOT) включать опцию места назначения Home Address.

Любой пакет, переносящий сообщение Home Test Init, которому не удается пройти все эти проверки, должен (MUST) молча игнорироваться.

В противном случае при подготовке к отправке соответствующего сообщения Home Test узел-корреспондент проверяет, что он имеет необходимый материал для участия в процедуре обратной маршрутизируемости, как специфицировано в разд. 5.2. Узел-корреспондент должен (MUST) иметь секретный ключ Kcn и одноразовый номер. Если он еще не имеет этот материал, то до продолжения выполнения процедуры обратной маршрутизируемости он должен (MUST) его сформировать.

В разд. 9.4.3 специфицируется дальнейшая обработка.

9.4.2. Прием сообщений Care-of Test Init

При получении сообщения Care-of Test Init узел-корреспондент проверяет следующее:

- Пакет не должен (MUST NOT) включать опцию места назначения Home Address.

Любой пакет, переносящий сообщение Care-of Test Init, которому не удается пройти все эти проверки, должен (MUST) молча игнорироваться.

В противном случае при подготовке посылки соответствующего сообщения Care-of Test узел-корреспондент проверяет, что он имеет необходимый материал для участия в процедуре обратной маршрутизируемости способом, описанным в разд. 9.4.1.

В разд. 9.4.4 специфицирована дальнейшая обработка.

9.4.3. Посылка сообщений Home Test

Узел-корреспондент создает маркер home keygen token и использует текущий индекс одноразовых номеров в качестве индекса Home Nonce Index. Затем он создает сообщение Home Test (разд. 6.1.5) и посылает его мобильному узлу на домашний адрес последнего.

9.4.4. Посылка сообщений Care-of Test

Узел-корреспондент создает маркер care-of keygen token и использует текущий индекс одноразовых номеров в качестве индекса Care-of Nonce Index. Затем он создает сообщение Care-of Test (разд. 6.1.6) и посылает его мобильному узлу на временный адрес последнего.

9.5. Обработка привязок

В данном разделе объясняется, как узел-корреспондент обрабатывает сообщения, связанные с привязками. Этими сообщениями являются сообщения:

- Binding Update
- Binding Refresh Request
- Binding Acknowledgement

- Binding Error

9.5.1. Прием сообщений Binding Update

Перед тем как признать годным сообщение Binding Update принимающий узел должен (MUST) его утвердить в соответствии со следующими проверками:

- Пакет должен (MUST) содержать индивидуальный маршрутизируемый домашний адрес либо в опции Home Address, либо в поле Source Address, если опция Home Address отсутствует.

- Значение поля Sequence Number в сообщении Binding Update больше, чем порядковый номер, полученный в предыдущем имевшем силу обновлении привязки для этого домашнего адреса, если таковое было.

Если принимающий узел не имеет элемента кэша привязок для указанного домашнего адреса, то он должен (MUST) признать годным любое значение порядкового номера в полученном сообщении Binding Update от этого мобильного узла.

Такое сравнение порядковых номеров должно выполняться по модулю 2**16, то есть, этот номер является свободно работающим счетчиком, представляющим модуль 65536. Порядковый номер в полученном обновлении привязки считается меньшим или равным последнему принятому номеру, если его значение лежит в диапазоне последнего полученного номера и предшествует 32768 значениям включительно. Например, если последний полученный номер был равен 15, то сообщения с порядковыми номерами от 0 до 15, а также от 32783 до 65535, будут считаться меньшими или равными.

Если бит Home Registration (H) не установлен, то требуется также следующее:

- Должна (MUST) присутствовать опция мобильности Nonce Indices, и значения Home Nonce Index и Care-of Nonce Index в этой опции должны (MUST) оцениваться узлом-корреспондентом как достаточно свежие. (Для запросов уничтожения привязки значения Care-of Nonce Index проверке не подвергаются).

- Узел-корреспондент должен (MUST) повторно сгенерировать маркер home keygen token и маркер care-of keygen token из информации, содержащейся в пакете. Затем он генерирует ключ управления привязкой Kbm и использует его для проверки поля Authenticator в сообщении Binding Update, как специфицировано в разд. 6.1.7.

- Опция мобильности Binding Authorization Data должна (MUST) присутствовать, а ее содержимое должно (MUST) удовлетворять правилам, представленным в разд. 5.2.6. Заметим, что временный адрес, отличный от адреса источника может быть (MAY) определен путем включения в сообщение Binding Update опции мобильности Alternate Care-of Address. Когда принимается такое сообщение, и в качестве метода авторизации используется процедура обратной маршрутизируемости, узел-корреспондент должен (MUST) проверить Authenticator, используя в вычислениях адрес из опции Alternate Care-of Address.

- Опция мобильности Binding Authorization Data должна (MUST) быть последней опцией и не должна (MUST NOT) иметь замыкающего заполнения.

Если бит Home Registration (H) установлен, то опция Nonce Indices не должна (MUST NOT) присутствовать.

Если мобильный узел посылает порядковый номер, который не больше порядкового номера из последнего годного сообщения Binding Update для данного домашнего адреса, то принимающий узел должен (MUST) послать назад сообщение Binding Acknowledgement с кодом состояния 135, и в поле Sequence Number сообщения Binding Acknowledgement последний принятый (считавшийся приемлемым) порядковый номер.

Если для данного домашнего адреса привязка уже существует и флаг регистрации в домашнем агенте имеет значение, отличное от значения бита Home Registration (H) в сообщении Binding Update, то принимающий узел должен (MUST) послать назад сообщение Binding Acknowledgement с кодом состояния 139 (registration type change disallowed). Флаг регистрации в домашнем агенте, хранящийся в элементе кэша привязок не должен (MUST NOT) меняться.

Если принимающий узел больше не признает годными значение Home Nonce Index, значение Care-of Nonce Index, или оба эти значения из сообщения Binding Update, то он должен (MUST) послать назад сообщение Binding Acknowledgement с кодом состояния 136, 137, или 138, соответственно.

Пакеты, переносящие сообщения Binding Update, которые не удовлетворяют всем этим проверкам по любой причине, отличной от недостаточности порядкового номера, изменения типа регистрации или устаревших значений индексов одноразовых номеров, должны (MUST) молча отбрасываться.

Если сообщение Binding Update с точки зрения указанных выше проверок обосновано, то оно обрабатывается далее следующим образом:

- Значение Sequence Number, полученное от мобильного узла в сообщении Binding Update, сохраняется принимающим узлом в элементе его кэша привязок для данного домашнего адреса.

- Если время жизни, указанное в сообщении Binding Update, не равно нулю и указанный временный адрес не равен домашнему адресу для этой привязки, то это запрос на кэширование привязки для данного домашнего адреса. Если бит Home Registration (H) в сообщении Binding Update установлен, то это сообщение обрабатывается в соответствии с процедурой, специфицированной в разд. 10.3.1; в противном случае, оно обрабатывается в соответствии с процедурой, специфицированной в разд. 9.5.2.

- Если время жизни, указанное в сообщении Binding Update, равно нулю или указанный временный адрес равен домашнему адресу для этой привязки, то это запрос на удаление кэшированной привязки для данного домашнего адреса. В этом случае сообщение Binding Update должно (MUST) включать достоверный индекс home nonce index, а индекс care-of nonce index должен (MUST) узлом-корреспондентом игнорироваться. Тогда генерация ключа управления привязкой зависит только от маркера home keygen token (разд. 5.2.5). Если в сообщении Binding Update бит Home Registration (H) установлен, то оно обрабатывается в соответствии с процедурой, специфицированной в разд. 10.3.2; в противном случае, оно обрабатывается в соответствии с процедурой, специфицированной в разд. 9.5.3.

Заданный временный адрес должен (MUST) определяться следующим образом:

- Если присутствует опция Alternate Care-of Address, то временным адресом является адрес из этой опции.

- В противном случае, временным адресом является поле Source Address в IPv6-заголовке пакета.

Домашний адрес для привязки должен (MUST) определяться следующим образом:

- Если присутствует опция места назначения Home Address, то домашним адресом является адрес из этой опции.

- В противном случае, домашним адресом является поле Source Address в IPv6-заголовке пакета.

9.5.2. Запросы на кэширование привязки

В этом разделе описывается обработка годного сообщения Binding Update, которое запрашивает узел кэшировать привязку, для которой бит Home Registration (H) в этом сообщении не установлен.

В этом случае принимающий узел должен (SHOULD) создать новый элемент в своем кэше привязок для данного домашнего адреса, или обновить существующий элемент кэша привязок для данного домашнего адреса, если такой элемент уже существует. Время жизни элемента кэша привязок инициализируется из поля Lifetime, указанного в сообщении Binding Update, хотя это время жизни может (MAY) быть уменьшено узлом, кэширующим привязку; время жизни для элемента кэша привязок не должно быть (MUST NOT) больше, чем значение поля Lifetime, указанного в сообщении Binding Update. Любой элемент кэша привязок должен быть (MUST) удален после истечения его времени жизни.

Заметим, что если мобильный узел не запросил сообщения Binding Acknowledgement, то он окажется не осведомленным о выбранном более коротком времени жизни. Таким образом, мобильный узел может использовать оптимизацию маршрутов и посылать пакеты с опцией места назначения Home Address. Как обсуждалось в разд. 9.3.1, такие пакеты будут отбрасываться, если привязка отсутствует. Эта ситуация исправима, но может временно вызвать потерю пакетов.

Узел-корреспондент может (MAY) отказаться признать годным новый элемент кэша привязок, если у него нет достаточного количества ресурсов. От нового элемента может (MAY) также произойти отказ, если узел-корреспондент уверен в том, что его ресурсы используются более эффективно для некоторых других целей, таких, например, как обслуживание другого мобильного узла с большим объемом трафика. В обоих случаях узел-корреспондент должен (SHOULD) вернуть сообщение Binding Acknowledgement со значением поля состояния 130.

9.5.3. Запросы на удаление привязки

В этом разделе описывается обработка годного сообщения Binding Update, которое запрашивают узел удалить привязку, когда бит Home Registration (H) в этом сообщении не установлен.

Любая существующая привязка для данного домашнего адреса должна (MUST) быть удалена. В ответ на получение сообщения Binding Update элемент кэша привязок для домашнего адреса создаваться не должен (MUST NOT).

Если элемент кэша привязок был создан с помощью одноразовых номеров обратной маршрутизируемости, то узел-корреспондент должен (MUST) гарантировать, что одни и те же одноразовые номера с конкретным домашним и временным адресом снова не используются. Если оба одноразовых номера все еще являются годными, узел-корреспондент должен запомнить конкретную комбинацию индексов одноразовых номеров, адресов и порядкового номера как незаконную до тех пор, пока по крайней мере один из одноразовых номеров не устареет.

9.5.4. Посылка сообщений Binding Acknowledgement

Сообщения Binding Acknowledgement могут посылаться для индикации получения сообщения Binding Update следующим образом:

- Если сообщение Binding Update было отброшено, как описывалось в разд. 9.2 или 9.5.1, то сообщение Binding Acknowledgement не должно (MUST NOT) посылаться. В противном случае обработка зависит от следующих правил.

- Если в сообщении Binding Update бит Acknowledge (A) установлен, то сообщение Binding Acknowledgement должно (MUST) посылаться. В противном случае обработка зависит от следующего правила.

- Если узел отвергает сообщение Binding Update из-за устаревшего индекса одноразового номера, порядкового номера, выходящего за пределы окна (разд. 9.5.1), или из-за недостаточности ресурсов (разд. 9.5.2), то сообщение Binding Acknowledgement должно (MUST) посылаться. Если узел признает годным сообщение Binding Update, то сообщение Binding Acknowledgement не должно (SHOULD NOT) посылаться.

Если узел признает годным сообщение Binding Update и создает или обновляет элемент для данной привязки, то поле Status в сообщении Binding Acknowledgement должно (MUST) быть установлено в значение, меньшее, чем 128. В противном случае поле Status должно (MUST) быть установлено в значение, большее или равное 128. Значения для поля Status описываются в разд. 6.1.8 и в реестре присвоенных номеров IANA [19].

Если поле Status в сообщении Binding Acknowledgement содержит значение 136 (expired home nonce index), 137 (expired care-of nonce index), или 138 (expired nonces), то это сообщение не должно (MUST NOT) включать опцию мобильности Binding Authorization Data. В противном случае опция мобильности Binding Authorization Data должна (MUST) быть включена, и должна (MUST) соответствовать конкретным требованиям аутентификации для сообщений Binding Acknowledgement, как определено в разд. 5.2.

Если поле Source Address в заголовке IPv6, который переносит сообщение Binding Update, не содержит индивидуального адреса, то сообщение Binding Acknowledgement не должно (MUST NOT) посылаться, а пакет Binding Update должен (MUST) молча отбрасываться. В противном случае подтверждение должно (MUST) посылаться на адрес источника (Source Address). В отличие от обработки обычных пакетов, эта процедура адресации не использует информацию из кэша привязок. Однако в некоторых случаях требуется заголовок маршрутизации. Если адресом источника является домашний адрес мобильного узла, например, сообщение Binding Update не содержало опции места назначения Home Address, то сообщение Binding Acknowledgement должно (MUST) посылаться на этот адрес, а заголовок маршрутизации не должен (MUST NOT) использоваться. В противном случае сообщение Binding Acknowledgement должно (MUST) посылаться с помощью заголовка маршрутизации типа 2, который содержит домашний адрес мобильного узла.

9.5.5. Посылка сообщений Binding Refresh Request

Если удаляемый элемент кэша привязок еще активно использовался при посылке пакетов мобильному узлу, то следующий пакет, посылаемый мобильному узлу, будет маршрутизироваться обычным образом на домашний линк мобильного узла. Обмен информацией с мобильным узлом продолжается, но туннелирование от домашней сети создает дополнительные накладные расходы и задержку при доставке пакетов мобильному узлу.

Если отправитель знает, что элемент кэша привязок все еще активно используется, он может (MAY) послать мобильному узлу сообщение Binding Refresh Request, пытаясь избежать этих накладных расходов и задержки, связанной с уничтожением и повторным созданием элемента кэша привязок. Это сообщение всегда посылается на домашний адрес мобильного узла.

Узел-корреспондент может (MAY) повторно посылать сообщения Binding Refresh Request до тех пор, пока не будет применено ограничение скорости. Узел-корреспондент должен (MUST) остановить повторную передачу, когда он получает сообщение Binding Update.

9.6. Политика замещения кэша

Концептуально узел поддерживает отдельный таймер для каждого элемента в своем кэше привязок. При создании или обновлении элемента кэша привязок в ответ на полученное и признанное годным сообщение Binding Update, узел для этого элемента устанавливает таймер на указанный период времени жизни. Любой элемент в кэше привязок узла должен (MUST) быть удален после истечения времени жизни, указанного в сообщении Binding Update, на основании которого этот элемент был создан или в последний раз обновлялся.

Любой кэш привязок узла по необходимости будет иметь конечный размер. Для управления пространством в своем кэше привязок узел может (MAY) использовать любую разумную локальную политику.

Чтобы освободить место для нового элемента, узел может (MAY) принять решение о сбросе любого элемента, уже находящегося в его кэше привязок. Например, для замещения элементов кэша должна хорошо работать стратегия LRU (least-recently used), если только размер кэша привязок не является совсем недостаточным. При удалении элементов узел-корреспондент должен (MUST) следовать правилам разд. 5.2.8, чтобы защитить процедуру обратной маршрутизируемости от атак повторного воспроизведения.

Если узел посылает пакет на место назначения, для которого он сбросил элемент из своего кэша привязок, пакет будет маршрутизирован через домашний линк мобильного узла. Мобильный узел может это обнаружить и установить, если необходимо, новую привязку.

Однако если мобильный узел уверен в том, что привязка еще существует, он может использовать оптимизацию маршрутов и посылать пакеты с опцией места назначения Home Address. Как обсуждалось ранее, это может создать временную потерю пакетов в контексте сокращения времени жизни пакетов, выполняемого узлом-корреспондентом (разд. 9.5.2).

10. Работа домашнего агента

10.1. Концептуальные структуры данных

Каждый домашний агент должен (MUST) поддерживать кэш привязок (Binding Cache) и список домашних агентов (Home Agents List).

Правила поддержки кэша привязок для домашних агентов и узлов-корреспондентов одни и те же, и уже описаны в разд. 9.1.

Каждым домашним агентом поддерживается список домашних агентов, в котором хранится информация относительно каждого маршрутизатора, который действует как домашний агент на том же самом линке. Этот список используется механизмом динамического определения адреса домашнего агента. Говорят, что маршрутизатор действует как домашний агент, если он посылает сообщение Router Advertisement, в котором бит Home Agent (H) установлен. Когда истекает время жизни элемента списка (определено ниже), этот элемент удаляется из списка домашних агентов. Список домашних агентов похож на концептуальную структуру данных списка подразумеваемых маршрутизаторов (Default Router List), поддерживаемого каждым хостом для протокола Neighbor Discovery [12]. Список домашних агентов может (MAY) быть реализован любым способом, согласующимся с внешним поведением, описанным в данном документе.

Каждый домашний агент поддерживает отдельный список домашних агентов для каждого линка, на котором он служит домашним агентом. Новый элемент создается или существующий элемент обновляется в ответ на получение годного сообщения Router Advertisement, в котором бит Home Agent (H) установлен. Концептуально каждый элемент списка домашних агентов содержит следующие поля:

- «Локальный для линка» IP-адрес домашнего агента на этом линке. Этот адрес узнается по адресу источника сообщения Router Advertisements [12], полученного от маршрутизатора.

- Один или несколько глобальных IP-адресов для этого домашнего агента. Глобальные адреса узнаются из опций Prefix Information с установленным битом Router Address (R) и принимаются в сообщениях Router Advertisement от данного «локального для линка» адреса. Глобальные адреса для маршрутизатора в элементе списка домашних агентов должны (MUST) удаляться, когда префикс, ассоциированный с этим адресом, перестает быть годным [12].

- Оставшееся время жизни этого элемента списка домашних агентов. Если в сообщении Router Advertisement, полученном от домашнего агента, имеется опция Home Agent Information Option, время жизни элемента списка домашних агентов, представляющего этого домашнего агента, инициализируется из поля Home Agent Lifetime этой опции (если она имеется); в противном случае, время жизни инициализируется из поля Router Lifetime в полученном сообщении Router Advertisement. Если время жизни элемента в списке домашних агентов становится равным нулю, то этот элемент из списка домашних агентов должен (MUST) быть удален.

- Приоритет данного домашнего агента; большие значения указывают на более предпочтительного домашнего агента. Значение приоритета берется из поля Home Agent Preference в полученном сообщении Router Advertisement, если оно содержит опцию Home Agent Information Option и, в противном случае, устанавливается в 0 (значение по умолчанию). Домашний агент использует этот приоритет при упорядочивании списка домашних агентов, когда он посылает сообщение ICMP Home Agent Address Discovery.

10.2. Обработка заголовков мобильности

Все домашние агенты IPv6 при обработке заголовков мобильности должны (MUST) соблюдать правила, описанные в разд. 9.2.

10.3. Обработка привязок

10.3.1. Регистрация основного временного адреса

Когда узел принимает сообщение Binding Update, он должен (MUST) его признать годным и определить тип обновления привязки в соответствии с шагами, описанными в разд. 9.5.1. Более того, он должен (MUST) аутентифицировать обновление привязки, как описано в разд. 5.1. Чтобы гарантировать, что только правильный узел может контролировать конкретный домашний адрес, необходим также шаг авторизации, специфический для домашнего агента. Это обеспечивается с помощью того, что домашний адрес недвусмысленно идентифицирует контекст безопасности, который должен использоваться.

В данном разделе описана обработка годного и авторизованного сообщения Binding Update, когда оно запрашивает регистрацию основного временного адреса мобильного узла.

Чтобы начать обработку сообщения Binding Update, домашний агент должен (MUST) выполнить следующую последовательность проверок:

- Если узел реализует только функциональность узла-корреспондента, или не был сконфигурирован для работы в качестве домашнего агента, то он должен (MUST) отклонить сообщение Binding Update. Узел должен (MUST) также вернуть мобильному узлу сообщение Binding Acknowledgement, в котором поле Status установлено в значение 131 (home registration not supported – регистрация в домашнем агенте не поддерживается).

- Иначе, если домашний адрес для привязки (в пакете поле Home Address в опции Home Address) в соответствии с текущим списком Prefix List домашнего агента не является для линка IPv6-адресом, то домашний агент должен (MUST) отклонить сообщение Binding Update и должен (SHOULD) вернуть мобильному узлу сообщение Binding Acknowledgement, в котором поле Status установлено в значение 132 (not home subnet – не домашняя подсеть).

- Иначе, если домашний агент решит отвергнуть сообщение Binding Update по любой другой причине (например, из-за недостаточности ресурсов, чтобы служить домашним агентом другому мобильному узлу), то он должен (SHOULD) вернуть мобильному узлу сообщение Binding Acknowledgement, в котором поле Status установлено в соответствующее значение, чтобы указать причину отклонения.

- В сообщении должна (MUST) присутствовать опция места назначения Home Address. Она должна (MUST) быть признана годной, как описано в разд. 9.3.1 со следующим дополнительным правилом. Проверка наличия элемента кэша привязок не должна (MUST NOT) выполняться для пакетов IPsec, когда опция Home Address содержит адрес, для которого принимающий узел может действовать как домашний агент.

Если домашний агент считает сообщение Binding Update годным, он должен (MUST) для этого мобильного узла создать новый элемент в своем кэше привязок или обновить существующий элемент кэша привязок, если такой элемент уже существует. Поле Home Address, полученное в опции Home Address, задает домашний адрес мобильного узла.

Домашний агент должен (MUST) пометить этот элемент кэша привязок признаком регистации в домашнем агенте для указания того, что узел для этой привязки служит домашним агентом. Элементы кэша привязок, помеченные признаком регистрации в домашнем агенте, должны (MUST) быть исключены из обычной политики замещения, используемой для кэша привязок (разд. 9.6) и не должны (MUST NOT) удаляться из кэша привязок до тех пор, пока не истечет период времени жизни.

Домашний агент до возвращения сообщения Binding Acknowledgement должен (MUST) выполнить процедуру Duplicate Address Detection [13] на домашнем линке мобильного узла, если только этот домашний агент уже не имеет привязки к данному домашнему адресу. Это гарантирует, что никакой другой узел на домашнем линке не воспользовался домашним адресом мобильного узла при поступлении сообщения Binding Update. Если процедура определения дублирования адресов дает отрицательный результат для данного домашнего адреса или ассоциированного «локального для линка» адреса, то домашний агент должен (MUST) отвергнуть все сообщения Binding Update и должен (MUST) вернуть мобильному узлу сообщение Binding Acknowledgement, в котором поле Status установлено в значение 134 (Duplicate Address Detection failed – процедура определения дублирования адреса дала отрицательный результат). Когда домашний агент посылает мобильному узлу успешное подтверждение привязки, домашний агент гарантирует мобильному узлу, что он будет сохранять его адрес (адреса) уникальным до тех пор, пока не истечет время жизни, предоставленное для привязки.

Конкретные адреса, которые должны быть проверены до признания годным сообщения Binding Update, а позднее должны быть защищены путем выполнения процедуры определения дублирования адресов, зависят от установки бита Link-Local Address Compatibility (L) следующим образом:

- L=0: Защищать только данный адрес. Не получать «локальный для линка» адрес.

- L=1: Защищать как данный «не локальный для линка» индивидуальный (домашний) адрес, так и полученный «локальный для линка» адрес. «Локальный для линка» адрес получается путем замещения префикса подсети в домашнем адресе мобильного узла «локальным для линка» префиксом.

Время жизни элемента кэша привязок зависит от целого ряда факторов:

- Время жизни элемента кэша привязок не должно быть (MUST NOT) больше значения Lifetime, указанного в сообщении Binding Update.

- Время жизни элемента кэша привязок не должно быть (MUST NOT) больше действительно оставшегося времени жизни для префикса подсети в домашнем адресе мобильного узла, указанного сообщением Binding Update. Действительно оставшееся время жизни для этого префикса определяется домашним агентом на основе его собственного элемента списка префиксов (Prefix List) [12].

