Network Working Group
Request for Comments: 3344
Obsoletes: 3220
Category: Standards Track

C. Perkins, Ed.
Nokia Research Center

August 2002

Поддержка IP