Оставшееся предпочтительное время жизни не должно (SHOULD NOT) иметь какого-либо влияния на время жизни элемента кэша привязок.

Домашний агент должен (MUST) удалить привязку, когда истечет действительное время жизни связанного с ним префикса.

- Домашний агент может (MAY) далее уменьшить указанное время жизни для привязки, например, базируясь на локальной политике. Результирующее время жизни запоминается домашним агентом в элементе кэша привязок, и этот элемент кэша привязок должен (MUST) быть удален домашним агентом после истечения этого времени жизни.

Независимо от состояния бита Acknowledge (A) в сообщении Binding Update, домашний агент должен (MUST) вернуть мобильному узлу сообщение Binding Acknowledgement, сконструированное следующим образом:

- Поле Status должно (MUST) быть установлено в значение, указывающее положительный результат. Значение 1 (accepted but prefix discovery necessary – признано годным, но необходимо определение префикса) должно (MUST) использоваться, если префикс подсети указанного домашнего адреса является опротестованным, или будет опротестован в течение времени жизни привязки, или в конце времени жизни привязки станет недействительным. В противном случае

должно (MUST) использоваться значение 0. С целью сравнения времен жизни привязки и префикса, времена жизни префиксов сначала преобразуются в четырехсекундные единицы путем игнорирования двух младших бит.

- Бит Key Management Mobility Capability (K) устанавливается, если полностью соблюдены следующие условия, и обнуляется в противном случае:

  * Бит Key Management Mobility Capability (K) был установлен в сообщении Binding Update.

  * Контексты безопасности IPsec между мобильным узлом и домашним агентом были установлены динамически.

  * Домашний агент имеет возможность обновить свою конечную точку в используемом протоколе управления ключами на новый временный адрес каждый раз, когда он перемещается.

  В зависимости от окончательного значения этого бита в сообщении Binding Acknowledgement, домашний агент должен (SHOULD) выполнить следующие действия:

  K = 0

  Сбросить соединения управления ключами со старым временным адресом, если они были. Если мобильный узел не имел привязки до посылки данного сообщения Binding Update, сбросить соединения с домашним адресом.

  K = 1

  Перенести конечную точку партнера соединения протокола управления ключами, если оно было, на новый временный адрес. Для соединения фазы 1 IKE это означает, что любые пакеты IKE, посланные партнеру, посылаются на этот адрес, а пакеты с этого адреса с оригинальными идентифицирующими цепочками ISAKMP считаются годными.

  Заметим, что документ RFC 2408 [8] разд. 2.5.3 дает конкретные правила, которым должны удовлетворять идентифицирующие цепочки ISAKMP: они должны зависеть от конкретных сторон и могут генерироваться только самим объектом. Затем он рекомендует конкретный способ сделать это, а именно, хэшем IP-адресов. При бите K, установленным в 1, этот рекомендованный метод реализации прямо не работает. Чтобы удовлетворить обоим правилам, конкретные стороны должны вести себя как оригинальные IP-адреса, а не те, которые используются в конкретный момент времени.

- Поле Sequence Number должно (MUST) быть скопировано из поля Sequence Number, заданного в сообщении Binding Update.

- Поле Lifetime должно (MUST) быть установлено в значение оставшегося для привязки времени жизни, которое, как описано выше, установлено для мобильного узла домашним агентом в своем элементе кэша привязок, который помечен признаком регистрации в домашнем агенте.

- Если домашний агент хранит элемент кэша привязок в долговременной памяти, то опция мобильности Binding Refresh Advice должна (MUST) быть опущена. В противном случае, домашний агент может (MAY) включить эту опцию, чтобы посоветовать мобильному узлу обновить свою привязку до истечения ее реального времени жизни.

  Если опция мобильности Binding Refresh Advice присутствует, то поле Refresh Interval в этой опции должно (MUST) быть установлено в значение, меньшее значения времени жизни, возвращаемого в сообщении Binding Acknowledgement. Это указывает на то, что мобильный узел должен (SHOULD) пытаться обновлять свою регистрацию в домашнем агенте с указанным более коротким периодом

времени. Домашний агент должен (MUST) сохранять регистрацию на весь период времени жизни, даже если мобильный узел не обновляет свою регистрацию с указанным периодом обновления.

Правила выбора IP-адреса места назначения (и, возможно, конструкции заголовка маршрутизации) для сообщения Binding Acknowledgement, посылаемого мобильному узлу, являются теми же самыми, что и в разд. 9.5.4.

Дополнительно домашний агент должен (MUST) следовать процедуре, определенной в разд. 10.4.1, для перехвата на домашнем линке мобильного узла пакетов, адресованных мобильному узлу, пока домашний агент служит домашним агентом этому мобильному узлу. Домашний агент должен (MUST) также быть готовым принять туннелируемые в обратном направлении пакеты от нового временного адреса мобильного узла, как описано в разд. 10.4.5. Наконец, домашний агент должен (MUST) также распространять новые префиксы домашней сети, как описано в разд. 10.6.

10.3.2. Отмена регистрации основного временного адреса

Отмена регистрации привязки может потребоваться, когда мобильный узел возвращается домой или когда мобильный узел знает, что он в посещаемой сети не будет иметь никаких временных адресов.

Сообщение Binding Update признается годным и авторизуется способом, описанным в предыдущем разделе; заметим, что когда мобильный узел отменяет регистрацию, находясь дома, он может не включать опцию места назначения Home Address, в этом случае домашним адресом мобильного узла является IP-адрес источника сообщения Binding Update, отменяющего регистрацию. В данном разделе описана обработка годного сообщения Binding Update, которое просит принимающий узел больше не служить домашним агентом, отменяя регистрацию своего основного временного адреса.

Чтобы начать обработку сообщения Binding Update, домашний агент должен (MUST) выполнить следующую проверку:

- Если принимающий узел в своем кэше привязок не имеет элемента для данного мобильного узла, помеченного признаком регистрации в домашнем агенте, то этот узел должен (MUST) отвергнуть сообщение Binding Update, и должен (SHOULD) вернуть мобильному узлу сообщение Binding Acknowledgement, в котором поле Status установлено в значение 133 (not home agent for this mobile node – не домашний агент для этого мобильного узла).

Если домашний агент не отвергает сообщение Binding Update, как в описанном выше случае, то он должен (MUST) удалить любой существующий элемент для этого мобильного узла из своего кэша привязок. Затем домашний агент должен (MUST) вернуть мобильному узлу сообщение Binding Acknowledgement, сконструированное следующим образом:

- Поле Status должно (MUST) быть установлено в значение 0, указывающее на благоприятный исход.

- Бит Key Management Mobility Capability (K) устанавливается или обнуляется, и действия, основанные на его значении, выполняются так, как описано в предыдущем разделе. Домашний адрес мобильного узла используется как его новый временный адрес с целью переноса соединения управления ключами на новую оконечную точку.

- Поле Sequence Number должно (MUST) быть скопировано из поля Sequence Number, заданного в сообщении Binding Update.

- Поле Lifetime должно (MUST) быть установлено в ноль.

- Опция мобильности Binding Refresh Advice должна (MUST) быть опущена.

Кроме того, домашний агент должен (MUST) прекратить на домашнем линке мобильного узла перехватывать пакеты, которые адресуются этому мобильному узлу (разд. 10.4.1).

Правила выбора IP-адреса места назначения (и, если требуется, конструкции заголовка маршрутизации) для сообщения Binding Acknowledgement мобильному узлу остаются теми же самыми, что и в предыдущем разделе. Когда значение поля Status в сообщении Binding Acknowledgement больше или равно 128 и адрес источника сообщения Binding Update находился на домашнем линке, домашний агент должен (MUST) послать его на канальный адрес (адрес канального уровня) мобильного узла (отыскиваемый либо из сообщения Binding Update, либо с помощью сообщения Neighbor Solicitation).

10.4. Обработка пакетов

10.4.1. Перехват пакетов для мобильного узла

Когда узел служит мобильному узлу домашним агентом, он должен (MUST) прилагать усилия по перехвату на домашнем линке пакетов, которые адресованы мобильному узлу.

Чтобы это сделать, в начале службы домашним агентом узел должен (MUST) от имени мобильного узла выполнить по домашнему линку групповую рассылку (multicast) сообщения Neighbor Advertisement [12]. Для домашнего адреса, указанного в сообщении Binding Update, домашний агент посылает сообщение Neighbor Advertisement [12] на групповой адрес всех узлов на домашнем линке (all-nodes multicast address), чтобы от имени мобильного узла объявить для этого IP-адреса собственный канальный адрес домашнего агента. Если в сообщении Binding Update был указан флаг Link-Layer Address Compatibility (L), домашний агент должен (MUST) делать то же самое для «локального для линка» адреса мобильного узла.

Все поля в каждом сообщении Neighbor Advertisement должны (SHOULD) быть установлены точно такими же, какими они были бы установлены мобильным узлом, если бы он, находясь дома, посылал это сообщение Neighbor Advertisement [12], со следующими исключениями:

- Целевой адрес (Target Address) в сообщении Neighbor Advertisement должен (MUST) быть установлен равным конкретному IP-адресу мобильного узла.

- Объявление должно включать опцию Target Link-layer Address, определяющую канальный адрес домашнего агента.

- Бит Router (R) в объявлении должен (MUST) быть установлен в ноль.

- Флаг Solicited Flag (S) в объявлении не должен (MUST NOT) быть установленным, поскольку никаким сообщением Neighbor Solicitation оно не было запрошено.

- Флаг Override Flag (O) в объявлении должен (MUST) быть установлен, указывая на то, что это объявление должно (SHOULD) в любом получившим его узле аннулировать любой существующий элемент в кэше соседей (Neighbor Cache).

- Адрес источника (Source Address) в заголовке IPv6 должен (MUST) быть установлен равным IP-адресу домашнего агента на интерфейсе, используемом для посылки объявления.

Любой узел на домашнем линке, который получит одно из (описанных выше) сообщений Neighbor Advertisement, обновит свой кэш соседей так, чтобы связать адрес мобильного узла с канальным адресом домашнего агента, что послужит причиной передачи любых будущих пакетов, в обычном случае предназначенных мобильному узлу, домашнему агенту этого мобильного узла.

Поскольку групповое вещание на локальном линке (например, Ethernet) обычно не дает гарантии надежности, домашний агент для повышения надежности может (MAY) повторно передавать это сообщение Neighbor Advertisement до MAX_NEIGHBOR_ADVERTISEMENT раз (см. [12]). Однако имеется вероятность того, что некоторые узлы на домашнем линке так и не получат ни одного сообщения Neighbor Advertisement. Но эти узлы, в конечном счете, с помощью механизма определения недостижимости соседей (Neighbor Unreachability Detection) [12] будут способны обнаружить изменение канального адреса для адреса мобильного узла.

Когда узел служит некоторому мобильному узлу домашним агентом, для перехвата на домашнем линке индивидуальных пакетов, адресованных мобильному узлу, домашний агент использует протокол IPv6 Neighbor Discovery [12]. Чтобы перехватывать пакеты таким способом, домашний агент должен (MUST) действовать для этого мобильного узла как агент-посредник (proxy) и отвечать на каждое полученное для него сообщение Neighbor Solicitation. Когда домашний агент получает сообщение Neighbor Solicitation, он должен (MUST) проверить, соответствует ли целевой адрес (Target Address), указанный в сообщении, адресу любого мобильного узла, для которого он имеет элемент кэша привязок, помеченный признаком регистрации в домашнем агенте.

Если в кэше привязок домашнего агента такой элемент существует, то домашний агент должен (MUST) ответить на сообщение Neighbor Solicitation сообщением Neighbor Advertisement, передавая собственный канальный адрес домашнего агента вместо канального адреса указанного целевого адреса. Кроме того, бит Router (R) в объявлении должен (MUST) быть установлен в ноль. Таким образом, работа домашнего агента в качестве агента-посредника дает возможность другим узлам на домашнем линке мобильного узла разрешить (определить) адрес мобильного узла, а домашнему агенту - защитить эти адреса на домашнем линке процедурой определения дублированного адреса [12].

10.4.2. Обработка перехваченных пакетов

Для любого пакета, посланного мобильному узлу от домашнего агента мобильного узла (в котором домашний агент является первоисточником-отправителем пакета), домашний агент для этого пакета работает как узел-корреспондент мобильного узла, и применяются процедуры, описанные в разд. 9.3.2. Следовательно, домашний агент использует заголовок маршрутизации для пересылки пакета мобильному узлу по пути основного временного адреса из кэша привязок домашнего агента.

Когда мобильный узел находится вне дома, домашний агент перехватывает на домашнем линке все пакеты, адресованные на домашний адрес мобильного узла, как описано в разд. 10.4.1. Чтобы переслать каждый перехваченный пакет мобильному узлу, домашний агент должен (MUST) туннелировать пакет мобильному узлу, используя IPv6-инкапсуляцию [15]. Когда домашний агент инкапсулирует перехваченный пакет для пересылки мобильному узлу, он устанавливает адрес источника (Source Address) в новом туннельном IP-заголовоке в значение собственного IP-адреса домашнего агента, а адрес места назначения (Destination Address) в туннельном IP-заголовке в значение основного временного адреса мобильного узла. При приеме мобильным узлом обычная обработка туннельного пакета [15] приведет к декапсуляции и обработке оригинального пакета мобильным узлом.

Однако пакеты, адресованные на «локальный для линка» адрес мобильного узла, не должны (MUST NOT) туннелироваться мобильному узлу. Вместо этого, эти пакеты должны (MUST) быть отброшены, и домашний агент должен (SHOULD) вернуть на адрес источника пакета (если только этот адрес источника не является групповым адресом) сообщение ICMP Destination Unreachable, Code 3. Пакеты, адресованные на «локальный для сайта» адрес мобильного узла, по умолчанию не должны (SHOULD NOT) туннелироваться мобильному узлу.

Перехват и туннелирование последующих групповых (multicast) пакетов в домашней сети выполняются, только если домашний агент поддерживает управляющие сообщения

участия в мультикастовой группе от мобильного узла, как описано в следующем разделе. Туннелирование групповых пакетов мобильному узлу следует ограничениям, подобным ограничениям, определенным выше для индивидуальных пакетов, адресованных на адреса мобильного узла типа «локальный для линка» и «локальный для сайта». Групповые пакеты, адресованные на групповой адрес с областью действия «локальный для линка» [3], на который мобильный узел подписывается, туннелироваться мобильному узлу не должны (MUST NOT). Эти пакеты должны (SHOULD) быть молча отброшены (после доставки другим локальным групповым получателям). Групповые пакеты, адресованные на групповой адрес с областью действия большей, чем «локальный для линка», но меньшей, чем «глобальный» (например, «локальный для сайта» и «локальный для организации» [3]), на который подписывается мобильный узел, туннелироваться мобильному узлу не должны (SHOULD NOT). Групповые пакеты, адресуемые с глобальной областью действия, на которую мобильный узел успешно подписался, должны (MUST) туннелироваться мобильному узлу.

Перед туннелированием пакета мобильному узлу домашний агент должен (MUST) выполнить любую обработку IPsec, как указано базой данных политики безопасности.

10.4.3. Управление участием в мультикастовых группах

Данный раздел является предварительным условием для пересылки групповых пакетов данных, описанных в предыдущем разделе. Если такая поддержка не обеспечивается, то управляющие сообщения о членстве в мультикастовой группе молча игнорируются.

Чтобы переслать групповые пакеты данных из домашней сети всем подходящим мобильным узлам, домашний агент должен (SHOULD) быть способным принимать от мобильного узла туннелируемую управляющую информацию о членстве в мультикастовой группе, чтобы определить, на какие группы подписался мобильный узел. Эти сообщения о членстве в мультикастовой группе являются сообщениями Listener Report, специфицированными в MLD [17] или в других протоколах, таких как [37].

Сообщения выдаются мобильным узлом, но посылаются домашнему агенту через обратный туннель. Эти сообщения выдаются всякий раз, когда мобильный узел примет решение разрешить прием пакетов для мультикастовой группы, или в ответ на запрос MLD Query от домашнего агента. Мобильный узел будет также выдавать управляющие сообщения о членстве в мультикастовой группе, чтобы запретить прием групповых пакетов, когда он больше не заинтересован в получении групповых рассылок для конкретной группы.

Чтобы получить информацию о текущем членстве мобильного узла в мультикастовых группах, домашний агент должен периодически передавать мобильному узлу через туннель сообщения MLD Query. Эти периодические передачи MLD будут гарантировать, что домашний агент имеет точную регистрацию групп, в которых заинтересован мобильный узел, несмотря на потери пакетов сообщений MLD о членстве мобильного узла в группах.

Все пакеты MLD посылаются непосредственно между мобильным узлом и домашним агентом. Поскольку все эти пакеты имеют местом назначения групповой адрес с областью действия «линк» и ограничены одним интервалом (hop limit = 1), прямая пересылка таких пакетов между домашней сетью и мобильным узлом отсутствует. Пакеты MLD между мобильным узлом и домашним агентом инкапсулируются в тот же самый туннельный заголовок, который используется для других потоков пакетов между мобильным узлом и домашним агентом.

Заметим, что в данный момент, хотя в MLD-пакетах используется «локальный для линка» источник, от этих являющихся уникальными адресов никакая функциональность не зависит, и эти пакеты не вызывают прямых ответов. Все сообщения MLD посылаются на групповые места назначения. Чтобы избежать в домашнем агенте неопределенности из-за мобильных узлов, которые для своей работы MLD могут выбрать одинаковые «локальные для линка» адреса источников, домашний агент должен идентифицировать, какой мобильный узел действительно был источником

конкретного сообщения MLD. Это может быть сделано путем пометки, по какому туннелю такое MLD прибыло, какой контекст IPsec SA использовался или с помощью других средств различения.

Данная спецификация не налагает требований на то, как должны выполняться функции этого раздела и функции групповой пересылки раздела 10.4.2. В момент написания данного документа существовало мнение, что в домашнем агенте будет необходима реализация работы полного маршрутизатора группового трафика IPv6, но может оказаться возможным достичь того же результата с помощью применения «агента-посредника MLD» (proxy MLD), объединенного с групповой пересылкой в ядре. Это может стать предметом будущих спецификаций.

10.4.4. Контекстное автокофигурирование адресов

В этом разделе описывается, как домашние агенты поддерживают использование механизмов контекстного автоконфигурирования адресов, таких как DHCPv6 [29], от мобильных узлов. Если эта поддержка не обеспечивается, то в сообщениях Mobile Prefix Advertisement биты M и O должны оставаться обнуленными. Любой мобильный узел, посылающий сообщения DHCPv6 домашнему агенту, не имеющему этой поддержки, не получит ответа.

Если используется DHCPv6, то пакеты посылаются с «локальными для линка» адресами источника либо на групповой адрес с областью действия «линк», либо на «локальный для линка» адрес. Мобильные узлы, желающие систематезировать сервис DHCPv6, могут туннелировать в обратном направлении домашнему агенту стандартные пакеты DHCPv6. Поскольку эти пакеты с областью действия «линк» не могут пересылаться в домашнюю сеть, домашний агент должен реализовать либо работу агента-ретранслятора DHCPv6, либо работу самого сервера DHCPv6. Входящий туннель или IPsec SA сообщений DHCPv6 с областью действия «линк» от мобильного узла должны помечаться так, чтобы можно было отправить назад соответствующему мобильному узлу ответы DHCPv6 с «локальным для линка» местом назначения. Сообщения DHCPv6, посланные мобильному узлу «с локальным для линка» местом назначения, должны туннелироваться в том же самом туннельном заголовке, который используется для других потоков пакетов.

10.4.5. Обработка пакетов, туннелируемых в обратном направлении

Трафик от мобильного узла узлу-корреспонденту идет через обратный туннель, если только между мобильным узлом и узлом-корреспондентом не установлена привязка. Домашние агенты должны (MUST) поддерживать туннелирование в обратном направлении следующим образом:

- Туннелируемый трафик прибывает на адрес домашнего агента с использованием IPv6-инкапсуляции [15].

- В зависимости от используемой домашним агентом политики безопасности туннелируемые в обратном направлении пакеты могут (MAY) быть отброшены, если не сопровождаются правомерным заголовком ESP. Поддержка аутентифицированного туннелирования в обратном направлении позволяет домашнему агенту защитить домашнюю сеть и узлы-корреспонденты от злонамеренных узлов, маскирующихся под мобильный узел.

- В противном случае, когда домашний агент декапсулирует туннелированный от мобильного узла пакет, он должен (MUST) проверить, что адрес источника в туннельном IP-заголовке является основным временным адресом мобильного узла. В противном случае, любой узел в Internet мог бы посылать трафик через домашнего агента и избежать ограничений входной фильтрации. Эта простая проверка вынуждает злоумышленника знать текущее местоположение реального мобильного узла и быть способным преодолеть входную фильтрацию. Такая проверка не является обязательной, если туннелируемый в обратном направлении пакет защищен ESP в туннельном режиме.

10.4.6. Защита пакетов обратной маршрутизируемости

Процедура обратной маршрутизируемости, описанная в разд. 5.2.5, предполагает, что конфиденциальность сообщений Home Test Init и Home Test защищена, поскольку они туннелируются между домашним агентом и мобильным узлом. Поэтому, для защиты пакетов, принадлежащих процедуре обратной маршрутизируемости, домашний агент должен (MUST) поддерживать туннельный режим IPsec ESP. Должна (MUST) быть доступной поддержка ненулевых алгоритмов шифровальных преобразований и аутентификации. Во время процедуры обратной маршрутизируемости не обязательно различать различные виды пакетов.

Для обеспечения этой защиты требуются контексты безопасности. Когда в результате признанного годным сообщения Binding Update меняется временный адрес мобильного узла, для следующих пакетов, посылаемых с использованием этих контекстов безопасности, требуется специальная обработка. Домашний агент должен (MUST) установить новый временный адрес в качестве адреса места назначения этих пакетов, как если бы в контексте безопасности изменился адрес места назначения во внешнем заголовке [21].

Описанная выше защита должна(SHOULD) использоваться всеми мобильными узлами. Такое использование контролируется при конфигурировании базы данных политики безопасности IPsec как на мобильном узле, так и на домашнем агенте.

Как описано ранее, сообщения Binding Update и Binding Acknowledgement требуют защиты между домашним агентом и мобильным узлом. Протокол заголовка мобильности переносит оба этих сообщения, а также сообщения процедуры обратной маршрутизируемости. С точки зрения базы данных политики безопасности эти сообщения являются неразличимыми. Когда для защиты сигнализации обратной маршрутизируемости или пакетов данных используется IPsec, эта защита должна (MUST) применяться только для пакетов обратной маршрутизируемости входящих в IPv6-инкапсулированный туннельный интерфейс между мобильным узлом и домашним агентом. Этого можно достичь, например, путем определения элементов базы данных политики безопасности конкретно для туннельного интерфейса. А именно, элементы политики в целом не применяются ко всему трафику, а только к трафику входящему в туннель. Это позволяет воспользоваться элементами базы данных политики безопасности, выделенными для каждого интерфейса [4], специфическими для туннельного интерфейса (подсоединению узла к туннелю [11]).

10.5. Динамическое определение адреса домашнего агента

В данном разделе описано, как домашний агент может помочь мобильным узлам определить адреса домашних агентов. Домашний агент отслеживает наличие других домашних агентов на том же самом линке и отвечает на запросы, посылаемые мобильным узлом.

10.5.1. Прием сообщений Router Advertisement

Для каждого линка, на котором маршрутизатор оказывает услуги домашнего агента, этот маршрутизатор поддерживает список домашних агентов, хранящий информацию относительно всех других домашних агентов на этом линке. Этот список используется в механизме динамического определения адреса домашнего агента, описанном в разд. 10.5. Информация для этого списка узнается посредством приема периодических незапрошенных групповых сообщений Router Advertisement способом, подобным концептуальным структурам данных, поддерживаемым каждым хостом для протокола Neighbor Discovery [12]. В структуре списка домашних агентов имеются объявления маршрутизаторов (Router Advertisements) от каждого (другого) находящегося на линке домашнего агента, и в них установлен бит Home Agent (H).

При получении правомерного сообщения Router Advertisement, как определено в алгоритме обработки, специфицированного для протокола Neighbor Discovery [12],

домашний агент выполняет следующие шаги дополнительно к любым шагам, которые требует от него протокол Neighbor Discovery:

- Если бит Home Agent (H) в сообщении Router Advertisement не установлен, то удалить элемент посылавшего узла в текущем списке домашних агентов (если он существует). Пропустить все следующие шаги.

- В противном случае, извлечь адрес источника из IP-заголовка сообщения Router Advertisement. Это «локальный для линка» IP-адрес на данном линке домашнего агента, посылающего это объявление [12].

- Определить приоритет этого домашнего агента. Если сообщение Router Advertisement содержит опцию Home Agent Information Option, то приоритет берется из поля Home Agent Preference этой опции; в противном случае должен (MUST) использоваться подразумеваемый приоритет (приоритет по умолчанию) равный 0.

- Определить время жизни для этого домашнего агента. Если сообщение Router Advertisement содержит опцию Home Agent Information Option, то время жизни берется из поля Home Agent Lifetime этой опции; в противном случае должно (SHOULD) использоваться время жизни, определенное полем Router Lifetime в сообщении Router Advertisement.

- Если «локальный для линка» адрес домашнего агента, посылающего это объявление, уже имеется в списке домашних агентов данного домашнего агента, и принятое значение времени жизни домашнего агента равно нулю, немедленно удалить этот элемент из списка домашних агентов.

- В противном случае, если «локальный для линка» адрес домашнего агента, посылающего это объявление, уже имеется в списке домашних агентов принимающего домашнего агента, переустановить его время жизни и приоритет определенными выше значениями.

- Если «локальный для линка» адрес домашнего агента, посылающего это объявление, еще не имеется в списке домашних агентов, поддерживаемом принимающим домашним агентом, и время жизни для посылающего домашнего агента не равно нулю, создать новый элемент списка и инициализировать его время жизни и приоритет определенными выше значениями.

- Если элемент списка домашних агентов для «локального для линка» адреса домашнего агента, посылающего это объявление, не был удален, как описано выше, определить каждый глобальный адрес (адреса) домашнего агента на основе каждой опции Prefix Information, полученной в этом объявлении, в которой бит Router Address (R) установлен (разд. 7.2). Добавить все такие глобальные адреса к списку глобальных адресов в данном элементе списка домашних агентов.

Домашний агент должен (SHOULD) поддерживать элемент в своем списке домашних агентов для каждого правомерного адреса домашнего агента до тех пор, пока не истечет время жизни этого элемента, спустя это время элемент должен быть удален.

Как описано в разд. 11.4.1, мобильный узел делает попытку динамического определения адреса домашнего агента путем посылки сообщения ICMP Home Agent Address Discovery Request на адрес «Mobile IPv6 Home-Agents anycast address» [16] для префикса своей домашней IP-подсети. Домашний агент, получающий сообщение Home Agent Address Discovery Request и обслуживающий эту подсеть, должен (SHOULD) вернуть мобильному узлу сообщение ICMP Home Agent Address Discovery Reply с полем адреса источника в пакете ответа, установленном в значение одного из глобальных уникальных адресов домашнего агента. Поле Home Agent Addresses в сообщении ответа конструируется следующим образом:

- Поле Home Agent Addresses должно (SHOULD) содержать все глобальные IP-адреса для каждого домашнего агента, перечисленного в собственном списке домашних агентов этого домашнего агента (разд. 10.1).

- IP-адреса в поле Home Agent Addresses должны (SHOULD) быть перечислены в порядке уменьшения значений приоритета, базируясь либо на соответствующем объявленном приоритете из опции Home Agent Information, либо на нулевом по умолчанию приоритете, если никакой приоритет не объявляется (либо на конфигурируемом приоритете домашнего агента для самого этого домашнего агента).

- Между домашними агентами с одинаковым приоритетом их IP-адреса в поле Home Agent Addresses должны (SHOULD) быть перечислены в порядке, который рандомизируется по отношению к другим домашним агентам с равными приоритетами каждый раз, когда сообщение Home Agent Address Discovery Reply возвращается этим домашним агентом.

- Если с домашним агентом связано более одного глобального IP-адреса, эти адреса должны (SHOULD) быть перечислены в случайном порядке.

- Домашний агент должен (SHOULD) сокращать количество IP-адресов домашних агентов так, чтобы пакет соответствовал минимальному значению IPv6 MTU [11]. Адреса домашних агентов, выбранные для включения в пакет, должны (SHOULD) быть адресами домашних агентов из полного списка, имеющими наивысший приоритет. Это ограничение ликвидирует опасность фрагментации пакета сообщения ответа (или его отвержения промежуточным маршрутизатором с сообщением ICMP Packet Too Big [14]).

10.6. Посылка префиксной информации мобильному узлу

10.6.1. Список префиксов домашней сети

Протокол Mobile IPv6 систематизирует распространение важной префиксной информации мобильному узлу, когда он находится вне дома так, что она может быть использована при конфигурировании домашнего адреса мобильного узла и при перенумерации сети. В этом механизме мобильные узлы, находящиеся вне дома, получают сообщения Mobile Prefix Advertisement. Эти сообщения включают опции Prefix Information Options для префиксов, конфигурируемых на интерфейсе (интерфейсах) домашней подсети домашнего агента.

Если имеется несколько домашних агентов, отличия в объявлениях, посланных разными домашними агентами, могут привести к неоднозначности использования конкретного домашнего адреса при переходе на другого домашнего агента. Чтобы гарантировать, что мобильные узлы получают одну и ту же информацию от разных домашних агентов, выдвигается требование, чтобы все домашние агенты на одном и том же линке конфигурировались одним и тем же способом.

Чтобы это поддерживать, домашний агент наблюдает за префиксами, объявляемыми им самим и другими домашними агентами на домашнем линке. В документе RFC 2461 [12] допускается, чтобы два маршрутизатора на одном и том же линке объявляли разные наборы префиксов. Для домашних агентов должны обнаруживаться отличия для заданного домашнего адреса, поскольку мобильный узел за один раз осуществляет обмен информацией только с одним домашним агентом и ему надо знать полный набор префиксов, присвоенных домашнему линку. Все другие сравнения объявлений маршрутизаторов выполняются так, как описано в разд. 6.2.7 RFC 2461.

10.6.2. Планирование доставки префиксов

Домашний агент, обслуживающий мобильный узел, будет планировать доставку новой префиксной информации этому мобильному узлу, когда возникает любое из следующих условий:

Должен (MUST):

- Меняется состояние флагов для префикса зарегистрированного домашнего адреса мобильного узла.

- Действительное или предпочтительное время жизни переконфигурируется или изменяется по любой причине, отличной от течения реального времени.

- Мобильный узел запрашивает информацию сообщением Mobile Prefix Solicitation (см. разд. 11.4.2).

Должен (SHOULD):

- К интерфейсу (интерфейсам) домашней подсети домашнего агента добавляется новый префикс.

Может (MAY):

- Меняется действительное или предпочтительное время жизни или состояние флагов для префикса, который не используется ни в одном элементе кэша привязок для данного мобильного узла.

Домашний агент использует следующий алгоритм для определения того, когда посылать мобильному узлу префиксную информацию.

- Если мобильный узел посылает запрос, отвечать немедленно.

- Если мобильному узлу не посылалось сообщение Mobile Prefix Advertisement в течение последних MaxMobPfxAdvInterval секунд (см. разд. 13), то гарантировать, что передача планируется. Действительное время передачи рандомизируется, как описано ниже.

- Если на интерфейс домашней подсети добавляется префикс, соответствующий регистрации мобильного узла в домашнем агенте, или если его информация меняется любым способом, который не опротестовывает адрес мобильного узла, то гарантировать, что передача планируется. Действительное время передачи рандомизируется, как описано ниже.

- Если истекает срок регистрации в домашнем агенте, отменить любые спланированные объявления мобильному узлу.

Во всех случаях посылается полный список префиксов.

Если домашний агент уже спланировал передачу мобильному узлу сообщения Prefix Advertisement, то он заменит это объявление новым, которое должно быть отправлено в спланированное время.

В противном случае, домашний агент вычисляет новое значение для RAND_ADV_DELAY, которое является смещением от текущего момента времени для планируемой передачи. Сначала вычислить максимальную задержку для планируемого объявления:

```
MaxScheduleDelay = min (MaxMobPfxAdvInterval, Preferred Lifetime),
```

где MaxMobPfxAdvInterval равен значению, определенному в разд. 12. Затем вычислить окончательную задержку для объявления:

```
RAND_ADV_DELAY = MinMobPfxAdvInterval +
      (rand() % abs(MaxScheduleDelay - MinMobPfxAdvInterval))
```

Здесь rand() возвращает случайное целое значение в диапазоне от 0 до максимально возможного целого значения. Предполагается, что это вычисление позволит смягчить взрывной характер объявлений в случае изменения префиксной информации. Кроме того, домашний агент может (MAY), когда необходимо, еще больше уменьшить скорость передачи пакетов путем дополнительной задержки индивидуальных

объявлений, чтобы избежать переполнения ресурсов локальной сети. Домашний агент должен (SHOULD) продолжать периодически повторно посылать мобильному узлу незапрошенное объявление до тех пор, пока оно не будет подтверждено получением от мобильного узла сообщения Mobile Prefix Solicitation.

Домашний агент должен (MUST) подождать PREFIX_ADV_TIMEOUT (см. разд. 12) перед первой повторной передачей и удваивать время ожидания повторной передачи для каждой последующей повторной передачи до тех пор, пока не сделано максимальное количество попыток PREFIX_ADV_RETRIES (см. разд. 12). Если привязки мобильного узла истекут до того, как будет получено соответствующее сообщение Binding Update, то домашний агент не должен (MUST NOT) больше повторять передачи, даже если не было повторно сделано PREFIX_ADV_RETRIES попыток. Между тем, если мобильный узел посылает другое сообщение Binding Update без возврата домой, то домашний агент снова должен (SHOULD) начать передавать незапрошенные объявления.

Если, как описано выше, на домашнем линке возникает некоторое условие, которое является причиной необходимости посылки мобильному узлу другого сообщения Prefix Advertisement до того, как мобильный узел подтвердил предыдущую передачу, домашний агент должен (SHOULD) объединить все опции Prefix Information из неподтвержденного объявления Mobile Prefix Advertisement в новое объявление. Затем домашний агент сбрасывает старое объявление.

10.6.3. Посылка объявлений

При посылке мобильному узлу объявления Mobile Prefix Advertisement домашний агент должен (MUST) сконструировать пакет следующим образом:

- Адрес источника (Source Address) в IPv6-заголовке пакета должен (MUST) быть установлен в значение IP-адреса домашнего агента, на который мобильный узел адресовал свою текущую регистрацию в домашнем агенте, или по умолчанию глобальный адрес его домашнего агента, если не существует привязки.

- Если объявление было запрошено, оно должно (MUST) иметь местом назначения адрес источника запроса. Если оно было инициировано изменением префикса или перенумерацией, то местом назначения объявления будет домашний адрес мобильного узла в привязке, которая инициировала это правило.

- Должен (MUST) быть включен заголовок маршрутизации типа 2 с домашним адресом мобильного узла.

- Заголовки IPsec должны (MUST) поддерживаться и должны (SHOULD) использоваться.

- Домашний агент должен (MUST) посылать пакет, как если бы это был любой другой индивидуальный IPv6-пакет, который он порождает.

- Установить флаг Managed Address Configuration (M), если соответствующий флаг был установлен в любом из объявлений Router Advertisement, из которого была получена префиксная информация (включая информацию, посылаемую данным домашним агентом).

- Установить флаг Other Stateful Configuration (O), если соответствующий флаг был установлен в любом из объявлений Router Advertisement, из которого была получена префиксная информация (включая информацию, посылаемую данным домашним агентом).

10.6.4. Время жизни для измененных префиксов

Как описано в разд. 10.3.1, время жизни, возвращаемое домашним агентом в сообщении Binding Acknowledgement, не должно (MUST) быть больше, чем действительно оставшееся время для префикса подсети в домашнем адресе мобильного узла. Это ограничение на время жизни привязки служит для того, чтобы запретить

использование домашнего адреса мобильного узла после того, как он становится недействительным.

11. Работа мобильного узла

11.1. Концептуальные структуры данных

Каждый мобильный узел должен (MUST) поддерживать список обновлений привязки (Binding Update List).

Список обновлений привязки хранит информацию для каждого посланного данным мобильным узлом сообщения Binding Update, для которого время жизни привязки еще не истекло. Список обновлений привязки содержит все привязки, посланные мобильным узлом либо его домашнему агенту, либо узлам-корреспондентам. Он также содержит сообщения Binding Update, которые ожидают окончания процедуры обратной маршрутизируемости до того момента, когда они могут быть посланы. Однако для нескольких сообщений Binding Update, посланных на один и тот же адрес места назначения, список обновлений привязки содержит только самое последнее посланное на это место назначения сообщение Binding Update (т.е. сообщение с наибольшим значением порядкового номера). Список обновлений привязки может (MAY) быть реализован любым способом, который согласуется с внешнем поведением, описанным в данном документе.

Концептуально, элемент списка обновлений привязки содержит следующие поля:

- IP-адрес узла, которому было послано сообщение Binding Update.
- Домашний адрес, для которого это сообщение Binding Update было послано.
- Временный адрес, посланный в данном сообщении Binding Update. Это значение необходимо мобильному узлу для того, чтобы определить, послал ли он сообщение Binding Update, задав свой новый временный адрес этому месту назначения после смены своего временного адреса.
- Начальное значение поля Lifetime, посланное в данном сообщении Binding Update.
- Оставшееся время жизни этой привязки. Это время жизни инициализируется из значения поля Lifetime, посланного в сообщении Binding Update, и декрементируется до тех пор, пока не станет равным нулю. В этот момент этот элемент должен (MUST) быть удален из списка обновлений привязки.
- Максимальное значение поля Sequence Number, посланное на это место назначения в предыдущих сообщениях Binding Update. Поле Sequence Number имеет длину 16 бит, и все сравнения значений порядковых номеров должны (MUST) выполняться по модулю 2**16 (см. разд. 9.5.1).
- Время, когда было послано последнее сообщение Binding Update на данное место назначения, как это требуется для реализации ограничения скорости посылки сообщений Binding Update.
- Состояние всех повторных передач, потребовавшихся для данного сообщения Binding Update. Это состояние включает время, оставшееся до следующей попытки повторной передачи сообщения Binding Update, и текущее состояние механизма экспоненциальной отсрочки повторных передач.
- Флаг, указывающий на то, должны ли, или нет, на данное место назначения посылаться будущие сообщения Binding Update. Мобильный узел устанавливает этот флаг в элементе списка обновлений привязки, когда он получает сообщение об ошибке ICMP «Parameter Problem, Code 1» в ответ на сообщение обратной маршрутизируемости или на сообщения Binding Update, посланные на это место назначения, как описано в разд. 11.3.5.

Список обновлений привязки используется для того, чтобы определить, должен ли конкретный пакет посылаться непосредственно узлу-корреспонденту, или туннелироваться через домашнего агента (см. разд. 11.3.1).

Концептуально список обновлений привязки содержит следующие данные, связанные с выполнением процедуры обратной маршрутизируемости. Эти данные важны только для сообщений Binding Update, посылаемых узлам-корреспондентам.

- Время, когда на данное место назначения в последний раз посылалось сообщение Home Test Init или Care-of Test Init, которое требуется для реализации ограничения скорости для процедуры обратной маршрутизируемости.

- Состояние всех повторных передач, потребовавшихся для данной процедуры обратной маршрутизируемости. Это состояние включает время, оставшееся до следующей попытки повторной передачи, и текущее состояние механизма экспоненциальной отсрочки повторных передач.

- Значения идентифицирующих цепочек, используемые в сообщениях Home Test Init и Care-of Test Init.

- Маркеры home keygen token и care-of keygen token, полученные от узла-корреспондента.

- Индексы одноразовых номеров home nonce index и care-of nonce index, полученные от узла-корреспондента.

- Время, когда каждый из маркеров и одноразовых номеров был получен от узла-корреспондента, которое требуется для реализации повторного использования при перемещениях.

11.2. Обработка заголовков мобильности

Все мобильные узлы IPv6 при обработке заголовков мобильности должны (MUST) соблюдать правила, описанные в разд. 9.2.

11.3. Обработка пакетов

11.3.1. Посылка пакетов при нахождении вне дома

Когда мобильный узел находится вне дома, он продолжает использовать свой домашний адрес, и, кроме того, использует также один или несколько временных адресов. При посылке пакета, находясь вне дома, мобильный узел может (MAY) выбрать один из этих адресов, чтобы использовать в качестве адреса источника пакета, следующим образом:

- Оычно протоколы, расположенные выше уровня IP, для большинства пакетов будут рассматривать домашний адрес мобильного узла, как его IP-адрес. Для посылаемых пакетов, которые являются частью соединений транспортного уровня, установленных, когда мобильный узел находился дома, мобильный узел должен (MUST) использовать свой домашний адрес. Подобным образом, для посылаемых пакетов, которые являются частью соединений транспортного уровня, которые мобильный узел может все еще использовать после перемещения на новое местоположение, мобильный узел должен (SHOULD) использовать свой домашний адрес этим способом. Если существует привязка, мобильный узел должен (SHOULD) посылать пакеты непосредственно узлу-корреспонденту. В противном случае, если привязка отсутствует, мобильный узел должен (MUST) использовать туннелирование в обратном направлении.

- Мобильный узел может (MAY) принять решение прямо использовать один из своих временных адресов в качестве адреса источника пакета, не требуя использования в пакете опции Home Address. Это особенно полезно для кратковременных обменов информацией, которые можно легко повторить, если они не удаются.

Использование временного адреса мобильного узла в качестве источника таких запросов обычно будет иметь меньшие накладные расходы, чем использование домашнего адреса мобильного узла, поскольку ни в запросе, ни в ответе на него нет неоходимости использовать никакие дополнительные опции. Такие пакеты могут маршрутизироваться обычным образом, прямо между их источником и местом назначения, не зависимо от протокола Mobile IPv6. Однако если приложение, работающее на мобильном узле, не имеет конкретных знаний о том, что посылаемое сообщение подогнано к этому общему способу обмена информацией, мобильный узел не должен использовать свой временный адрес в качестве источника пакета этим способом.

Выбор наиболее эффективного метода обмена информацией зависит от приложения и находится за рамками данной спецификации. Программные интерфейсы API, необходимые для управления этим выбором, также находятся за рамками данной спецификации.

o Когда мобильный узел находится не на своем домашнем линке, он не должен (MUST NOT) использовать опцию места назначения Home Address при обмене информацией с «локальными для линка» или «локальными для сайта» партнерами, если область действия домашнего адреса больше области действия адреса партнера.

Подобным образом, мобильный узел не должен (MUST NOT) использовать опцию места назначения Home Address для пакетов IPv6 Neighbor Discovery [12].

Детальная работа в этих случаях описана позже в данном разделе, а также обсуждается в [31].

Для пакетов, посылаемых мобильным узлом, когда он находится дома, не требуется никакой специальной обработки мобильного IPv6. Подобным образом, если мобильный узел использует любой адрес, отличный от своего домашнего адреса, в качестве источника пакета, посылаемого, когда он находится вне дома, никакой специальной обработки мобильного IPv6 не требуется. В любом случае, пакет просто адресуется и передается тем же самым способом, как любой обычный пакет IPv6.

Для пакетов, посылаемых мобильным узлом, когда он находится вне дома, с использованием домашнего адреса мобильного узла в качестве источника, требуется специальная обработка пакета мобильным IPv6. Это может быть сделано следующими двумя способами:

Оптимизация маршрута

Этот способ доставки пакетов не требует прохода через домашнюю сеть и обычно дает возможность осуществления более быстрой и надежной передачи.

Мобильный узел нуждается в гарантии того, что для его домашнего адреса имеется элемент кэша привязок так, чтобы узел-корреспондент мог обработать пакет (в разд. 9.3.1 определены правила обработки опции места назначения Home Address на узле-корреспонденте). Мобильный узел должен (SHOULD) проверить свой список обновлений привязки на наличие элемента, удовлетворяющего следующим условиям:

* Поле Source Address посылаемого пакета равно домашнему адресу в элементе списка.

* Поле Destination Address посылаемого пакета равно адресу узла-корреспондента в этом элементе списка.

* Один из временных адресов мобильного узла появляется в качестве временного адреса в этом элементе списка.

* Элемент списка указывает на то, что привязка была успешно создана.

* Оставшееся время жизни привязки больше нуля.

Если эти условия соблюдены, мобильный узел знает, что узел-корреспондент имеет подходящий элемент кэша привязок.

Мобильный узел должен (SHOULD) организовать доставку домашнего адреса в опции Home Address, и должен (MUST) установить поле Source Address в заголовке IPv6 в значение временного адреса, который мобильный узел зарегистрировал для использования в данном узле-корреспонденте. Тогда узел-корреспондент будет использовать адрес, доставленный в опции Home Address, для выполнения функции, традиционно выполняемой адресом источника IP в заголовке IPv6. Затем домашний адрес мобильного узла доставляется более высоким протокольным уровням и приложениям.

Более точно:

* Конструировать пакет, используя домашний адрес мобильного узла, как адрес источника (Source Address) пакета тем же способом, как если бы мобильный узел был дома. Это включает вычисление контрольной суммы верхнего уровня, используя домашний адрес в качестве значения источника.

* Вставить в пакет опцию Home Address с полем Home Address, скопированным из первоначального значения поля Source Address в пакете.

* Заменить поле Source Address в IPv6-заголовке пакета на один из временных адресов мобильного узла. Обычно это будет текущий основной временный адрес, но должен (MUST) быть адрес, присвоенный интерфейсу на используемом линке.

При использовании временного адреса в качестве адреса источника в IPv6-заголовке и домашнего адреса мобильного узла в опции Home Address пакет будет способным благополучно пройти через любой маршрутизатор, реализующий входную фильтрацию [26].

Туннелирование в обратном направлении

Это механизм, который туннелирует пакеты через домашнего агента. Он не столь эффективен, как описанный выше механизм, но необходим, если привязка в узле-корреспонденте еще отсутствует.

Этот механизм используется для пакетов, которые в IPv6-заголовке имеют в качестве адреса источника домашний адрес мобильного узла, или с пакетами управляющих протоколов групповой пересылки, как описано в разд. 11.3.4. Более точно:

* Пакет посылается домашнему агенту, используя IPv6-инкапсуляцию [15].

* Адрес источника в туннельном пакете равен основному временному адресу, который зарегистрирован в домашнем агенте.

* Адрес места назначения в туннельном пакете является адресом домашнего агента.

Затем домашний агент передаст инкапсулированный пакет узлу-корреспонденту.

11.3.2. Взаимодействие с исходящей обработкой IPsec

В данном разделе в общих чертах описано взаимодействие между исходящей обработкой мобильного IPv6 и исходящей обработкой IPsec для пакетов, посылаемых мобильным узлом, находящимся вне дома. Любая конкретная реализация может (MAY) использовать алгоритмы и структуры данных, отличные от предлагаемых здесь, однако ее обработка должна (MUST) быть согласованной с описанными здесь результатами работы и с соответствующими спецификациями IPsec. В описанных ниже шагах предполагается, что IPsec используется в транспортном режиме [4], и что

мобильный узел использует свой домашний адрес, как источник пакета (с точки зрения протоколов более высоких уровней и приложений, как описано в разд. 11.3.1):

- Пакет создается протоколами более высокого уровня и приложениями (например, TCP), как если бы мобильный узел находился дома, и протокол мобильного IPv6 не использовался.

- Определить для пакета исходящий интерфейс. (Заметим, что выбор между туннелированием в обратном направлении и оптимизацией маршрута может предполагать разные интерфейсы, в частности, если туннели также считаются интерфейсами).

- Как часть исходящей обработки пакета в IP, пакет сравнивается с базой данных политики безопасности IPsec для того чтобы определить, какая обработка для него требуется [4].

- Если требуется обработка IPsec, пакет либо сопоставляется с существующим контекстом безопасности SA (или со связкой контекстов безопасности), либо для пакета создается новый SA (или связка SA), в соответствии с процедурами, определенными для IPsec.

- Поскольку мобильный узел находится вне дома, чтобы достичь узла-корреспондента, он использует либо туннелирование в обратном направлении, либо оптимизацию маршрута.

  Если используется туннелирование в обратном направлении, пакет конструируется обычным способом и затем туннелируется через домашнего агента.

  Если используется оптимизация маршрута, то мобильный узел вставляет в пакет опцию места назначения Home Address, заменяя поле Source Address в IP-заголовке пакета временным адресом, используемым совместно с данным узлом-корреспондентом, как описано в разд. 11.3.1. Заголовок Destination Options, в который вставляется опция места назначения Home Address, должен (MUST) появляться в пакете после заголовка маршрутизации, если таковой имеется, и до заголовка IPsec (AH [5] или ESP [6]), так что опция места назначения Home Address обрабатывается узлом места назначения до обработки заголовка IPsec.

  Наконец, когда пакет собран полностью, над ним выполняется необходимая аутентифицирующая IPsec-обработка (и, если требуется, шифрация), инициализирующая аутентификационные данные (Authentication Data) в заголовке IPsec.

  Обработка опций места назначения RFC 2402 расширяется следующим образом. Аутентификационные данные AH должны (MUST) вычисляться, как если бы истинными были следующие условия:

  * IPv6-адрес источника в заголовке IPv6 содержит домашний адрес мобильного узла,

  * поле Home Address в опции места назначения Home Address содержит новый временный адрес.

- Это позволяет, но не требует, приемнику пакета, содержащего опцию места назначения Home Address, поменять местами эти два поля поступающего пакета, чтобы получить описанную выше ситуацию, упрощая обработку всех последующих заголовков пакета. Однако такой обмен не требуется до тех пор, пока результат аутентификационных вычислений остается тем же самым.

Если для создания новых контекстов безопасности для партнера используется протокол автоматического управления ключами, то важно гарантировать, чтобы партнер мог посылать мобильному узлу пакеты протокола управления ключами. Это

может оказаться невозможным, если партнером является домашний агент мобильного узла и назначением контекстов безопасности является посылка домашнему агенту сообщения Binding Update. Пакеты, адресованные на домашний адрес мобильного узла, не могут использоваться до окончания обработки сообщения Binding Update. Для подразумеваемого случая использования IKE [9] в качестве протокола автоматического управления ключами (случая по умолчанию), таких проблем можно избежать с помощью выполнения следующих требований при обмене информацией со своим домашним агентом:

- Когда мобильный узел находится вне дома, он должен (MUST) использовать свой временный адрес в качестве адреса источника всех пакетов, которые он посылает как часть протокола управления ключами (без использования для этих пакетов протокола мобильного IPv6, как предлагается в разд. 11.3.1).

- Кроме того, для всех установленных IKE контекстов безопасности, привязанных к домашнему адресу мобильного узла, мобильный узел должен (MUST) включать в обмен фазы 2 IKE полезные данные идентификации (ISAKMP Identification Payload) [8], задающие домашний адрес мобильного узла как инициатора контекста безопасности [7].

Чтобы избежать необходимости повторного выполнения IKE после перемещений, в сообщениях Binding Update и Binding Acknowledgement может использоваться бит Key Management Mobility Capability (K).

11.3.3. Прием пакетов при нахождении вне дома

Находясь вне дома, мобильный узел будет получать пакеты, адресованные на его домашний адрес, одним из двух методов:

- Пакеты, посылаемые узлом-корреспондентом, который не имеет элемента кэша привязок для данного мобильного узла, будут посылаться на домашний адрес, захваченный домашним агентом, и туннелироваться мобильному узлу.

- Пакеты, посылаемые узлом-корреспондентом, который для мобильного узла имеет элемент кэша привязок, содержащий текущий временный адрес мобильного узла, будут посылаться узлом-корреспондентом, используя заголовок маршрутизации типа 2. Пакет будет адресован на временный адрес мобильного узла с последним интервалом в заголовке маршрутизации, направляющим пакет на домашний адрес мобильного узла; обработка этого последнего интервала заголовка маршрутизации полностью выполняется внутри мобильного узла, поскольку оба адреса, временный адрес и домашний адрес, являются адресами внутри мобильного узла.

Для пакетов, полученных первым методом, мобильный узел должен (MUST) проверить, что IPv6-адрес источника туннельного пакета является IP-адресом его домашнего агента. В этом методе мобильный узел может также послать сообщение Binding Update первоначальному отправителю пакета, как описано в разд. 11.7.2, которое является предметом ограничения скорости, определенного в разд. 11.8. Мобильный узел должен (MUST) также обрабатывать принятый пакет способом, определенным для IPv6-инкапсуляции [15], что приведет к тому, что инкапсулированный (внутренний) пакет будет обрабатываться внутри узла протоколами более высокого уровня обычным образом, как если бы он был адресован (только) на домашний адрес мобильного узла.

Для пакетов, полученных вторым методом, следующие правила приведут к тому, что пакет будет обрабатываться внутри узла протоколами более высокого уровня обычным образом, как если бы он был адресован (только) на домашний адрес мобильного узла.

Узел, принимающий пакет, адресованный себе самому (т.е. один из адресов узла находится в поле места назначения IPv6), идет по цепочке «следующий заголовок» и обрабатывает их. Когда во время этой обработки он обнаруживает заголовок

маршрутизации типа 2, он выполняет следующие проверки. Если любая из этих проверок не пройдет, узел должен (MUST) молча отбросить этот пакет.

- Поле длины в заголовке маршрутизации в точности равно 2.

- Поле segments left в заголовке маршрутизации «на линии» равно 1. (Но реализации могут обрабатывать заголовок маршрутизации так, что это значение может стать равным 0 после завершения обработки заголовка маршрутизации, но до того, как обрабатывается оставшаяся часть пакета).

- Поле Home Address в заголовке маршрутизации является одним из домашних адресов узла, если поле segments left было равно 1. Таким образом, требуется, в частности, чтобы поле адреса представляло индивидуальный маршрутизируемый адрес.

Когда указанные выше проверки выполнены, узел осуществляет обмен поля места назначения IPv6 с полем Home Address в заголовке маршрутизации, декрементирует значение segments left на единицу от его значения «на линии» и повторно представляет пакет IP для обработки следующего заголовка.

Концептуально это следует той же самой модели, что и в RFC 2460. Однако в случае заголовка маршрутизации типа 2 это может быть упрощено, поскольку известно, что пакет не будет пересылаться на другой узел.

Определение AH требует, чтобы отправитель вычислял контрольное значение целостности AH заголовка маршрутизации тем же самым способом, каким оно получается в приемнике после того, как он обработал заголовок. Поскольку заголовки IPsec следуют за заголовком маршрутизации, любая обработка IPsec будет работать над пакетом с домашним адресом в поле места назначения IP и полем segments left, равным нулю. Таким образом, вычисления AH на отправителе и приемнике будут иметь идентичный вид пакета.

11.3.4. Маршрутизация групповых пакетов

Мобильный узел, который подсоединен к своему домашнему линку, функционирует точно так же, что и любой другой (стационарный) узел. Таким образом, когда мобильный узел находится дома, он функционирует идентично другим групповым отправителям и приемникам. Поэтому в данном разделе описывается поведение мобильного узла, который не находится на своем домашнем линке.

Чтобы получать пакеты, посылаемые некоторой мультикастовой группе, мобильный узел должен присоединиться к этой мультикастовой группе. Один из методов, с помощью которого мобильный узел может (MAY) присоединиться к группе, заключается в подсоединении через групповой маршрутизатор (multicast router) на внешнем посещаемом линке. В этом случае мобильный узел, посылая пакеты MLD [17], должен (MUST) использовать свой временный адрес и не должен (MUST NOT) использовать опцию места назначения Home Address.

Альтернативно, мобильный узел может (MAY) присоединиться к мультикастовой группе через двунаправленный туннель к своему домашнему агенту. Мобильный узел туннелирует своему домашнему агенту пакеты управления членством в мультикастовых группах (например, пакеты, определенные в [17] или [37]), а домашний агент пересылает групповые пакеты по туннелю мобильному узлу. Мобильный узел не должен (MUST NOT) туннелировать пакеты управления членством в мультикастовых группах до тех пор, пока (1) мобильный узел не имеет привязки на домашнем агенте и (2) последний не послал через туннель, по крайней мере, один пакет управления членством в мультикастовых группах. Когда эти условия являются истинными, мобильный узел должен (SHOULD) предполагать, что они не изменятся до тех пор, пока не закончится привязка.

Мобильный узел, желающий послать пакет мультикастовой группе, имеет также две возможности:

1. Послать прямо с внешнего посещаемого линка

   Приложение осведомлено о временном адресе и использует его в качестве адреса источника для группового трафика, подобно тому, как оно использовало бы стационарный адрес. В таком трафике мобильный узел не должен (MUST NOT) использовать опцию места назначения Home Address.

2. Послать через туннель своему домашнему агенту

   Поскольку в общем случае групповая маршрутизация зависит от адреса источника, используемого в заголовке IPv6 группового пакета, мобильный узел, туннелирующий групповой пакет своему домашнему агенту, должен (MUST) использовать свой домашний адрес в качестве IPv6-адреса источника внутреннего группового пакета.

Заметим, что прямая посылка с внешнего линка применима только тогда, когда мобильный узел находится на этом внешнем линке. Это происходит потому, что сопутствующее дерево мультикастинга является специфическим для этого местоположения источника, и любое изменение местоположения и адреса источника сделает недействительным специфическое для этого источника дерево, или его ветвь, и прикладной контекст других членов мультикастовой группы.

Данная спецификация не предоставляет механизмов, которые бы позволили такому локальному групповому сеансу пережить передачу обслуживания и бесшовно продолжиться с нового временного адреса на каждом новом внешнем линке. Любой такой механизм, разработанный в качестве расширения к данной спецификации, нуждается в учете влияния быстро перемещающихся мобильных узлов на протоколы мультикастовой маршрутизации и в их способности поддерживать целостность специфических для источника деревьев мультикастинга и ветвей.

Несмотря на то, что использование двунаправленного туннелирования может гарантировать, что деревья мультикастинга являются независимыми от перемещений мобильных узлов, в некоторых случаях такое туннелирование может иметь неблагоприятные последствия. Будет затронута задержка конкретных типов мультикастовых приложений (таких, например, как основанные на мультикастинге протоколы определения - discovery protocols), если время на передачу и подтверждение приема (round-trip time) между внешней подсетью и домашним агентом является существенным по сравнению со временем выяснения топологии, которая должна быть определена. Кроме того, дерево доставки от домашнего агента в таких обстоятельствах зависит от индивидуальной инкапсуляции от агента к мобильному узлу. Поэтому использование полосы пропускания не будет эффективным по сравнению с естественной групповой пересылкой во внешней мультикастовой системе.

11.3.5. Прием сообщений об ошибках ICMP

Любой узел, который не распознает заголовок мобильности, будет возвращать отправителю пакета сообщение ICMP Parameter Problem, Code 1. Если мобильный узел получает такое ICMP-сообщение об ошибке в ответ на процедуру обратной маршрутизируемости или сообщение Binding Update, он должен (SHOULD) зарегистрировать в своем списке обновлений привязки, что будущие обновления привязки не должны (SHOULD NOT) посылаться на это место назначения. Чтобы позволить повторить попытку оптимизации маршрута, такие элементы списка обновлений привязки должны (SHOULD) удаляться спустя некоторый период времени.

Новые элементы списка обновлений привязки в результате получения ICMP-сообщений об ошибке не должны (MUST NOT) создаваться.

Узлы-корреспонденты, которые участвовали в процедуре обратной маршрутизируемости, должны (MUST) реализовывать возможность правильно обрабатывать принимаемые пакеты, содержащие опцию места назначения Home Address. Поэтому, правильно реализованные узлы-корреспонденты должны всегда быть

способными распознать опции Home Address. Если мобильный узел получает от некоторого узла сообщение ICMP Parameter Problem, Code 2 о том, что тот не поддерживает опцию Home Address, то мобильный узел должен (SHOULD) записать ошибку в журнал, а затем отбросить это сообщение ICMP.

11.3.6. Прием сообщений Binding Error

Когда мобильный узел принимает пакет, содержащий сообщение Binding Error, он должен сначала проверить, имеет ли мобильный узел элемент списка обновлений привязки для источника сообщения Binding Error. Если мобильный узел такого элемента не имеет, он должен (MUST) игнорировать это сообщение. Это необходимо для предотвращения пустой траты ресурсов, например, на процедуру обратной маршрутизируемости, из-за подложных сообщений Binding Error.

В противном случае, если значение поля Status сообщения было равно 1 (unknown binding for Home Address destination option – неизвестная привязка для опции места назначения Home Address), то мобильный узел должен выполнить одно из следующих двух действий:

- Если мобильный узел имеет недавнюю информацию о продвижении пакетов на более высоких уровнях, которая указывает на то, что обмены информацией с узлом-корреспондентом успешно развиваются, он может (MAY) игнорировать это сообщение. Это может быть сделано, чтобы ограничить ущерб, который может быть нанесен исходящим обменам информацией подложными сообщениями Binding Error.

- Если мобильный узел не имеет информации о продвижении пакетов на более высоких уровнях, он должен (MUST) удалить элемент и пересылать дальнейшие обмены через домашнего агента. Факультативно он может (MAY) также начать процедуру обратной маршрутизируемости (см. разд. 5.2).

Если поле Status сообщения было равно 2 (unrecognized MH Type value – нераспознанное значение типа заголовка маршрутизации), мобильный узел должен выполнить одно из следующих двух действий:

- Если мобильный узел не ожидал подтверждения или ответа от узла-корреспондента, то он должен (SHOULD) игнорировать это сообщение.

- В противном случае, мобильный узел должен (SHOULD) прекратить использование любых расширенний данной спецификации. Если же никаких расширений и не использовалось, то мобильный узел должен прекратить попытки использования оптимизации маршрута.

11.4. Управление домашними агентами и префиксами

11.4.1. Динамическое определение адреса домашнего агента

Иногда, когда мобильному узлу нужно послать обновление привязки своему домашнему агенту для регистрации своего нового основного временного адреса, как описано в разд. 11.7.1, мобильный узел может не знать адреса ни одного маршрутизатора на своем домашнем линке, который мог бы служить ему домашним агентом. Например, когда мобильный узел находился вне дома, некоторые узлы на его домашнем линке могли быть переконфигурированы таким образом, что маршрутизатор, работавший домашним агентом мобильного узла, был заменен другим маршрутизатором, выполняющим эту роль.

В этом случае, мобильный узел может (MAY) попытаться определить адрес подходящего домашнего агента на своем домашнем линке. Чтобы это сделать, мобильный узел посылает сообщение Home Agent Address Discovery Request на адрес «Mobile IPv6 Home-Agents anycast address» [16] для префикса своего домашнего

линка. Как описано в разд. 10.5, находящийся на его домашнем линке домашний агент, который получает это сообщение запроса, вернет сообщение-ответ Home Agent Address Discovery Reply. Это сообщение передает адреса домашних агентов на домашнем линке.

Тогда, после получения сообщения Home Agent Address Discovery Reply, мобильный узел может (MAY) послать свое сообщение Binding Update для регистрации в домашнем агенте на любой индивидуальный IP-адрес, указанный в ответе в поле Home Agent Addresses. Например, мобильный узел может (MAY) пытаться провести свою регистрацию в домашнем агенте по очереди на каждый из этих адресов до тех пор, пока его регистрация не будет одобрена. Мобильный узел посылает сообщение Binding Update на один из адресов и ждет соответствующего сообщения Binding Acknowledgement, переходя на следующий адрес, если не было ответа. Однако до посылки сообщения Binding Update другому домашнему агенту мобильный узел должен (MUST) ждать по крайней мере InitialBindackTimeoutFirstReg секунд (см. разд. 13). При опробывании каждого из возвращенных адресов домашних агентов мобильный узел должен (SHOULD) пробовать каждый из них в том порядке, в котором они находятся в поле Home Agent Addresses в полученном сообщении Home Agent Address Discovery Reply.

Если домашний узел имеет текущую регистрацию в каком-то домашнем агенте (время жизни этой регистрации еще не истекло), то он должен (MUST) попытаться выполнить любую новую регистрацию сначала в этом домашнем агенте. Если эта попытка регистрации не удалась (например, была завершена по тайм-ауту или была забракована), то тогда мобильный узел должен (MUST) повторить попытку этой регистрации на другом домашнем агенте. Если мобильный узел не знает никаких подходящих домашних агентов, то он может (MAY) попытаться использовать описанный выше механизм динамического определения адресов домашних агентов.

Если после передачи сообщения Home Agent Address Discovery Request на адрес «Home Agents Anycast address» мобильный узел в течение INITIAL_DHAAD_TIMEOUT секунд (см. разд. 12) не получает соответствующего сообщения Home Agent Address Discovery Reply, то он может (MAY) повторно передать то же самое сообщение запроса на тот же самый адрес типа anycast. Эта повторная передача может (MAY) повторяться максимально до DHAAD_RETRIES попыток (см. разд. 12). Каждая повторная передача по сравнению с предыдущей повторной передачей должна (MUST) быть задержена на удвоенный интервал времени.

11.4.2. Посылка сообщений Mobile Prefix Solicitation

Когда мобильный узел имеет домашний адрес, который почти что стал недействительным, он должен (SHOULD) послать своему домашнему агенту сообщение Mobile Prefix Solicitation (запрос мобильного префикса), чтобы попытаться получить обновленную маршрутную информацию о префиксах. Новая информация позволяет также мобильному узлу участвовать в затрагивающих домашнюю сеть операциях по ее перенумерации, как описано в разд. 10.6.

Для передачи своего домашнего адреса мобильный узел должен (MUST) использовать опцию места назначения Home Address. Для защиты этого запроса мобильный узел должен (MUST) поддерживать и должен (SHOULD) использовать IPsec. Мобильный узел должен (MUST) присвоить полю Identifier в заголовке ICMP случайное значение.

Как описано в разд. 11.7.2, сообщения Binding Update, посылаемые мобильным узлом другим узлам, должны (MUST) использовать время жизни не большее, чем оставшееся время жизни регистрации в домашнем агенте его основного временного адреса. Мобильный узел должен (SHOULD) еще больше ограничить времена жизни, которые он посылает в любых сообщениях Binding Update так, чтобы они находились в границах оставшегося действительного времени жизни префикса в его домашнем адресе (см. разд. 10.6.2).

Если время жизни для измененного префикса сокращается, и это изменение станет причиной того, что кэшированные привязки в узлах-корреспондентах в списке

обновлений привязки должны храниться сверх вновь укороченного времени жизни, мобильный узел должен (MUST) выдать сообщение Binding Update всем таким узлам-корреспондентам.

Эти ограничения на время жизни привязок предназначены для того, чтобы воспрепятствовать использованию домашнего адреса мобильного узла после того, как он станет недействительным.

11.4.3. Прием сообщений Mobile Prefix Advertisement

В разд. 10.6 описана работа домашнего агента, связанная с поддержкой конфигурирования во время начальной загрузки и перенумерации домашней подсети мобильного узла, когда мобильный узел находится вне дома. Домашний агент посылает мобильному узлу, когда тот находится вне дома, сообщения Mobile Prefix Advertisement (объявление мобильного префикса), задающие опции «важной» префиксной информации (Prefix Information), которые описывают изменения в используемых префиксах на домашнем линке мобильного узла.

Сообщение Mobile Prefix Solicitation подобно сообщению Router Solicitation, которое используется в протоколе Neighbor Discovery [12] за исключением того, что оно маршрутизируется от мобильного узла на посещаемой сети к домашнему агенту в домашней сети по обычным правилам индивидуальной маршрутизации.

Когда мобильный узел принимает сообщение Mobile Prefix Advertisement, он должен (MUST) его признать годным в соответствии со следующими проверками:

- Поле Source Address в IP-пакете, переносящем сообщение Mobile Prefix Advertisement, совпадает с адресом домашнего агента, которому мобильный узел в последний раз посылал признанное годным сообщение Binding Update для регистрации в домашнем агенте своего основного временного адреса. В противном случае, если такие регистрации не выполнились, это должен (SHOULD) быть хранимый мобильным узлом адрес домашнего агента, если таковой существует. В противном случае, если мобильный узел пока не определил адрес своего домашнего агента, то он не должен (MUST NOT) признавать годными сообщения Mobile Prefix Advertisement.

- Пакет должен (MUST) иметь заголовок маршрутизации типа 2 и должен (SHOULD) быть защищен заголовком IPsec, как описано в разд. 5.4 и 6.8.

- Если значение поля ICMP Identifier соответствует значению поля ICMP Identifier в совсем недавно посланном сообщении Mobile Prefix Solicitation, и никакие другие объявления для этого значения еще не были получены, то объявление должно считаться запрошенным, и будет далее обрабатываться.

  В противном случае, объявление является не запрошенным и должно (MUST) быть отброшено. В этом случае мобильный узел должен (SHOULD) послать сообщение Mobile Prefix Solicitation.

Любое принятое сообщение Mobile Prefix Advertisement, не удовлетворяющее этим проверкам, должно (MUST) быть молча отброшено.

Для признанного годным сообщения Mobile Prefix Advertisement мобильный узел должен (MUST) обработать биты Managed Address Configuration (M), Other Stateful Configuration (O), и опции Prefix Information Options, как если бы они прибыли в сообщении Router Advertisement [12] на домашнем линке мобильного узла. (Однако данная спецификация не описывает, как получить домашние адреса с помощью контекстных протоколов). Такая обработка может привести к конфигурированию на мобильном узле нового домашнего адреса, хотя благодаря разделению между предпочтительным временем жизни и действительным временем жизни, такие изменения не должны затрагивать большинство обменов информацией мобильного узла, точно так же, как и для узлов, которые находятся дома.

Данная спецификация предполагает, что на мобильном узле были заранее сконфигурированы все контексты безопасности и элементы политики безопасности, которые могут потребоваться для новых префиксов. Заметим, что хотя динамическое управление ключами устраняет необходимость создавать новые контексты безопасности, все еще остается необходимость добавлять элементы политики для защиты обменов информацией, затрагивающие домашний адрес (адреса). Механизмы автоматической установки этих элементов выходят за рамки данной спецификации.

11.5. Перемещение

11.5.1. Определение перемещения

Основной задачей определения перемещения является определение передач обслуживания на уровне L3. Этот раздел не пытается специфицировать алгоритм определения быстрого перемещения, который будет функционировать оптимально для всех типов приложений, канальных уровней и сценариев развертывания; вместо этого, в нем описан общий метод, который использует средства протокола IPv6 Neighbor Discovery, включая определение маршрутизаторов (Router Discovery) и определение недостижимости соседей (Neighbor Unreachability Detection). На момент написания данного документа этот метод считается достаточно хорошо понятым для того, чтобы его рекомендовать для стандартизации, однако ожидается, что будущие версии данной спецификации или другие спецификации могут содержать обновленные версии алгоритма определения перемещения, который имеет лучшую производительность.

Общий метод определения перемещения использует механизм определения недостижимости соседей для определения того, когда подразумеваемый маршрутизатор (маршрутизатор, используемый по умолчанию) больше не является двунаправленно достижимым, в этом случае мобильный узел должен определить новый подразумеваемый маршрутизатор (обычно на новом линке). Однако такое определение происходит только тогда, когда мобильный узел имеет пакеты для отсылки, и при отсутствии частых сообщений Router Advertisement или указаний от канального уровня мобильный узел может оказаться не осведомленным относительно передачи обслуживания L3, которая произошла. Поэтому, мобильный узел должен дополнять этот метод другой информацией всякий раз, когда она становится доступной мобильному узлу (например, от более низких протокольных уровней).

Когда мобильный узел обнаруживает передачу обслуживания L3, он выполняет процедуру определения дублирования адреса (Duplicate Address Detection [13]) со своим «локальным для линка» адресом, выбирает новый подразумеваемый маршрутизатор, как следствие процедуры Router Discovery, и затем выполняет процедуру Prefix Discovery с этим новым маршрутизатором для формирования нового временного адреса (адресов), как описано в разд. 11.5.2. Затем он регистрирует свой новый основной временный адрес в своем домашнем агенте, как описано в разд. 11.7.1. После обновления своей регистрации в домашнем агенте, мобильный узел обновляет связанные с ней привязки мобильности в узлах-корреспондентах, которые вместе с ним выполняют оптимизацию маршрутов, как описано в разд. 11.7.2.

Из-за временного нарушения потока пакетов и накладных расходов сигнализации, возникающих в результате обновления привязок мобильности, мобильный узел должен избегать выполнения передачи обслуживания L3 до тех пор, пока это не станет абсолютно необходимо. А именно, когда мобильный узел получает сообщение Router Advertisement от нового маршрутизатора, которое содержит другой набор префиксов «на линке», если мобильный узел определяет, что выбранный в настоящее время подразумеваемый маршрутизатор на старом линке все еще остается двунаправленно достижимым, он должен, как правило, продолжить использование старого маршрутизатора на старом линке, а не переключаться с него для использования нового подразумеваемого маршрутизатора.

Для определения передач обслуживания L3 мобильные узлы могут использовать информацию из принятых сообщений Router Advertisement. Выполняя это, мобильный узел должен рассматривать следующие проблемы:

- На том же самом линке может быть несколько маршрутизаторов, поэтому прослушивание нового маршрутизатора не обязательно создает передачу обслуживания L3.
- Когда на одном и том же линке имеется несколько маршрутизаторов, они могут объявлять различные префиксы. Таким образом, даже прослушивание нового маршрутизатора с новым префиксом не является надежной индикацией передачи обслуживания L3.
- «Локальные для линка» адреса маршрутизаторов не являются глобально уникальными, поэтому после завершения передачи обслуживания L3 мобильный узел может продолжать получать сообщения Router Advertisement с тем же самым «локальным для линка» адресом источника. Это может оказаться обычным случаем, если маршрутизаторы используют один и тот же «локальный для линка» адрес на нескольких интерфейсах. Эту проблему можно избежать, если маршрутизаторы используют бит Router Address (R), поскольку он предоставляет глобальный адрес маршрутизатора.

Кроме того, мобильный узел должен рассматривать следующие события в качестве индикации того, что могла произойти передача обслуживания L3. После приема таких указаний мобильный узел должен выполнить процедуру Router Discovery для определения маршрутизаторов и префиксов на новом линке, как описано в разд. 6.3.7 RFC 2461 [12].

- Если сообщения Router Advertisement, которые принимает мобильный узел, включают опцию Advertisement Interval, то мобильный узел может использовать ее поле Advertisement Interval, как индикацию частоты, с которой он должен продолжать получение будущих объявлений от этого маршрутизатора. Это поле указывает минимальную скорость (максимальное время между последовательными объявлениями), которую должен ожидать мобильный узел. Если это время проходит, а мобильный узел не получил ни одного объявления от этого маршрутизатора, он может быть уверенным в том, что по крайней мере одно объявление, посланное маршрутизатором, потеряно. Тогда мобильный узел может реализовать свою собственную политику для определения того, сколько потерянных объявлений от этого текущего подразумеваемого маршрутизатора являются индикацией состоявшейся передачи обслуживания L3.

- Процедура Neighbor Unreachability Detection определяет, что подразумеваемый маршрутизатор больше не доступен.

- В некоторых типах сетей предупреждение о том, что произошла передача обслуживания L2, может быть получено от протоколов более низких уровней или от программного обеспечения драйвера устройства в мобильном узле. Хотя дальнейшие подробности относительно обработки указаний L2, как намеков на перемещения, являются пунктом для дальнейшего исследования, во время написания данной спецификации разумным считается следующее:

  Индикация передачи обслуживания L2 может подразумевать, а может и не подразумевать перемещение L2, а перемещение L2 может подразумевать, а может и не подразумевать перемещение L3; эти взаимоотношения могут быть функцией типа L2, но могут быть также функцией реального развертывания беспроводной топологии.

  Если только не известно наверняка, что индикация передачи обслуживания L2 вероятно подразумевает перемещение L3, то вместо немедленной групповой рассылки сообщений запроса маршрутизаторов возможно окажется лучше попытаться проверить, является ли подразумеваемый маршрутизатор все еще двунаправленно достижимым. Это может быть выполнено путем посылки индивидуального сообщения Neighbor Solicitation и ожидания ответного сообщения Neighbor Advertisement с установленным флагом solicited (запрошенное). Заметим, что это подобно определению недостижимости соседей, но не имеет того же самого конечного автомата, например, состояния STALE.

Если подразумеваемый маршрутизатор не отвечает на это сообщение Neighbor Solicitation, имеет смысл продолжить групповую рассылку сообщений Router Solicitation.

11.5.2. Формирование новых временных адресов

После определения того, что он переместился, мобильный узел должен (SHOULD) сгенерировать новый основной временный адрес, используя обычные механизмы IPv6. Это должно быть (SHOULD) также сделано, когда текущий основной временный адрес становится опротестованным. Мобильный узел может (MAY) сформировать новый основной временный адрес в любой момент времени, но он не должен (MUST NOT) посылать своему домашнему агенту сообщение Binding Update относительно нового временного адреса чаще MAX_UPDATE_RATE раз в секунду.

Кроме того, мобильный узел может (MAY) формировать новые не основные временные адреса даже, когда он не переключился на новый подразумеваемый маршрутизатор. В каждый момент времени мобильный узел может иметь только один основной временный адрес (который регистрируется в его домашнем агенте), но может (MAY) иметь дополнительный временный адрес для любого префикса или для всех префиксов на своем текущем линке. Более того, поскольку интерфейс беспроводной сети в действительности может позволить мобильному узлу в каждый момент времени быть достижимым более чем на одном линке, (например, в рамках диапазона беспроводного передатчика маршрутизаторов на более чем одном отдельном линке), мобильный узел может (MAY) иметь временные адреса более чем на одном линке в каждый момент времени. Использование более одного временного адреса в каждый момент времени описывается в разд. 11.5.3.

Как описано в разд. 4, чтобы сформировать новый временный адрес, мобильный узел может (MAY) использовать либо бесконтекстное [13], либо контекстное (например, DHCPv6 [29]) автоконфигурирование адресов. Если в пакетах, являющихся частью процесса автоконфигурирования адресов, мобильному узлу необходимо использовать адрес источника (отличный от неспецифицированного адреса), он должен (MUST) использовать «локальный для линка» адрес, а не свой собственный домашний IPv6-адрес.

Спецификация RFC 2462 [13] указывает, что при обычной обработке определения дублирования адресов, узел должен (SHOULD) задержать посылку начального сообщения Neighbor Solicitation на случайное значение, находящееся в диапазоне от 0 до MAX_RTR_SOLICITATION_DELAY. Поскольку задержка определения дублирования адреса может привести к существенным задержкам при конфигурировании нового временного адреса, когда мобильный узел перемещается на новый линк, мобильный узел предпочтительно не должен (SHOULD NOT) задерживать процедуру DAD при конфигурировании нового временного адреса. Мобильный узел должен (SHOULD) обеспечивать задержку в соответствии с механизмами, специфицированными в RFC 2462, если только поведение реализации не нарушает синхронизацию шагов, которые происходят до DAD в случае, когда несколько узлов испытывают передачу обслуживания в один и тот же момент времени. Такое разсинхронизованное поведение может проявляться из-за случайных задержек в протоколах L2 или драйверах устройств, или из-за используемого механизма определения перемещения.

11.5.3. Использование нескольких временных адресов

Как описано в разд. 11.5.2, мобильный узел в каждый момент времени может (MAY) использовать более одного временного адреса. В частности, в случае нескольких беспроводных сетей в один и тот же момент времени мобильный узел может быть эффективно достижим по нескольким линкам (например, при перекрытии беспроводных ячеек), на которых могут существовать различные (on-link) префиксы подсетей. Мобильный узел должен (MUST) гарантировать, что его основной временный адрес всегда имеет префикс, который объявляется его текущим подразумеваемым

маршрутизатором. После выбора нового основного временного адреса мобильный узел должен (MUST) послать своему домашнему агенту сообщение Binding Update, содержащее этот временный адрес. Сообщение Binding Update для домашнего агента должно (MUST) иметь установленные биты Home Registration (H) и Acknowledge (A), как описано в разд. 11.7.1.

Чтобы способствовать плавным передачам обслуживания, мобильный узел должен (SHOULD) сохранять свой предыдущий основной временный адрес, как (не основной) временный адрес, и должен (SHOULD) все еще принимать пакеты на этот адрес, даже после регистрации своего нового основного временного адреса в своем домашнем агенте. Это разумно, поскольку мобильный узел может принимать пакеты на свой предыдущий основной временный адрес только если он действительно подсоединен к этому линку. Если предыдущий основной временный адрес был распределен с помощью контекстного автоконфигурирования адресов [29], мобильный узел может не пожелать освободить этот адрес немедленно после переключения на новый основной временный адрес.

Когда же мобильный узел определит, что он больше не достижим через данный линк, он должен (SHOULD) сделать недействительными все временные адреса, связанные с адресными префиксами, которые он получил от маршрутизаторов на недостижимом линке и которые не попадают в текущий набор адресных префиксов, объявленных (возможно новым) текущим подразумеваемым маршрутизатором.

11.5.4. Возвращение домой

С помощью используемого алгоритма определения перемещения (разд. 11.5.1) мобильный узел определяет, что он вернулся на свой домашний линк, когда он обнаруживает, что его домашний префикс снова «на линке». Тогда мобильный узел должен (SHOULD) послать своему домашнему агенту сообщение Binding Update, чтобы проинструктировать его больше не перехватывать или не туннелировать для него пакеты. В этой регистрации в домашнем агенте мобильный узел должен (MUST) установить биты Acknowledge (A) и Home Registration (H), установить поле времени жизни в ноль и установить временный адрес для привязки, равным собственному домашнему адресу мобильного узла. В сообщении Binding Update мобильный узел должен (MUST) использовать свой домашний адрес в качестве адреса источника.

Когда мобильный узел посылает своему домашнему агенту это сообщение Binding Update, он должен быть внимательным в том, как он использует запрос Neighbor Solicitation [12] (если таковой необходим) для того, чтобы узнать канальный адрес домашнего агента, поскольку домашний агент в текущий момент времени сконфигурирован для перехвата пакетов на домашний адрес мобильного узла с помощью процедуры определения дублирования адреса (DAD - Duplicate Address Detection). В частности, мобильный узел не может использовать свой домашний адрес в качестве адреса источника в запросе соседей до тех пор, пока домашний агент не прекратит защищать домашний адрес.

Обычно запрос мобильным узлом соседей для выяснения адреса домашнего агента не нужен, поскольку мобильный узел уже узнал канальный адрес домашнего агента из опции Source Link-Layer Address в сообщении Router Advertisement. Однако, если имеется несколько домашних агентов, то может быть еще необходимо послать запрос. В этом специальном случае возвращения мобильного узла домой, мобильный узел должен (MUST) групповым способом (multicast) разослать пакет и дополнительно установить поле Source Address этого сообщения Neighbor Solicitation в значение неспецифицированного адреса (0:0:0:0:0:0:0:0). Целевой адрес сообщения Neighbor Solicitation должен быть (MUST) установлен в значение адреса Solicited-Node multicast address [3]. Домашний агент пошлет обратно мобильному узлу групповое сообщение Neighbor Advertisement с установленным в ноль флагом Solicited flag (S). В любом случае мобильный узел должен (SHOULD) записать информацию из опции Source Link-Layer Address или из объявления, и установить состояние элемента кэша соседей для домашнего агента в состояние REACHABLE.

Затем мобильный узел посылает свое сообщение Binding Update на канальный адрес домашнего агента, инструктируя своего домашнего агента больше не служить ему домашним агентом. При обработке этого сообщения Binding Update домашний агент прекратит защищать домашний адрес мобильного узла процедурой определения дублированного адреса, и не будет больше отвечать на сообщения Neighbor Solicitation с этим домашним адресом мобильного узла. Тогда мобильный узел станет единственным узлом на линке, принимающим пакеты на этот домашний адрес мобильного узла. Кроме того, при возвращении домой до истечения времени текущей привязки для своего домашнего адреса, и конфигурировании своего домашнего адреса на своем сетевом интерфейсе на своем домашнем линке, мобильный узел не должен (MUST) выполнять для своего собственного домашнего адреса процедуру определения дублирования адреса, чтобы избежать путаницы или конфликта с использованием того же самого адреса своим домашним агентом. Это правило применяется также и к производному «локальному для линка» адресу мобильного узла, если бит Link Local Address Compatibility (L) был установлен, когда создавалась привязка. Если мобильный узел возвращается домой после того, как истекли времена привязки для всех его временных адресов, то он должен (SHOULD) выполнять процедуру DAD.

После посылки мобильным узлом сообщения Binding Update, он должен (MUST) подготовиться к ответам на сообщения Neighbor Solicitation для своего домашнего адреса. Эти ответы должны (MUST) посылаться на канальный адрес отправителя, используя индивидуальное сообщение Neighbor Advertisement. Отвечать необходимо, поскольку посылка сообщения Binding Acknowledgement от домашнего агента может потребовать выполнения протокола Neighbor Discovery, и мобильный узел может оказаться не в состоянии различить сообщения Neighbor Solicitation, поступившие от домашнего агента, от других сообщений Neighbor Solicitation. Заметим, что существует условие гонок, при котором как мобильный узел, так и домашний агент отвечают на одни и те же запросы, посланные другими узлами; однако оно будет существовать только временно, до тех пор, пока сообщение Binding Update не будет признано годным.

После приема сообщения Binding Acknowledgement для своего сообщения Binding Update, посланного своему домашнему агенту, мобильный узел должен (MUST) выполнить на домашнем линке групповую рассылку сообщения Neighbor Advertisement (на адрес all-nodes multicast address) [12], чтобы объявить собственный канальный адрес мобильного узла для своего собственного домашнего адреса. В поле Target Address в этом сообщении Neighbor Advertisement должно быть (MUST) установлено значение домашнего адреса мобильного узла, а само объявление должно (MUST) включать опцию Target Link-layer Address, определяющую канальный адрес мобильного узла. Мобильный узел должен (MUST) выполнить групповую рассылку такого сообщения Neighbor Advertisement для каждого из своих домашних адресов, как определялось текущими префиксами на линке, включая его «локальный для линка» адрес и «локальный для сайта» адрес. В этих объявлениях флаг Solicited Flag (S) не должен (MUST NOT) устанавливаться, поскольку никакими сообщениями Neighbor Solicitation они не были запрошены. Флаг Override Flag (O) в этих объявлениях должен (MUST) быть установлен, указывая на то, что объявления должны (SHOULD) аннулировать все существующие элементы кэша соседей в любом принимающем их узле.

Поскольку обычно надежность группового вещания на локальном линке (например, Ethernet) не гарантируется, то для повышения надежности мобильный узел может (MAY) повторно передавать эти сообщения Neighbor Advertisement [12] до MAX_NEIGHBOR_ADVERTISEMENT раз. Существует вероятность, что некоторые узлы на домашнем линке не получат ни одного такого сообщения Neighbor Advertisement, но, в конечном счете, такие узлы могут восстановиться с помощью использования процедуры определения недостижимости соседей [12].

Заметим, что обычно туннель через домашнего агента приостанавливает работу в то же самое время, когда удаляется регистрация в домашнем агенте.

11.6. Процедура обратной маршрутизируемости

В данном разделе определяются правила, которым должен следовать мобильный узел при выполнении процедуры обратной маршрутизируемости. В разд. 11.7.2 описаны правила, когда необходимо инициализировать процедуру обратной маршрутизируемости.

11.6.1. Посылка сообщений Test Init

Мобильный узел, инициирующий процедуру обратной маршрутизируемости, должен (MUST) послать (одновременно) сообщения Home Test Init и Care-of Test Init. Однако, если мобильный узел незадолго до этого принял для требуемых адресов (см. разд. 5.2.7) один или оба маркера home keygen token или care-of keygen token, и связанные с ними индексы одноразовых номеров, он может (MAY) их повторно использовать. Поэтому в некоторых случаях процедура обратной маршрутизируемости может завершиться только одной парой сообщений. Она может завершиться даже вообще без каких-либо сообщений, если мобильный узел имеет свежий (новый) маркер home keygen token и имеет тот же самый ранее посещенный временный адрес так, что он также имеет свежий (новый) маркер care-of keygen token. Если мобильный узел планирует послать обновление привязки с установленным в ноль временем жизни и временным адресом, равным его домашнему адресу – например, в случае возвращения домой - то достаточно посылки сообщения Home Test Init. В этом случае, генерация ключа управления привязкой зависит исключительно от маркера home keygen token (разд. 5.2.5).

Сообщение Home Test Init должно (MUST) создаваться так, как описано в разд. 6.1.3.

Сообщение Care-of Test Init должно (MUST) создаваться так, как описано в разд. 6.1.4. При посылке сообщений Home Test Init или Care-of Test Init мобильный узел должен (MUST) сохранить в своем списке обновлений привязки следующие поля из этих сообщений:

- IP-адрес узла, которому было послано сообщение.
- Домашний адрес мобильного узла. Это значение появится в поле Source Address сообщения Home Test Init. При посылке сообщения Care-of Test Init этот адрес в сообщении не появляется, но представляет домашний адрес, для которого требуется привязка.
- Момент времени, когда были посланы эти сообщения.
- Идентифицирующие цепочки, используемые в сообщениях.

Заметим, что одного сообщения Care-of Test Init может быть достаточно даже когда имеется несколько домашних адресов. В этом случае мобильный узел может (MAY) сохранять одну и ту же информацию в нескольких элементах списка обновлений привязки.

11.6.2. Прием сообщений Test

После получения пакета, переносящего сообщение Home Test, мобильный узел должен (MUST) признать годным пакет в соответствии со следующими проверками:

- Адрес источника пакета принадлежит узлу-корреспонденту, для которого мобильный узел имеет элемент списка обновлений привязки с состоянием, указывающим, что выполняется процедура обратной маршрутизируемости. Заметим, что таких элементов может быть несколько.

- Список обновлений привязки указывает на то, что маркер home keygen token еще не получен.

- Адрес места назначения пакета равен домашнему адресу мобильного узла, и пакет был принят через туннель от домашнего агента.

- Поле Home Init Cookie в сообщении соответствует значению, сохраненному в списке обновлений привязки.

Любое сообщение Home Test, не удовлетворяющее всем этим проверкам, должно (MUST) молча игнорироваться. В противном случае, мобильный узел должен (MUST) сохранить Home Nonce Index и маркер home keygen token в списке обновлений привязки. Если элемент списка обновлений привязки не имеет маркера care-of keygen token, мобильный узел должен (SHOULD) продолжить ожидание сообщения Care-of Test.

После приема пакета, переносящего сообщение Care-of Test, мобильный узел должен (MUST) признать годным пакет в соответствии со следующими правилами:

- Адрес источника пакета принадлежит узлу-корреспонденту, для которого мобильный узел имеет элемент списка обновлений привязки с состоянием, указывающим на то, что выполняется процедура обратной маршрутизируемости. Заметим, что таких элементов может быть несколько.

- Список обновлений привязки указывает на то, что маркер care-of keygen token еще не получен.

- Адрес места назначения пакета равен текущему временному адресу мобильного узла.

- Поле Care-of Init Cookie в сообщении соответствует значению, хранящемуся в списке обновлений привязки.

Любое сообщение Care-of Test, не удовлетворяющее всем этим проверкам должно (MUST) молча игнорироваться. В противном случае, мобильный узел должен (MUST) записать Care-of Nonce Index и маркер care-of keygen token в список обновлений привязки. Если элемент списка обновлений привязки не имеет маркера home keygen token, то мобильный узел должен (SHOULD) продожить ожидание сообщения Home Test.

Если после приема либо сообщения Home Test, либо сообщения Care-of Test и выполнения указанных выше действий элемент списка обновлений привязки имеет оба маркера home keygen token и care-of keygen token, то процедура обратной маршрутизируемости завершена. Тогда мобильный узел должен (SHOULD) продолжить посылку сообщения Binding Update, как описано в разд. 11.7.2.

До момента публикации данной спецификации узлы-корреспонденты могли не поддерживать протокол заголовка мобильности. Такие узлы будут отвечать на сообщения Home Test Init и Care-of Test Init сообщением ICMP Parameter Problem code 1. Мобильный узел должен (SHOULD) принимать такие сообщения как индикацию того, что узел-корреспондент не может обеспечивать оптимизацию маршрутов, и вернуться назад к использованию двунаправленного туннелирования.

11.6.3. Защита пакетов обратной маршрутизируемости

Мобильный узел должен (MUST) поддерживать защиту сообщений Home Test и Home Test Init, как описано в разд. 10.4.6.

Когда для защиты сигнализации обратной маршрутизируемости или пакетов полезных данных используется IPsec, мобильный узел должен (MUST) установить адрес источника, который он использует для исходящих туннельных пакетов, равным текущему основному временному адресу. Мобильный узел начинает использовать новый основной временный адрес немедленно после посылки домашнему агенту сообщения Binding Update для регистрации этого нового адреса.

11.7. Обработка привязок

11.7.1. Посылка сообщений Binding Update домашнему агенту

После принятия решения о смене своего основного временного адреса, как описано в разд. 11.5.1 и 11.5.2, мобильный узел должен (MUST) зарегистрировать этот временный адрес в своем домашнем агенте для того, чтобы сделать его основным временным адресом.

Кроме того, если мобильный узел хочет иметь услуги домашнего агента, выходящие за пределы текущего периода регистрации, мобильный узел задолго до истечения этого периода времени должен послать ему новое сообщение Binding Update, даже если он не меняет своего основного временного адреса. Однако если домашний агент вернул сообщение Binding Acknowledgement для текущей регистрации с полем Status, установленным в 1 (признано действительным, но требуется определение префиксов), то мобильный узел не должен пытаться зарегистрироваться вновь до тех пор, пока он не выяснит пригодность своих домашних префиксов с помощью процедуры определения мобильных префиксов. Это обычно необходимо каждый раз, когда принимается такое значение поля Status, поскольку ранее полученная информация могла измениться.

Для регистрации временного адреса или для увеличения времени жизни существующей регистрации мобильный узел посылает своему домашнему агенту пакет, содержащий сообщение Binding Update, при этом пакет конструируется следующим образом:

- В сообщении Binding Update бит Home Registration (H) должен быть (MUST) установлен.

- В сообщении Binding Update бит Acknowledge (A) должен быть (MUST) установлен.

- Пакет должен (MUST) содержать опцию места назначения Home Address, которая задает для привязки домашний адрес мобильного узла.

- В качестве адреса источника (Source Address) в IPv6-заголовке пакета должен (MUST) использоваться временный адрес для привязки, если только в сообщение Binding Update не включена опция мобильности Alternate Care-of Address. Эта опция должна (MUST) быть включена во все регистрации в домашнем агенте, поскольку протокол ESP не сможет защитить временные адреса в IPv6-заголовке. (Реализации мобильного IPv6, которые знают, что для защиты конкретного сообщения используют IPsec AH, могут обойти эту опцию. Для краткости использование AH в данном документе не обсуждается).

- Если «локальный для линка» адрес мобильного узла имеет тот же самый идентификатор интерфейса, что и домашний адрес, для которого он поставляет новый временный адрес, то мобильный узел должен (SHOULD) установить бит Link-Local Address Compatibility (L).

- Если домашний адрес был сгенерирован на основе RFC 3041 [18], то «локальный для линка» адрес, вероятно, имеет совместимый идентификатор интерфейса. В этом случае мобильный узел должен (MUST) обнулить бит Link-Local Address Compatibility (L).

- Если контексты безопасности IPsec между мобильным узлом и домашним агентом были установлены динамически, и мобильный узел имеет возможность обновить свою оконечную точку в используемом протоколе управления ключами на новый временный адрес каждый раз, когда он перемещается, то мобильный узел должен (SHOULD) в сообщении Binding Update установить бит Key Management Mobility Capability (K). В противном случае, мобильный узел должен (MUST) обнулить этот бит.

- Значение, указанное в поле Lifetime, должно (MUST) быть ненулевым и должно (SHOULD) быть меньше или равно действительно оставшимся временам жизни домашнего адреса и временного адреса, определенных для привязки.

  Мобильные узлы, использующие динамическое определение адреса домашнего агента, должны быть осторожны с использованием продолжительных времен жизни. Если мобильный узел теряет знания о своей привязке с конкретным домашним агентом, то регистрация новой привязки в другом домашнем агенте может оказаться невозможной, поскольку предыдущий домашний агент все еще сохраняет существующую привязку. Поэтому, чтобы гарантировать, что мобильные узлы, использующие процедуру определения адреса домашнего агента, не потеряют информацию о своей привязке, они должны (SHOULD) отменить регистрацию до потери этой информации, или использовать короткие времена жизни.

Бит Acknowledge (A) в сообщении Binding Update требует, чтобы в ответ на данное сообщение домашний агент вернул сообщение Binding Acknowledgement. Как описано в разд. 6.1.8, мобильный узел должен (SHOULD) повторно посылать домашнему агенту это сообщение Binding Update до тех пор, пока он не получит соответствующее сообщение Binding Acknowledgement. Достигнув значения периода таймаута MAX_BINDACK_TIMEOUT, мобильный узел должен (SHOULD) заново начать процесс доставки сообщения Binding Update, но попробовать следующего домашнего агента, возвращенного в процессе динамического определения адресов домашних агентов (см. разд. 11.4.1). Если же существовал только один домашний агент, мобильный узел должен (SHOULD), вместо этого, продолжить периодически повторно передавать сообщение Binding Update на данной скорости до тех пор, пока оно не будет подтверждено (или до тех пор, пока он не начнет попытку зарегистрировать другой основной временный адрес). Относительно повторных передач сообщений Binding Update см. информацию в разд. 11.8.

Своим сообщением Binding Update мобильный узел просит домашнего агента служить ему домашним агентом для данного домашнего адреса. До тех пор, пока не истечет время жизни этой регистрации, домашний агент считает себя домашним агентом для этого домашнего адреса.

Как определено в разд. 5.1, каждое сообщение Binding Update должно (MUST) быть аутентифицировано как пришедшее от правильного мобильного узла. Мобильный узел должен (MUST) использовать свой домашний адрес в сообщениях Binding Update, посылаемых домашнему агенту, – либо в опции места назначения Home Address, либо в поле Source Address IPv6-заголовка. Это необходимо, чтобы предоставить возможность сопоставить политики IPsec с правильным домашним адресом.

При посылке сообщения Binding Update своему домашнему агенту мобильный узел должен (MUST) также создать или обновить соответствующий элемент списка обновлений привязки, как определено в разд. 11.7.2.

Последнее значение порядкового номера, посланное домашнему агенту в сообщении Binding Update, запоминается мобильным узлом. Если посылающий мобильный узел не знает правильного значения порядкового номера, он может начать с любого значения. Если домашний агент бракует это значение, то он посылает назад сообщение Binding Acknowledgement с кодом состояния 135 и последний одобренный порядковый номер в поле Sequence Number сообщения Binding Acknowledgement. Мобильный узел должен (MUST) сохранить эту информацию и использовать для следующего посылаемого им обновления привязки следующее значение порядкового номера.

Если мобильный узел имеет дополнительные домашние адреса, то для регистрации временного адреса он должен (SHOULD) для каждого такого домашнего адреса послать своему домашнему агенту дополнительный пакет, содержащий сообщение Binding Update.

Домашний агент будет выполнять процедуру DAD для домашнего адреса мобильного узла только тогда, когда мобильный узел поставил правомерную привязку между

своим домашним адресом и временным адресом. Если проходит какое-то время, в течение которого мобильный узел не имеет привязки в домашнем агенте, то имеется вероятность того, что другой узел выполнит автоконфигурирование этого домашнего адреса мобильного узла. Поэтому, мобильный узел должен (MUST) рассматривать создание новой привязки в домашнем агенте, используя существующий домашний адрес, точно так же, как создание нового домашнего адреса. В маловероятной ситуации, когда происходит автоконфигурирование домашнего адреса мобильного узла в качестве IPv6-адреса другого сетевого узла в домашней сети, домашний агент ответит на последующее сообщение Binding Update сообщением Binding Acknowledgement, содержащим поле Status равным 134 (Duplicate Address Detection failed – проверка на дублирование адреса не прошла). В этом случае мобильный узел не должен (MUST NO) пытаться повторно использовать тот же самый домашний адрес. Он должен (SHOULD) продолжить регистрацию временных адресов для своих других домашних адресов, если таковые имеются. (Механизмы, обрисованные в Приложении B.5, в будущем могут позволить мобильным узлам обзавестись новыми домашними адресами, чтобы заменить один из тех адресов, для которых было получено состояние 134).

11.7.2. Регистрация в узле-корреспонденте

Когда мобильный узел уверен в том, что его домашний адрес является годным, он может инициировать регистрацию в узле-корреспонденте с целью разрешения узлу-корреспонденту кэшировать текущий временный адрес мобильного узла. Эта процедура включает процедуру обратной маршрутизируемости, за которой следует регистрация.

В данном разделе определено, когда должна инициироваться регистрация в узле-корреспонденте, и правила, которым необходимо следовать во время ее выполнения.

После того, как мобильный узел послал сообщение Binding Update домашнему агенту, регистрируя свой новый основной временный адрес (как описано в разд. 11.7.1), мобильный узел должен (SHOULD) инициировать регистрацию в узле-корреспонденте для каждого узла, который уже имеется в списке обновлений привязки мобильного узла. Запускаемые процедуры могут использоваться либо для обновления, либо для удаления информации о привязке в узле-корреспонденте.

Для тех узлов, которые отсутствуют в списке обновлений привязки мобильного узла, мобильный узел может (MAY) инициировать регистрацию в узле-корреспонденте в любой момент времени после посылки сообщения Binding Update своему домашнему агенту.

Соображения относительно того, когда (и при каких условиях) инициировать эту процедуру, зависят от конкретного перемещения и характера трафика мобильного узла и выходят за рамки данного документа.

Кроме того, мобильный узел может (MAY) инициировать регистрацию в узле-корреспонденте в ответ на получение пакета, который удовлетворяет всем следующим проверкам:

- Пакет был туннелирован с использованием IPv6-инкапсуляции.
- Адрес места назначеия в туннельном (внешнем) IPv6-заголовке равен любому из временных адресов мобильного узла.
- Адрес места назначеия в оригинальном (внутреннем) IPv6-заголовке равен любому из домашних адресов мобильного узла.
- Адрес источника в туннельном (внешнем) IPv6-заголовке отличается от адреса источника в оригинальном (внутреннем) IPv6-заголовке.
- Пакет не содержит сообщений Home Test, Home Test Init, Care-of Test или Care-of Test Init.

Если мобильный узел имеет несколько домаших адресов, то для использования в регистрации в узле-корреспонденте важно выбрать правильный адрес. Используемый домашний адрес должен (MUST) быть адресом места назначения оригинального (внутреннего) пакета.

Адрес партнера, используемый в этой процедуре, должен (MUST) определяться следующим образом:

- Если в оригинальном (внутреннем) пакете опция места назначения Home Address присутствует, то используется адрес из этой опции.

- В противном случае, используется адрес источника в оригинальном (внутреннем) IPv6-заголовке пакета.

Заметим, что законность (правильность) оригинального пакета проверяется до попытки инициирования регистрации в узле-корреспонденте. Например, если в оригинальном пакете имеется опция места назначения Home Address, то применяются правила из разд. 9.3.1.

Мобильный узел может (MAY) также принять решение сохранить свое топологическое местоположение в секрете от некоторых узлов-корреспондентов, и, таким образом, не нуждается в инициировании регистрации в узле-корреспонденте.

После успешного завершения процедуры обратной маршрутизируемости, а также после получения от домашнего агента успешного сообщения Binding Acknowledgement, узлу-корреспонденту может (MAY) быть послано сообщение Binding Update.

В любом сообщении Binding Update, посылаемом мобильным узлом, временный адрес (либо адрес источника в IPv6-заголовке пакета, либо временный адрес в опции мобильности Alternate Care-of Address данного сообщения Binding Update) должен (MUST) быть установлен равным одному из временных адресов, используемому мобильным узлом в настоящий момент времени, или домашнему адресу мобильного узла. Для посылки сообщений Binding Update различным узлам-корреспондентам мобильный узел может (MAY) установить временный адрес по-разному.

Мобильный узел может (MAY) также послать такому узлу-корреспонденту сообщение Binding Update, отдавая ему распоряжение удалить любую существующую привязку для мобильного узла из его кэша привязок, как описано в разд. 6.1.7. Даже в этом случае, сначала требуется успешное завершение процедуры обратной маршрутизируемости.

Если временный адрес не установлен равным домашнему адресу мобильного узла, то сообщение Binding Update требует, чтобы узел-корреспондент создал или обновил для этого мобильного узла элемент кэша привязок в узле-корреспонденте. Это делается для того, чтобы сохранить временный адрес для использования при посылке будущих пакетов мобильному узлу. В этом случае значение, указанное в поле Life-time и посылаемое в сообщении Binding Update, должно быть (SHOULD) меньше или равно оставшемуся времени жизни регистрации в домашнем агенте и временного адреса, указанного для привязки. Временный адрес, заданный в сообщении Binding Update, может (MAY) отличаться от основного временного адреса мобильного узла.

Если сообщение Binding Update посылается узлу-корреспонденту, требуя стирания любого существующего элемента кэша привязок, который он имеет для этого мобильного узла, то временный адрес устанавливается равным домашнему адресу мобильного узла, а поле Lifetime устанавливается в ноль. В этом случае генерация ключа управления привязкой зависит исключительно от маркера home keygen token (разд. 5.2.5). В этом случае индекс одноразового номера care-of nonce index должен (SHOULD) быть установлен в ноль. При соблюдении указанных ниже правил создания сообщений Binding Update временный адрес должен (MUST) быть установлен равным домашнему адресу, если мобильный узел находится дома, или текущему временному адресу, если он находится вне дома.

Если мобильный узел хочет иметь гарантию того, что его новый временный адрес был записан в кэш привязок узла-корреспондента, он должен потребовать подтверждения путем установки в сообщение Binding Update бита Acknowledge (A).

Сообщение Binding Update создается следующим образом:

- Текущий временный адрес мобильного узла должен (MUST) посылаться либо в поле Source Address IPv6-заголовка, либо в опции мобильности Alternate Care-of Address.

- Поле Destination Address IPv6-заголовка должно (MUST) содержать адрес узла-корреспондента.

- Заголовок мобильности конструируется в соответствии с правилами из разд. 6.1.7 и 5.2.6, включая поле Binding Authorization Data (вычисленное, как определено в разд. 6.2.7), и возможно опции мобильности Nonce Indices.

- К пакету в опции места назначения Home Address должен (MUST) быть добавлен домашний адрес мобильного узла, если только поле Source Address не является этим домашним адресом.

Каждое сообщение Binding Update должно (MUST) иметь порядковый номер больший, чем значение Sequence Number, посланное в предыдущем сообщении Binding Update на тот же самый адрес места назначения (если оно было). Порядковые номера сравниваются по модулю 2**16, как описано в разд. 9.5.1. Однако отсутствует требование на то, чтобы порядковый номер строго увеличивался на 1 при каждой посылке или приеме нового сообщения Binding Update до тех пор, пока это значение находится внутри окна. Последнее значение порядкового номера, посланное на некоторое место назначения в сообщении Binding Update, сохраняется мобильным узлом в его элементе списка обновлений привязки для данного места назначения. Если посылающий мобильный узел не имеет элемента списка обновлений привязки, порядковый номер должен (SHOULD) начинаться со случайного значения. Мобильный узел не должен (MUST NOT) использовать тот же самый порядковый номер в двух различных сообщениях Binding Update для одного и того же узла-корреспондента, даже если эти сообщения Binding Update предоставляют различные временные адреса.

Мобильный узел несет ответственность за завершение регистрации в узле-корреспонденте, а так же за любые повторные передачи, которые могут потребоваться (предмет для ограничения скорости, определенного в разд. 11.8).

11.7.3. Прием сообщений Binding Acknowledgement

После приема пакета, переносящего сообщение Binding Acknowledgement, мобильный узел должен (MUST) признать пакет годным в соответствии со следующими проверками:

- Пакет соответствует требованиям аутентификации для сообщений Binding Acknowledgement, определенным в разд. 6.1.8 и 5. А именно, если сообщение Binding Update было послано домашнему агенту, то используется лежащая в основе защита IPsec. Если сообщение Binding Update было послано узлу-корреспонденту, то должна (MUST) присутствовать и иметь правомерное значение опция мобильности Binding Authorization Data.

- Опция мобильности Binding Authorization Data, если присутствует, должна (MUST) быть последней опцией и не должна (MUST) иметь замыкающего заполнения.

- Поле Sequence Number соответствует полю Sequence Number, посланному мобильным узлом на этот адрес места назначения в исходящем сообщении Binding Update.

Любое сообщение Binding Acknowledgement, которое не удовлетворяет всем этим проверкам должно(MUST) молча игнорироваться.

Когда мобильный узел получает пакет, переносящий правомерное сообщение Binding Acknowledgement, он должен (MUST) проверить поле Status следующим образом:

- Если поле Status указывает на то, что сообщение Binding Update было признано годным (значение поля Status меньше 128), то мобильный узел должен (MUST) обновить соответствующий элемент в своем списке обновлений привязки для указания того, что сообщение Binding Update было подтверждено; тогда мобильный узел должен (MUST) прекратить посылку повторных сообщений Binding Update. Кроме того, если значение, указанное в поле Lifetime сообщения Binding Acknowledgement, меньше значения поля Lifetime, посланного в сообщении Binding Update, которое подтверждается, то мобильный узел должен (MUST) вычесть разницу между этими двумя значениями времени жизни из оставшегося времени жизни привязки, которое поддерживается в соответствующем элементе списка обновлений привязки (с минимальным значением времени жизни для элемента списка обновлений привязки, равным 0). Т.е., если значение времени жизни, посланное в сообщении Binding Update, было равно L_update, значение времени жизни, полученное в сообщении Binding Acknowledgement было равно L_ack, а текущее значение оставшегося времени жизни элемента списка обновлений привязки составляет L_remain, то новое значение оставшегося времени жизни элемента списка обновлений привязки должно стать равным

  max((L_remain - (L_update - L_ack)), 0)

  где max(X, Y) равно максимальному из значений X или Y. Результат этого шага заключается в том, чтобы правильно, с точки зрения мобильного узла, управлять оставшимся временем жизни привязки (которое поддерживается в соответствующем элементе списка обновлений привязки) так, чтобы оно правильно учитывало значение времени жизни, заданное в сообщении Binding Acknowledgement, но с учетом отсчета таймера, который начинал работать во время посылки сообщения Binding Update.

  Чтобы продлить время жизни, мобильные узлы должны (SHOULD) посылать новое сообщение Binding Update задолго до истечения этого периода времени. Это позволяет избежать нарушений связи, которые в противном случае могут стать причиной сетевых задержек или смещения времени.

- Кроме того, если значение поля Status равно 1 (accepted but prefix discovery necessary - признано действительным, но требуется определение префиксов), мобильный узел должен (SHOULD) послать сообщение Mobile Prefix Solicitation, чтобы обновить свою информацию относительно доступных префиксов.

- Если поле Status указывает на то, что сообщение Binding Update было признано негодным (значение поля Status больше или равно 128), то мобильный узел может предпринять шаги для устранения причины ошибки и повторной передачи сообщения Binding Update (с новым значением порядкового номера), что является предметом ограничения скорости, описанного в разд. 11.8. Если это не делается или не удается сделать, то мобильный узел в своем списке обновлений привязки должен отметить, что на это место назначения будущие сообщения Binding Update посылаться не должны (SHOULD NOT).

Обработка опции мобильности Binding Refresh Advice в сообщении Binding Acknowledgement зависит от того, откуда пришло подтверждение. Эта опция должна (MUST) игнорироваться, если подтверждение пришло от узла-корреспондента. Если оно пришло от домашнего агента, то мобильный узел использует поле Refresh Interval в этой опции как указание того, что он должен (SHOULD) пытаться обновлять свою регистрацию в домашнем агенте с указанным более коротким периодом времени.

Если подтверждение пришло от домашнего агента, то мобильный узел проверяет значение бита Key Management Mobility Capability (K). Если этот бит не установлен, мобильный узел должен (SHOULD) отказаться от соединений протокола управления ключами с домашним агентом, если они были. Мобильный узел может (MAY) также инициировать новое соединение управления ключами.

Если этот бит установлен, то мобильный узел должен (SHOULD) перенести свою собственную оконечную точку в соединениях протокола управления ключами, если они были. Новой оконечной точкой мобильного узла должен быть новый временный адрес. Для соединения фазы 1 IKE это означает, что пакеты, посылаемые на этот адрес с оригинальными идентифицирующими цепочками ISAKMP, считаются приемлемыми.

11.7.4. Прием сообщений Binding Refresh Request

Если мобильный узел получает пакет, содержащий сообщение Binding Refresh Request, данный мобильный узел имеет элемент списка обновлений привязки для источника этого сообщения, и данный мобильный узел хочет сохранить свой элемент кэша привязок в узле-корреспонденте, то мобильный узел должен запустить процедуру обратной маршрутизируемости. Если мобильный узел хочет удалить свой элемент кэша привязок, он может либо игнорировать запрос Binding Refresh Request и дождаться таймаута привязки, либо он может в любой момент времени уничтожить свою привязку в узле-корреспонденте посредством явного обновления привязки с нулевым временем жизни и временным адресом, установленным равным домашнему адресу. Если мобильный узел не знает, нужен ли ему элемент кэша привязок, он может принять решение способом, зависящим от реализации, например, основанным на доступных ресурсах.

Заметим, что мобильный узел должен осторожно относиться к вопросу о том, чтобы не отвечать на запросы Binding Refresh Request для адресов, отсутствующих в списке обновлений привязки, чтобы избежать возможности стать объектом атак типа «отказ в обслуживании».

Если процедура обратной маршрутизируемости завершается успешно, сообщение Binding Update должно (SHOULD) быть послано, как описано в разд. 11.7.2. Поле Lifetime в этом сообщении Binding Update должно (SHOULD) быть установлено равным новому времени жизни, расширяющему любое текущее время жизни, оставшееся от предыдущего сообщения Binding Update, посланного этому узлу (которое указывается в любом существующем элементе списка обновлений привязки для этого узла), и это время жизни снова должно (SHOULD) быть меньше или равно оставшемуся времени жизни регистрации в домашнем агенте и временного адреса, определенного для привязки. При посылке этого сообщения Binding Update мобильный узел должен (MUST) обновить свой список обновлений привязки тем же самым способом, что и для любого другого сообщения Binding Update, посылаемого мобильным узлом.

11.8. Повторные передачи и ограничение скорости

Мобильный узел несет ответственность за повторные передачи и ограничение скорости при выполнении процедуры обратной маршрутизируемости, регистраций и запрашиваемых определений префиксов.

Когда мобильный узел посылает сообщение Mobile Prefix Solicitation, Home Test Init, Care-of Test Init или Binding Update, для которого он ожидает ответ, он должен определить значение таймера для первой повторной передачи:

- Если мобильный узел посылает сообщение Mobile Prefix Solicitation, он должен (SHOULD) использовать интервал первой повторной передачи, равный INITIAL_SOLICIT_TIMER (см. разд. 12).

- Если мобильный узел посылает сообщение Binding Update и не имеет существующей привязки в домашнем агенте, то он должен (SHOULD) использовать в качестве значения таймера для первой повторной передачи InitialBindackTimeoutFirstReg (см разд. 13). Этот длинный интервал повторной передачи позволит домашнему агенту завершить процедуру определения дублирования адреса (DAD), которая в этом случае, как подробно описывается в разд. 11.7.1, является обязательной.

- В противном случае, мобильный узел должен использовать в качестве значения таймера для первой повторной передачи специфицированное значение INITIAL_BINDACK_TIMEOUT.

Если мобильному узлу не удалось получить соответствующий правомерный ответ в течение выбранного первого интервала повторной передачи, он должен (SHOULD) повторно передавать сообщение до тех пор, пока ответ не будет получен.

Повторные передачи, выполняемые мобильным узлом, должны (MUST) использовать процесс экспоненциальной отсрочки, при котором период таймаута удваивается после каждой повторной передачи до тех пор, пока либо узел не получит ответ, либо период таймаута не достигнет значения MAX_BINDACK_TIMEOUT. Мобильный узел может (MAY) бесконечно продолжать посылать эти сообщения с такой малой скоростью.

Мобильный узел должен начинать отдельный процесс отсрочки для различных типов сообщений, различных домашних адресов и различных временных адресов. Однако, кроме того, для сообщений, посылаемых конкретному узлу-корреспонденту, применяется ограничение суммарной скорости. Это гарантирует, что узел-корреспондент будет иметь достаточное количество времени, чтобы ответить в случае, когда, например, регистрируются привязки для нескольких домашних адресов. Мобильный узел не должен (MUST NOT) посылать сообщения мобильного заголовка определенного типа конкретному узлу-корреспонденту чаще MAX_UPDATE_RATE раз в секунду.

Повторно посланные сообщения Binding Update должны (MUST) использовать значения порядкового номера большие, чем использовались для предыдущей передачи этого сообщения Binding Update. Повторно посылаемые сообщения Home Test Init и Care-of Test Init должны (MUST) использовать новые значения идентифицирующих цепочек.

12. Протокольные константы

DHAAD_RETRIES	4 повторные передачи
INITIAL_BINDACK_TIMEOUT	1 секунда
INITIAL_DHAAD_TIMEOUT	3 секунды
INITIAL_SOLICIT_TIMER	3 секунды
MAX_BINDACK_TIMEOUT	32 секунды
MAX_NONCE_LIFETIME	240 секунд
MAX_TOKEN_LIFETIME	210 секунд
MAX_RR_BINDING_LIFETIME	420 секунд
MAX_UPDATE_RATE	3 раза
PREFIX_ADV_RETRIES	3 повторные передачи
PREFIX_ADV_TIMEOUT	3 секунды

13. Переменные конфигурирования протокола

MaxMobPfxAdvInterval	По умолчанию: 86,400 секунд
MinDelayBetweenRAs	По умолчанию: 3 секунды, Минимально: 0.03 секунды
MinMobPfxAdvInterval	По умолчанию: 600 секунд
InitialBindackTimeoutFirstReg	По умолчанию: 1.5 секунды

Домашние агенты должны (MUST) позволять конфигурировать три первые переменные с помощью управления системой, а мобильные узлы должны (MUST) позволять конфигурировать последнюю переменную с помощью управления системой.

Подразумеваемое значение (значение по умолчанию) для переменной InitialBindack-TimeoutFirstReg было вычислено как полуторакратное значение (x 1.5) произведения значения по умолчанию RetransTimer [12] на значение по умолчанию DupAddrDe-tectTransmits [13].

Значение MinDelayBetweenRAs аннулирует значение протокольной константы MIN_DELAY_BETWEEN_RAS, как описано в RFC 2461 [12]. Эта переменная должна (SHOULD) быть установлена равной MinRtrAdvInterval, если MinRtrAdvInterval меньше, чем 3 секунды.

14. Соображения IANA

Данный документ определяет новый IPv6-протокол, заголовок мобильности, описанный в разд. 6.1. Этому протоколу присвоен номер 135.

Данный документ создает также новое пространство имен "Mobility Header Type" (тип мобильного заголовка), для поля MH Type в заголовке мобильности. Текущие типы сообщений описываются, начиная с разд. 6.1.2, и являются следующими:

0 Binding Refresh Request

1 Home Test Init

2 Care-of Test Init

3 Home Test

4 Care-of Test

5 Binding Update

6 Binding Acknowledgement

7 Binding Error

Будущие значения поля MH Type могут распределяться с помощью процесса стандартизации или с санкции IESG [10].

Более того, каждое сообщение мобильности может содержать опции мобильности, как описано в разд. 6.2. Для идентификации этих опций данный документ определяет новое пространство имен "Mobility Option" (опция мобильности). Текущие опции мобильности определяются, начиная с разд. 6.2.2, и являются следующими:

0 Pad1

1 PadN

2 Binding Refresh Advice

3 Alternate Care-of Address

4 Nonce Indices

5 Authorization Data

Будущие значения типа опций могут распределяться с помощью процесса стандартизации или с санкции IESG [10].

Наконец, данный документ создает третье пространство имен "Status Code" (код статуса) для поля Status в сообщении Binding Acknowledgement. Текущие значения описываются в разд. 6.1.8, и являются следующими:

0 Binding Update accepted

1 Accepted but prefix discovery necessary

128 Reason unspecified

129 Administratively prohibited

130 Insufficient resources

131 Home registration not supported

132 Not home subnet

133 Not home agent for this mobile node

134 Duplicate Address Detection failed

135 Sequence number out of window

136 Expired home nonce index

137 Expired care-of nonce index

138 Expired nonces

139 Registration type change disallowed

Будущие значения поля Status могут распределяться с помощью процесса стандартизации или с санкции IESG [10].

Все поля, помеченные как "Reserved" (зарезервировано) могут распределяться только с помощью процесса стандартизации или с санкции IESG.

Данный документ определяет также новую IPv6-опцию места назначения, опцию Home Address, описанную в разд. 6.3. Этой опции присвоено значение типа опции 0xC9.

Данный документ определяет также новый тип 2 заголовка маршрутизации IPv6, описанный в разд. 6.4. Значение 2 назначено IANA.

Кроме того, данный документ определяет четыре типа сообщений ICMP, из которых два использовались как часть механизма динамического определения адресов домашних агентов, а два других использовались вместо запросов маршрутизатора и объявлений маршрутизатора, когда мобильный узел находится вне домашнего линка. Этим сообщениям присвоены номера типов ICMPv6 из диапазона информационных сообщений:

- Сообщение Home Agent Address Discovery Request, описанное в разд. 6.5;

- Сообщение Home Agent Address Discovery Reply, описанное в разд. 6.6;

- Сообщение Mobile Prefix Solicitation, описанное в разд. 6.7, и

- Сообщение Mobile Prefix Advertisement, описанное в разд. 6.8.

Данный документ определяет также две новых опции протокола Neighbor Discovery [12], которым присвоены значения типа опций в рамках пространства нумерации опций сообщений Neighbor Discovery:

Опция Advertisement Interval, описанная в разд. 7.3; и

Опция Home Agent Information, описанная в разд. 7.4.

15. Соображения по безопасности

15.1. Угрозы

Любое мобильное решение должно защищать себя от неправильного использования функций и механизмов мобильности. В мобильном IPv6 большинство потенциальных угроз связано с поддельными привязками, обычно приводящими к атакам типа «отказ в обслуживании» (Denial-of-Service). Некоторые угрозы представляют потенциал для атак типа «человек посередине» (Man-in-the-Middle), «хищение» (Hijacking), «нарушение конфиденциальности» (Confidentiality) и «имитация» (Impersonation). Данный протокол защищает от следующих основных угроз:

- Угрозы, связанные с сообщениями Binding Update, которые посылаются домашним агентам и узлам-корреспондентам. Например, злоумышленник может заявить, что определенный мобильный узел в настоящее время находится в другом месте, отличном от его реального местоположения. Если домашний агент воспримет такую посланную ему подложную информацию, то мобильный узел не сможет получать предназначенный для него трафик. Подобным образом, злонамеренный (мобильный) узел может использовать домашний адрес узла-жертвы в ложном сообщении Binding Update, посылаемом узлу-корреспонденту.

  Эти угрозы представляют собой угрозы конфиденциальности, целостности и доступности. То есть, злоумышленник может узнать содержимое пакетов, предназначенных для другого узла, путем переадресации трафика к самому себе. Более того, злоумышленник может использовать переадресованные пакеты и попытаться поставить самого себя в качестве «человека посередине» между мобильным узлом и узлом-корреспондентом. Это позволит злоумышленнику имитировать мобильный узел, что приведет к проблемам целостности и доступности.

  Злонамеренный (мобильный) узел может также послать сообщения Binding Update, в которых временный адрес заменен адресом узла-жертвы. Если такие сообщения Binding Update были восприняты, то злонамеренный узел может спровоцировать узел-корреспондент на посылку узлу-жертве потенциально большого объема данных; ответы узла-корреспондента на сообщения, посылаемые злонамеренным мобильным узлом, будут посылаться жертве-хосту или жертве-сети. Это может использоваться для того, чтобы стать причиной атаки типа «распределенного отказа в обслуживании» (Distributed Denial-of-Service). Например, узел-корреспондент может быть сайтом, который будет посылать широкополосный поток видео данных любому, кто об этом его попросит. Заметим, что использование протоколов с управлением потоком, таких как TCP, необязательно защищает против такого типа атаки, поскольку злоумышленник может подделывать и подтверждения. Не помогает даже хранение в секретном виде начальных порядковых номеров TCP, поскольку злоумышленник может получить несколько первых сегментов (включая начальный порядковый номер) на свой собственный адрес, и только после этого переадресовать поток на адрес жертвы. Эти типы атак могут быть направлены на сети, а не на узлы. Другие разновидности подобной угрозы описаны в [27, 34].

  Злоумышленник может также попытаться нарушить обмены мобильного узла путем повторного воспроизведения сообщения Binding Update, которое этот узел посылал раньше. Если старое сообщение Binding Update было воспринято, то пакеты, предназначенные для мобильного узла, будут посылаться на его старое, а не на новое местоположение.

  В заключение отметим, что имеются угрозы атак типа «отказ в обслуживании», «человек посередине», «нарушение конфиденциальности» и «имитация» сторнам, вовлеченным в посылку легальных (законных) сообщений Binding Update, а также угрозы атак типа «отказ в обслуживании» для любой другой стороны.

- Угрозы, связанные с пакетами полезных данных: Пакеты полезных данных, обмен которыми осуществляется мобильными узлами, не защищены от тех же самых угроз, что и весь нормальный трафик IPv6. Однако протокол мобильного IPv6 вводит дополнительную опцию места назначения «Home Address», новый тип заголовка маршрутизации (тип 2), и использует заголовки туннелирования в пакетах полезных данных. Протокол должен защищать от новых потенциальных угроз, связанных с использованием этих механизмов.

  В результате применения опции места назначения «Home Address» третьи стороны становятся подверженными угрозам «отражения», если только не следовать соответствующим мерам предосторожности. Опция места назначения «Home Address» может использоваться для указания необходимости посылки ответного трафика в направении узла, IP-адрес которого находится в опции. В этом случае входная фильтрация не будет обнаруживать поддельный «адрес возврата» [36, 32].

  Подобная угроза существует и для туннелей между мобильным узлом и домашним агентом. Злоумышленник может подделать туннелируемые между мобильным узлом и домашним агентом пакеты так, что будет казаться, что трафик приходит от мобильного узла, хотя это не верно. Заметим, что злоумышленник, который может подделывать туннелируемые пакеты, обычно способен также подделывать пакеты, которые кажутся приходящими непосредственно от мобильного узла. Как таковая, это не новая угроза. Однако для злоумышленника может оказаться проще избежать обнаружения путем обхода механизмов входной фильтрации и отслеживания пакетов. Более того, поддельные туннелируемые пакеты могут использоваться для получения доступа к домашней сети.

  Наконец, заголовок маршрутизации может также использоваться в атаках типа «отражение», а также в атаках, созданных для обхода межсетевых экранов. Он также позволит отражать трафик на другие узлы. Эти угрозы вообще существуют при использовании заголовков маршрутизации, даже если их использование, которого требует протокол мобильного IPv6, вполне надежно.

- Угрозы, связанные с динамическим определением домашнего агента и мобильного префикса.

- Угрозы, связанные с самими механизмами безопасности мобильного IPv6: Злоумышленник может, например, спровоцировать участников на выполнение дорогостоящих криптографических операций или на выделение памяти с целью сохранения состояния. У узла-жертвы не останется ресурсов для выполнения других задач.

  Ожидается, что мобильный IPv6, в качестве базисной службы стека IPv6, будет развернут в большинстве узлов IPv6 Internet. Поэтому указанные выше угрозы должны рассматриваться в свете применения к Internet в целом.

  Следует также заметить, что некоторые дополнительные угрозы поисходят из-за перемещений как таковых, даже без вовлечения протоколов мобильности. Мобильные узлы должны быть способными защищать сами себя в сетях, которые они посещают, поскольку применяемые в домашней сети обычные средства защиты периметра больше их не защищают.

15.2. Функции

Данная спецификация представляет комплект функций, разработанных для уменьшения риска, связанного с перечисленными выше угрозами. Основные функции безопасности следующие:

- Обратное туннелирование, как обязательная функция.
- Защита сообщений Binding Update, посылаемых домашним агентам.
- Защита сообщений Binding Update, посылаемых узлам-корреспондентам.
- Защита от атак отражения, которые используют опцию места назначения «Home Address».

- Защита туннелей между мобильным узлом и домашним агентом.
- Закрытие уязвимостей заголовка маршрутизации.
- Уменьшение угроз типа «отказ в обслуживании» для самих механизмов безопасности мобильного IPv6.

Поддержка зашифрованного обратного туннелирования (см. разд. 11.3.1) позволяет мобильным узлам ликвидировать некоторые виды анализа трафика.

Защита сообщений Binding Update, которые посылаются домашнему агенту, и сообщений Binding Update, которые посылаются произвольным узлам-корреспондентам, требует совершенно различных решений по безопасности из-за различия ситуаций. Мобильные узлы и домашние агенты естественно предполагаются предметом сетевого администрирования домашнего домена.

Таким образом, они могут иметь, и предполагается, что они имеют контекст безопасности (security association), который может быть использован для надежной аутентификации обмениваемых сообщений. См. разд. 5.1 для описания протокольных механизмов и ниже разд. 15.3 для обсуждения достигнутого в результате уровня безопасности.

Ожидается, что оптимизация маршрутов мобильного IPv6 будет использоваться в глобальном масштабе между узлами, принадлежащими различным административным доменам. Очень нужной задачей станет построение инфраструктуры аутентификации такого масштаба. Более того, традиционную инфраструктуру аутентификации нельзя будет просто использовать для аутентификации IP-адресов, поскольку IP-адреса могут часто меняться. Просто аутентифицировать мобильные узлы не достаточно. Чтобы заявить право на использование адреса, требуется также авторизация. Таким образом, необходим подход, который можно назвать «отсутствием инфраструктуры». Выбранный безифраструктурный метод описывается в разд. 5.2, а в разд. 15.4 обсуждается достигнутый в результате уровень безопасности и логическое объяснение этого подхода.

Специальные правила определяют использование опции места назначения Home Address, заголовка маршрутизации, а также заголовков туннелирования в пакетах полезных данных. Эти правила необходимы для того, чтобы убрать уязвимости, связанные с их неограниченным использованием. Последствия этих правил обсуждаются в разделах 15.7, 15.8 и 15.9.

Угрозы типа «отказ в обслуживании», связанные с самими механизмами безопасности мобильного IPv6, касаются, главным образом, процедур обновления привязки в узле-корреспонденте. Как будет описано в разд. 15.4.5, протокол разработан с целью ограничения последствий такого рода атак.

15.3. Сообщения Binding Update, посылаемые домашнему агенту

Сигнализация между мобильным узлом и домашним агентом требует целостности сообщений. Это необходимо, чтобы предоставить домашнему агенту гарантию того, что сообщение Binding Update получено от легитимного мобильного узла. Кроме того, дополнительно требуются правильное упорядочивание и защита от воспроизведения.

IPsec ESP защищает целостность сообщений Binding Update и Binding Acknowledgement путем обеспечения безопасности сообщений между мобильным узлом и домашним агентом.

IPsec может обеспечить защиту от повторного воспроизведения (anti-replay protection) только если используется динамическое управление ключами (keying) (что не всегда имеет место). IPsec также не гарантирует правильного упорядочивания пакетов, а только то, что они повторно не воспроизводятся. В этой связи, чтобы гарантировать правильное упорядочивание, в сообщениях мобильного IPv6 используются порядковые номера (см. разд. 5.1). Однако если 16-битовое пространство порядковых номеров мобильного IPv6 зацикливается, или домашний

агент перезапускается и теряет свое состояние, относящееся к порядковым номерам, атаки, связанные с повторным воспроизведением и переупорядочиванием, становятся возможными. В совокупности использование механизмов динамического управления ключами, защиты от повторного воспроизведения IPsec и порядковых номеров мобильного IPv6 может воспрепятствовать проведению подобного рода атак. Кроме того, домашним агентам, чтобы избежать потери их состояния, рекомендуется использовать энергонезависимую память.

Для порядковых номеров используется схема скользящего окна. Защита от атак, связанных с повторным воспроизведением и переупорядочиванием без механизма управления ключами, работает, когда злоумышленник запоминает максимально до 2**15 обновлений привязки.

Указанные выше механизмы не показывают, что временный адрес, находящийся в обновлении привязки, является корректным. Это дает возможность проведения атак типа «отказ в обслуживании» против третьих сторон. Однако, поскольку мобильный узел и домашний агент имеют контекст безопасности, домашний агент может всегда идентифицировать мобильный узел со зловредным поведением. Это позволяет оператору домашнего агента прекратить обслуживание мобильного узла и, возможно, предпринять дальнейшие акции, опираясь на деловые отношения с владельцем мобильного узла.

Заметим, что использование одной пары контекстов безопасности, управляемых вручную, противоречит формированию новых домашних адресов [18] для мобильного узла, или принятию нового префикса домашней подсети. Это происходит потому, что контексты безопасности IPsec привязаны к используемым адресам. В то время как основанное на сертификатах автоматическое управление ключами в некоторой степени смягчает эту проблему, все еще необходимо гарантировать, что данный мобильный узел не может посылать сообщения Binding Update для адреса другого мобильного узла. В общем случае это приводит к включению домашних адресов в поле Subject AltNam сертификатов. Это снова ограничивает введение новых адресов либо без ручных, либо без автоматических процедур для создания новых сертификатов. Поэтому, данная спецификация ограничивает формирование новых домашних адресов (по любым причинам) теми ситуациями, когда контекст безопасности или сертификат для нового адреса уже существуют. (В приложении B.4 перечислены улучшения системы безопасности для новых адресов, как одно из направлений будущего развития мобильного IPv6).

Поддержка IKE определяется как факультативная возможность. Что касается использования ручного управления ключами, то необходимо обратить внимание на следующее:

- Как обсуждалось выше, при ручном управлении ключами IPsec существует только ограниченная форма защиты от атак воспроизведения и переупорядочивания. В системе защиты существуют слабые места, если либо зацикливается пространство порядковых номеров, либо домашний агент перезагружается и забывает свои порядковые номера (и не использует энергозависимую память для хранения порядковых номеров).

  Если предположить, что мобильный узел постоянно перемещается через каждые 10 минут, то пройдет примерно 455 дней прежде, чем пространство порядковых номеров зациклится. Сегодняшние примеры типовой частоты перемещения редко достигают такого значения.

- Мобильный узел и его домашний агент принадлежат одному и тому же домену. Если бы это было не так, ручное управление было бы невозможным [28], но в мобильном IPv6 только эти две стороны должны знать ключи, сконфигурированные вручную. Подобным образом, мы замечаем, что мобильный IPv6 в IPsec применяет стандартные блочные шифры, и не уязвим для проблем, связанных с поточными шифрами и ручной манипуляцией.

- Предполагается, что владелец мобильного узла и администратор домашнего агента договорились об используемых ключах и других параметрах с помощью некоторого независимого механизма.

Использование IKEv1 в мобильном IPv6 более подробно документировано в [21]. Относительно использования IKEv1 необходимо обратить внимание на следующее:

- Необходимо не допускать того, чтобы мобильный узел предъявлял домашний адрес другого мобильного узла. Домашний агент должен проверить, что мобильный узел, пытающийся согласовать SA для конкретного домашнего адреса, авторизован для этого домашнего адреса. Это предполагает, что даже с использованием IKE элемент политики должен быть сконфигурирован для каждого домашнего адреса, обслуживаемого домашним агентом.

  Чтобы этого избежать, может оказаться возможным включить домашние адреса в поле Subject AltName сертификата. Однако реализациям не гарантируется поддержка использования конкретного IP-адреса (временного адреса), тогда как в сертификате появляется другой адрес (домашний адрес). В любом случае даже этот подход потребует решения специфических для пользователя задач в полномочном органе сертификации.

- Если применяется аутентификация с предварительно сформированным секретом, то основной режим IKEv1 использоваться не может. Вместо этого необходимо использовать агрессивный режим или групповые предварительно формируемые секреты с соответствующими последствиями для системы безопасности.

  Заметим, что подобно многим другим проблемам, это общая проблема IKEv1, связанная со способностью использования разных IP-адресов, а не специфическая проблема мобильного IPv6. Дополнительную информацию см. в разд. 4.4 в [21].

- В связи с проблемами, отмеченными в разд. 11.3.2, фаза 1 IKE между мобильным узлом и его домашним агентом устанавливается с помощью текущего временного адреса мобильного узла. Это предполагает, что когда мобильный узел переходит на новое местоположение, возможно, он должен переустановить фазу 1. Для реализаций, которые могут обновить оконечные точки фазы 1 IKE без переустановления фазы 1, предоставляется флаг Key Management Mobility Capability (K), но поддержка такого поведения является факультативной.

- Как обсуждалось в разд. 7 в [21], когда используются сертификаты, может произойти фрагментация IKE.

- Тем не менее, если требуется конфигурирование каждого мобильного узла даже для IKE, важное преимущество протокола IKE заключается в том, что он автоматизирует согласование криптографических параметров, включая индексы SPI, криптографические алгоритмы и т.д. Таким образом, требуется меньше конфигурационной информации.

- Если используется ручное управление ключами, то частота перемещений в некоторых канальных уровнях или сценариях развертывания может оказаться достаточно высокой для того, чтобы сделать возможными атаки воспроизведения и переупорядочивания. В этих случаях протокол IKE должен (SHOULD) использоваться. Потенциально уязвимые сценарии включают непрерывное перемещение через небольшие ячейки, или неконтролируемое чередование между доступными точками подключения к сети.

- Подобным образом, при некоторых сценариях развертывания количество мобильных узлов может быть очень большим. В этих случаях, возможно, необходимо использовать автоматические механизмы для сокращения усилий по управлению администрированием криптографических параметров, даже если некоторое конфигурирование каждого мобильного узла всегда необходимо. В этих случаях протокол IKE также должен (SHOULD) использоваться.

- Кроме IKEv1 существуют другие механизмы автоматического управления ключами, но данный документ не рассматривает связанных с ними проблем. Однако заметим, что большая часть приведенных выше соображений применима также и к IKEv2 [30], по крайней мере, к его текущей спецификации.

15.4. Сообщения Binding Update, посылаемые узлу-корреспонденту

Мотивацией разработки процедуры обратной маршрутизируемости (return routability procedure) было создание для мобильного IPv6 достаточной поддержки без порождения новых значительных проблем безопасности. Целью этой процедуры не была защита от атак, которые уже были возможны и до введения мобильного IPv6.

В следующих разделах будут описаны особенности системы безопасности, построенной на основе используемого метода, как с точки зрения злоумышленников, которые находятся на пути пакетов и могут видеть криптографические значения, посылаемые открыто (разд. 15.4.2 и разд. 15.4.3), так и с точки зрения других злоумышленников (разд. 15.4.6).

15.4.1. Обзор

Выбранный безифраструктурный метод проверяет, что мобильный узел «жив» (т.е. он отвечает на пробы) на своем домашнем и временном адресе. В разд. 5.2. подробно описана процедура обратной маршрутизируемости. Эта процедура использует следующие принципы:

- Обмен сообщениями проверяет, что мобильный узел доступен по своим адресам, т.е. по крайней мере, может передавать и принимать трафик, как по домашнему, так и по временному адресу.

- Окончательное сообщение Binding Update криптографически привязывается к маркерам, доставляемым в обмениваемых сообщениях.

- Чтобы избежать использования этого протокола в атаках типа «отражение» (reflection attacks), применяются симметричные обмены. В симметричном обмене ответы всегда посылаются на тот адрес, от которого был послан запрос.

- Узел-корреспондент работает в бесконтекстной манере (без сохранения состояния) до тех пор, пока он не получит полностью авторизованного сообщения Binding Update.

- Путем шифрования туннелей между мобильным узлом и домашним агентом с помощью IPsec ESP предоставляется некоторая дополнительная защита. Поскольку туннель транспортирует также и обмены одноразовыми номерами, это ограничивает возможность злоумышленника увидеть эти одноразовые номера. Например, это предотвращает атаки, запускаемые с текущего чужого линка мобильного узла, даже если на канальном уровне не доступны какие-либо средства конфиденциальности.

Теоретически результирующий уровень безопасности получается тем же, что и без применения этой дополнительной защиты: маркеры обратной маршрутизируемости по-прежнему остаются незащищенными только на одном пути в рамках всей Internet. Однако мобильные узлы часто находятся на небезопасном линке, таком, например, как беспроводные ЛВС с общим доступом. Таким образом, это дополнение во многих случаях дает практическое отличие.

Дальнейшую информацию относительно логического обоснования процедуры обратной маршрутизируемости см. в [27, 34, 33, 32]. Использованные механизмы заимствованы из этих документов.

15.4.2. Достигнутые свойства системы безопасности

Процедура обратной маршрутизируемости защищает обновления привязки от всех злоумышленников, которые не могут наблюдать путь между домашним агентом и узлом-корреспондентом. Эта процедура не защищает от злоумышленников, которые могут наблюдать за этим путем. Заметим, что такие злоумышленники в любом случае способны создать активную атаку на мобильный узел, когда он находится в домашней сети. Возможность такого рода атак не является препятствием для развертывания мобильного IPv6, поскольку эти атаки возможны независимо от того, используется ли мобильный IPv6.

Эта процедура защищает также от атак типа «отказ в обслуживании», в которых злоумышленник прикидывается мобильным узлом, но в качестве временного адреса использует адрес жертвы. Это послужит причиной посылки узлом-корреспондентом некоторого неожиданного трафика узлу-жертве. Процедура защищает от этих атак требуя, по крайней мере, пассивного присутствия злоумышленника по временному адресу или на пути от корреспондента до временного адреса. Обычно это будет мобильный узел.

15.4.3. Сравнение с обычными обменами информацией по IPv6

В данном разделе обсуждается защита, предоставляемая методом обратной маршрутизируемости, путем его сравнения с системой безопасности обычного обмена информацией по IPv6. Мы разделим уязвимости на три класса: (1) связанные со злоумышленниками, находящимися в локальной сети мобильного узла, домашнего агента или узла-корреспондента, (2) связанные со злоумышленниками, находящимися на пути между домашней сетью и узлом-корреспондентом, и (3) связанные со злоумышленниками, находящимися вне этого пути, т.е. в оставшейся части Internet.

Теперь мы обсудим уязвимости обычного обмена информацией по IPv6. Уязвимости обмена информацией по IPv6 на линке включают атаки типа «отказ в обслуживании», «маскарад» (Masquerading), «человек посередине», «перехват сообщений» и другие атаки. Эти атаки могут быть реализованы путем подделывания сообщений Router Discovery, Neighbor Discovery и других механизмов IPv6. Некоторые из этих атак могут быть предотвращены путем использования в пакетах криптографической защиты.

Подобная ситуация существует и со злоумышленниками, находящимися на пути пакетов. А именно, без криптографической защиты трафик является чрезвычайно уязвимым.

Если предположить, что злоумышленники не проникают сквозь систему безопасности протоколов маршрутизации Internet, то атаки с мест, находящихся вне пути пакетов, создать значительно сложнее. Атаки, которые можно запустить с этих мест, в основном являются атаками типа «отказ в обслуживании», такие как «затопление» и/или атаки типа «отражение». Злоумышленник, находящийся вне пути пакетов, не может стать «человеком посередине».

Далее мы рассмотрим уязвимости, которые существуют, когда IPv6 используется совместно с MIPv6 и процедурой обратной маршрутизируемости. На локальном линке уязвимости те же, что и в IPv6, но теперь атаки типа «маскарад» и «человек посередине» могут запускаться также против будущих обменов информацией. Если обновление привязки было послано, когда злоумышленник присутствовал на линке, его следствие сохраняется в течение времени жизни привязки. Это происходит даже в том случае, когда злоумышленник уходит с линка. В отличие от рассмотренной ситуации, злоумышленник, который использует только простой IPv6, чтобы продолжить атаку, как правило, должен оставаться на линке. Заметим, что чтобы запустить эти новые атаки, должен быть известен IP-адрес жертвы. Это делает такую атаку реальной в основном в контексте хорошо известных идентификаторов интерфейсов, таких как те, которые уже появлялись в трафике на линке или регистрировались в DNS.

Злоумышленники, находящиеся на пути пакетов, могут воспользоваться подобными уязвимостями, как и в обычной IPv6. Однако имеются несколько небольших отличий. Атаки типа «маскарад», «человек посередине» и «отказ в обслуживании» могут запускаться даже при перехвате нескольких пакетов, в то время как в обычной IPv6 необходимо перехватывать каждый пакет. Однако, независимо от метода, последствия от атак остаются теми же. В любом случае, наиболее сложной задачей, с которой сталкивается злоумышленник при реализации этих атак, является получение доступа к правильному пути.

Уязвимости для злоумышленников, находящихся вне пути, те же, что и обычном IPv6. Те узлы, которые не находятся на пути между домашним агентом и узлом-корреспондентом, не способны получать сообщения с образцами домашнего адреса.

В заключение мы можем констатировать следующие основные результаты этого сравнения:

- Процедура обратной маршрутизируемости предотвращает проведение любых атак со стороны находящихся вне пути узлов, сверх тех атак, которые и так возможны в обычном IPv6. Это наиболее важный результат, который препятствует злоумышленникам из Internet использовать какие-либо уязвимости.

- Уязвимости для злоумышленников, находящихся на линке домашнего агента, линке узла-корреспондента, или на пути между ними примерно те же, что и в обычном IPv6.

- Однако имеется одно отличие, заключающееся в том, что в основном IPv6 находящийся на пути пакетов злоумышленник должен постоянно присутствовать на линке или на этом пути, в то время как при использовании мобильного IPv6 злоумышленник может отправить привязку позже, после того, как он их покинет.

По этой причине данная спецификация ограничивает создание привязок самое большее MAX_RR_BINDING_LIFETIME секундами после того, как была выполнена последняя проверка маршрутизируемости, и ограничивает жизнь привязки самое большее MAX_RR_BINDING_LIFETIME секундами. При таких ограничениях злоумышленники не могут пулучить практические преимущества от этой уязвимости.

- Имеется также несколько других небольших отличий, например, последствия от уязвимостей типа «отказ в обслуживании». Они могут рассматриваться как несущественные.

- Обычно путь между домашним агентом и узлом-корреспондентом проще всего атаковать со стороны линков любого из концов связи, в частности, если эти линки представляют собой беспроводные ЛВС общего пользования.

  Атаки на маршрутизаторы или коммутаторы, находящиеся на этом пути, реализовать обычно труднее. Поэтому система безопасности линков уровня 2 играет главную роль в результирующей общей системе безопасности сети. Подобным образом, на этих линках имеет огромное значение безопасность протоколов IPv6 Neighbor Discovery и Router Discovery. Если с помощью каких-либо новых технологий в будущем они будут сделаны безопасными, это могло бы изменить ситуацию, касающуюся наиболее простого места для атаки.

Более глубокое обсуждение этих проблем см. в [32].

15.4.4. Атаки повторного воспроизведения

Процедура обратной маршрутизации защищает также участников от повторно воспроизведенных сообщений Binding Update. Злоумышленник не может повторно воспроизвести то же самое сообщение благодаря порядковым номерам, которые являются частью сообщения Binding Update. Невозможно также модифицировать сообщение Binding Update, поскольку после такой модификации проверка MAC выдаст ошибку.

Однако при удалении привязок в узле-корреспонденте необходимо соблюдать осторожность. Если привязка удаляется в тот момент, когда одноразовый номер, использованный при ее создании еще считается достоверным, злоумышленник может повторно воспроизвести старое обновление привязки. Правила, представленные в разд. 5.2.8 гарантируют, что это не может произойти.

15.4.5. Атаки типа «отказ в обслуживании»

Процедура обратной маршрутизируемости имеет защиту от атак типа «отказ в обслуживании», связанных с исчерпанием ресурсов. Узлы-корреспонденты не сохраняют никакого состояния относительно отдельных мобильных узлов до тех пор, пока не поступит аутентичное сообщение Binding Update. Это достигается благодаря конструированию маркеров keygen token из одноразовых номеров и узловых ключей, которые не являются специфическими для отдельных мобильных узлов. Маркеры keygen token могут быть реконструированы узлом-корреспондентом базируясь на информации о домашнем и временном адресе, которая поступает в сообщении Binding Update. Это означает, что узлы-корреспонденты защищены от атак, направленных на исчерпание памяти, за исключением случаев, когда злоумышленники находятся на пути передачи пакетов. Благодаря использованию симметричной криптографии узлы-корреспонденты также относительно защищены от атак, связанных с исчерпанием ресурсов ЦП.

Тем не менее, как описано в [27], имеются ситуации, в которых мобильный узел или узел-корреспондент не может определить, действительно ли им нужна привязка, или они введены в заблуждение злоумышленником, который заставляет их в это поверить. Поэтому необходимо рассматривать ситуации, при которых реализуются такие атаки.

Даже если оптимизация маршрута является очень важной оптимизацией, она все-таки остается только оптимизацией. Можильный узел может обмениваться данными с узлом-корреспондентом даже если корреспондент отказывается принимать какие-либо обновления привязки. Однако при этом пострадает производительность, поскольку пакеты от узла-корреспондента к мобильному узлу будут маршрутизироваться через домашнего агента мобильного узла, а не идти по более прямому маршруту. Узел-корреспондент может защитить самого себя от некоторых атак, направленных на исчерпание ресурсов, следующим образом. Если узел-корреспондент «заваливается» большим количеством сообщений Binding Update, криптографическая проверка целостности которых обнаруживает ошибки, он может приостановить обработку сообщений Binding Update. Если узел-корреспондент определяет, что он расходует больше ресурсов на проверку поддельных сообщений Binding Update, чем он вероятно может сохранить при приеме действительных сообщений Binding Update, то он может молча отбрасывать некоторые или все сообщения Binding Update без выполнения каких-либо криптографических операций.

Уровни, выше уровня IP, обычно предоставляют дополнительную информацию, чтобы решить, имеется ли необходимость установления привязки для конкретного партнера. Например, TCP знает, имеет ли узел очередь данных, которые он пытается переслать партнеру. Реализация данной спецификации не требует использования информации от более высоких протокольных уровней, однако некоторые реализации, вероятно, окажутся способными управлять ресурсами более эффективно благодаря использованию такого рода информации.

Мы также требуем, чтобы все реализации были способны административно отключать оптимизацию маршрутов.

15.4.6. Длина ключей

Злоумышленники могут пытаться взломать процедуру обратной маршрутизируемости многими способами. В разд. 15.4.2 обсуждается ситуация, при которой злоумышленник может видеть криптографические значения, посылаемые открыто, а в разделе 15.4.3 обсуждаются последствия этого на обмен информацией по IPv6. В

этом разделе обсуждается вопрос, может ли злоумышленник догадаться о правильных значениях без наблюдения за ними.

Когда выполняется процедура обратной маршрутизируемости, для защиты от подделанных ответов используются 64-битовые идентификационные цепочки. Это считается достаточным, предполагая, что для того чтобы вслепую подделать ответ, необходимо будет очень большое количество сообщений прежде, чем успех окажется вероятным.

Маркеры, используемые в процедуре обратной маршрутизируемости, представляют совместно 128 бит информации. Эта информация используется внутри в качестве входа хэш-функции для выработки 160-битовой величины, пригодной для выработки ключевого хэша в обновлении привязки с помощью алгоритма HMAC_SHA1. Длина конечного ключевого хэша составляет 96 бит. Ограничивающими факторами в этом случае являются длина входного маркера и длина конечного ключевого хэша. Применение внутренней хэш-функции не сокращает энтропию.

Конечный 96-битовый ключевой хэш имеет обычный размер и считается безопасным. 128-битовый вход из маркеров разбит на две части, маркер home keygen token и маркер care-of keygen token. Злоумышленник может попытаться отгадать правильное значение идентифицирующей цепочки, но снова повторим, что это потребует большого количества сообщений, в среднем 2**63 сообщений для первого и 2**127 сообщений для второго. Более того, поскольку идентифицирующие цепочки являются достоверными только в течение короткого интервала времени, для достижения конечного эффекта атака должна поддерживать высокую постоянную скорость сообщений. Это не представляется практичным.

Когда мобильный узел возвращается домой, как раз допускается использовать маркер home keygen token длиною 64 бита. Это меньше 128 бит, но атака на него вслепую все еще требует, чтобы было послано большое количество сообщений. Если злоумышленник находится на пути пакетов и способен видеть обновление привязки, он может, вероятно, взломать ключевой хэш методом грубой силы. Однако в этом случае злоумышленник должен находиться на пути следования пакетов, что, как кажется, предоставляет более простые способы для организации «отказа в обслуживании», чем препятствование оптимизации маршрута.

15.5. Динамическое определение адреса домашнего агента

Функция динамического определения адреса домашнего агента может использоваться для узнавания адресов домашних агентов в домашней сети.

Возможность узнать адреса узлов для злоумышленников может оказаться полезной, поскольку тупое сканирование адресного пространства в IPv6 представляется непрактичным. Таким образом, они могут извлечь пользу из любого средства, которое упростит отображение сетей. Например, если угроза системе безопасности, нацеленная на маршрутизаторы или даже на домашние агенты, выявлена, наличие простого механизма ICMP для выяснения возможных целей просто может стать дополнительным (хотя и небольшим) риском для системы безопасности.

Однако без возможности определения адресов домашних агентов, злоумышленники не будут способны узнать многое из этой информации, и мобильные узлы не могут быть вовлечены в использование неправильных домашних агентов, поскольку все другие связи с домашними агентами являются защищенными.

15.6. Определение мобильного префикса

Функция определения мобильного префикса для подслушивающих может выдать интересную информацию относительно топологии сети и времени жизни префикса, и по этой причине запросы этой информации должны быть аутентифицированы. Ответы и незапрошенная префиксная информация должны аутентифицироваться, чтобы предотвратить восприятие мобильными узлами неверной информации о префиксах, мешающей, возможно, обмену информацией с существующими адресами.

15.7. Туннелирование через домашнего агента

Туннели между мобильным узлом и домашним агентом могут быть защищены путем обеспечения надлежащего использования адресов источников и дополнительной криптографической защиты. Эти процедуры обсуждаются в разд. 5.5.

Сообщения Binding Update, посылаемые домашним агентам, защищены. При приеме туннелированного трафика домашний агент проверяет, что внешний IP-адрес соответствует текущему местоположению мобильного узла. Это действует как слабая форма защиты от подделывания пакетов, которые выглядят так, как будто они прибыли от мобильного узла. Это очень полезно, если между мобильным узлом и узлом-корреспондентом не применяется система сквозной безопасности. Проверка внешнего IP-адреса предотвращает атаки, когда злоумышленник контролируется входной фильтрацией. Она предотвращает также атаки, когда злоумышленник не знает текущего временного адреса мобильного узла. Злоумышленники, знающие временный адрес и не контролируемые входной фильтрацией, могут все еще посылать трафик через домашнего агента. Это включает злоумышленников, находящихся на том же самом локальном линке, на котором работает в текущий момент мобильный узел. Но такие злоумышленники могут в любом случае без атаки на туннель посылать пакеты, которые выглядят как пришедшие от мобильного узла; злоумышленник может просто посылать пакеты с адресом источника, совпадающим с домашним адресом мобильного узла. Однако такая атака не работает, если конечное место назначения пакета находится в домашней сети, и для пакетов, посылаемых на эти места назначения, применяется некоторая форма защиты периметра. В этих случаях рекомендуется, чтобы применялись либо система сквозной безопасности, либо дополнительная защита туннеля, как это обычно бывает в ситуациях с удаленным доступом.

Домашние агенты и мобильные узлы для защиты пакетов полезных данных, туннелируемых между ними, могут использовать IPsec ESP. Это полезно для защиты обменов информацией от злоумышленников, находящихся на пути туннеля.

Когда используются «локальные для сайта» домашние адреса, для посылки локального для сайта трафика из другого местоположения может использоваться обратное туннелирование. Об этом должны быть осведомлены администраторы, когда они позволяют использовать такие домашние адреса. В частности, описанной выше проверки внешнего IP-адреса для защиты от всех злоумышленников не достаточно. Использование зашифрованных туннелей особенно полезно для этого вида домашних адресов.

15.8. Опция Home Address

Когда мобильный узел посылает пакеты прямо узлу-корреспонденту, поле адреса источника в IPv6-заголовке пакета является временным адресом. Поэтому входная фильтрация [26] работает обычным образом даже для мобильных узлов, поскольку адрес источника топологически корректен. Опция Home Address используется для информирования узла-корреспондента о домашнем адресе мобильного узла.

Однако временный адрес в поле адреса источника не остается в ответах, посылаемых узлом-корреспондентом, если только он не имеет привязку для данного мобильного узла. Кроме того, когда пакеты «отражаются» через узлы-корреспонденты используя опцию Home Address, не все механизмы отслеживания злоумышленника работают. По этим причинам данная спецификация ограничивает использование опции Home Address. Она может использоваться только когда привязка уже установлена с участием узла по домашнему адресу, как описано в разд. 5.5 и разд. 6.3. Это предотвращает атаки «отражения», которые используют опцию Home Address. Это гарантирует также, что узлы-корреспонденты отвечают по тому же адресу, с которого мобильный узел посылает трафик.

Сверх указанного выше, никакой специальной аутентификации опции Home Address не требуется, но заметим, что если заголовок IPv6 пакета защищен заголовком аутентификации IPsec, то эта аутентификация защищает также и опцию Home Address.

Таким образом, даже когда аутентификация используется в заголовке IPv6, безопасность поля адреса источника в заголовке IPv6 наличием опции Home Address не подрывается. При отсутствии аутентификации пакета любое поле, включая поле адреса источника, а также любые другие части пакета, включая опцию Home Address, могут быть подделаны или модифицированы в пути. В этом случае содержимое опции Home Address является не более сомнительным, чем любая другая часть пакета.

15.9. Заголовок маршрутизации типа 2

Определение заголовка маршрутизации типа 2 описано в разд. 6.4. Это определение и связанные с ним правила обработки выбраны таким образом, чтобы этот заголовок нельзя было использовать для того, что традиционно рассматривается как маршрутизация от источника. В частности домашний адрес в заголовке маршрутизации будет всегда присвоен домашнему адресу принимающего узла. В противном случае, пакет будет отброшен.

Вообще маршрутизация от источника имеет целый ряд проблем безопасности. Они включают автоматическое реверсирование неаутентифицированных маршрутов от источника (которые используются для IPv4, но не для IPv6). Другая забота связана с возможностью использовать маршрутизацию от источника для «прыжка» между узлами внутри, а также вне межсетевого экрана. Благодаря упомянутым выше правилам эти проблемы безопасности в мобильном IPv6 не возникают.

По существу семантика заголовка маршрутизации типа 2 та же, что и у специальной формы туннелирования IP-in-IP, в которой внутренний и внешний адреса совпадают.

Это предполагает, что устройство, которое реализует фильтрацию пакетов должно быть способно отличать заголовок маршрутизации типа 2 от других заголовков маршрутизации, как требуется в разд. 8.3. Это необходимо, чтобы разрешить мобильный IPv6-трафик, имея при этом дополнительную возможность отфильтровывать другие использования заголовков маршрутизации.

16. Участники

Tuomas Aura, Mike Roe, Greg O'Shea, Pekka Nikander, Erik Nordmark, and Michael Thomas worked on the return routability protocols eventually led to the procedures used in this protocol. The procedures described in [34] were adopted in the protocol.

Significant contributions were made by members of the Mobile IPv6 Security Design Team, including (in alphabetical order) Gabriel Montenegro, Erik Nordmark and Pekka Nikander.

17. Благодарности

We would like to thank the members of the Mobile IP and IPng Working Groups for their comments and suggestions on this work. We would particularly like to thank (in alphabetical order) Fred Baker, Josh Broch, Samita Chakrabarti, Robert Chalmers, Noel Chiappa, Greg Daley, Vijay Devarapalli, Rich Draves, Francis Dupont, Thomas Eklund, Jun-Ichiro Itojun Hagino, Brian Haley, Marc Hasson, John Ioannidis, James Kempf, Rajeev Koodli, Krishna Kumar, T.J. Kniveton, Joe Lau, Jiwoong Lee, Aime Le Rouzic, Vesa-Matti Mantyla, Kevin Miles, Glenn Morrow, Thomas Narten, Karen Nielsen, Simon Nybroe, David Oran, Brett Pentland, Lars Henrik Petander, Basavaraj Patil, Mohan Parthasarathy, Alexandru Petrescu, Mattias Petterson, Ken Powell, Phil Roberts, Ed Remmell, Patrice Romand, Luis A. Sanchez, Jeff Schiller, Pekka Savola, Arvind Sevalkar, Keiichi Shima, Tom Soderlund, Hesham Soliman, Jim Solomon, Tapio Suihko, Dave Thaler, Benny Van Houdt, Jon-Olov Vatn, Carl E. Williams, Vladislav Yasevich, Alper Yegin, and Xinhua Zhao, for their detailed reviews of earlier versions of this document. Their suggestions have helped to improve both the design and presentation of the protocol.

We would also like to thank the participants of the Mobile IPv6 testing event (1999), implementors who participated in Mobile IPv6 interoperability testing at Connectathons (2000, 2001, 2002, and 2003), and the participants at the ETSI interoperability testing (2000, 2002). Finally, we would like to thank the TAHI project who has provided test suites for Mobile IPv6.

18. Ссылки

18.1. Нормативные ссылки

[1] Eastlake 3rd., D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

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

[3] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

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

[5] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[6] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[7] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[8] Maughan, D., Schertler, M., Schneider, M. and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[9] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

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

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

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

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

[14] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.

[15] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[16] Johnson, D. and S. Deering, "Reserved IPv6 Subnet Anycast Addresses", RFC 2526, March 1999.

[17] Deering, S., Fenner, W. and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

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

[19] Reynolds, J., Ed., "Assigned Numbers: RFC 1700 is Replaced by an On-line Database", RFC 3232, January 2002.

[20] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-1, April 1995, <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.

[21] Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

18.2. Информативные ссылки

[22] Perkins, C., Ed., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[23] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[24] Perkins, C., "Minimal Encapsulation within IP", RFC 2004, October 1996.

[25] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing

for Message Authentication", RFC 2104, February 1997.

[26] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[27] Aura, T. and J. Arkko, "MIPv6 BU Attacks and Defenses", Work in Progress, March 2002.

[28] Bellovin, S., "Guidelines for Mandating Automated Key Management", Work in Progress, August 2003.

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

[30] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", Work in Progress, April 2003.

[31] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[32] Nikander, P., Aura, T., Arkko, J., Montenegro, G. and E. Nordmark, "Mobile IP version 6 Route Optimization Security Design Background", Work in Progress, April 2003.

[33] Nordmark, E., "Securing MIPv6 BUs using return routability (BU3WAY)", Work in Progress, November 2001.

[34] Roe, M., Aura, T., O'Shea, G. and J. Arkko, "Authentication of Mobile IPv6 Binding Updates and Acknowledgments", Work in Progress, March 2002.

[35] Savola, P., "Use of /127 Prefix Length Between Routers Considered Harmful", RFC 3627, September 2003.

[36] Savola, P., "Security of IPv6 Routing Header and Home Address Options", Work in Progress, December 2002.

[37] Vida, R. and L. Costa, Eds., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

Приложение A. Будущие расширения

A.1. Комбинированные передачи

This document does not specify how to piggyback payload packets on the binding related messages. However, it is envisioned that this can be specified in a separate document when issues such as the interaction between piggybacking and IPsec are fully resolved (see also Appendix A.3). The return routability messages can indicate support for piggybacking with a new mobility option.

A.2. Треугольная маршрутизация

Due to the concerns about opening reflection attacks with the Home Address destination option, this specification requires that this option be verified against the Binding Cache, i.e., there must be a Binding Cache entry for the Home Address and Care-of Address.

Future extensions may be specified that allow the use of unverified Home Address destination options in ways that do not introduce security issues.

A.3. Новые методы авторизации

While the return routability procedure provides a good level of security, there exist methods that have even higher levels of security. Secondly, as discussed in Section 15.4, future enhancements of IPv6 security may cause a need to also improve the security of the return routability procedure. Using IPsec as the sole method for authorizing Binding Updates to correspondent nodes is also possible. The protection of the Mobility Header for this purpose is easy, though one must ensure that the IPsec SA was created with appropriate authorization to use the home address referenced in the Binding Update. For instance, a certificate used by IKE to create the security association might contain the home address. A future specification may specify how this is done.

A.4. Динамически генерируемые домашние адреса

A future version of this specification may include functionality that allows the generation of new home addresses without requiring pre-arranged security associations or certificates even for the new addresses.

A.5. Удаленное конфигурирование домашнего адреса

The method for initializing a mobile node's home address upon power-up or after an extended period of being disconnected from the network is beyond the scope of this specification. Whatever procedure is used should result in the mobile node having the same stateless or stateful (e.g., DHCPv6) home address autoconfiguration information it would have if it were attached to the home network. Due to the possibility that the home network could be renumbered while the mobile node is disconnected, a robust mobile node would not rely solely on storing these addresses locally.

Such a mobile node could be initialized by using the following procedure:

1. Generate a care-of address.

2. Query DNS for an anycast address associated with the FQDN of the home agent(s).

3. Perform home agent address discovery, and select a home agent.

4. Configure one home address based on the selected home agent's subnet prefix and the interface identifier of the mobile node.

5. Create security associations and security policy database entries for protecting the traffic between the selected home address and home agent.

6. Perform a home registration on the selected home agent.

7. Perform mobile prefix discovery.

8. Make a decision if further home addresses need to be configured.

This procedure is restricted to those situations where the home prefix is 64 bits and the mobile node knows its own interface identifier, which is also 64 bits.

A.6. Расширения протокола Neighbor Discovery

Future specifications may improve the efficiency of Neighbor Discovery tasks, which could be helpful for fast movements. One factor is currently being looked at: the delays caused by the Duplicate Address Detection mechanism. Currently, Duplicate Address Detection needs to be performed for every new care-of address as the mobile node moves, and for the mobile node's link-local address on every new link. In particular, the need and the trade-offs of re-performing Duplicate Address Detection for the link-local address every time the mobile node moves on to new links will need to be examined. Improvements in this area are, however, generally applicable and progress independently from the Mobile IPv6 specification.

Future functional improvements may also be relevant for Mobile IPv6 and other applications. For instance, mechanisms that would allow recovery from a Duplicate Address Detection collision would be useful for link-local, care-of, and home addresses.

Адреса авторов

David B. Johnson
Rice University
Dept. of Computer Science, MS 132
6100 Main Street
Houston TX 77005-1892
USA

EMail: dbj@cs.rice.edu

Charles E. Perkins
Nokia Research Center
313 Fairchild Drive
Mountain View CA 94043
USA

EMail: charliep@iprg.nokia.com

Jari Arkko
Ericsson
02420 Jorvas
Finland

EMail: jari.arkko@ericsson.com

Полная формулировка авторских прав

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.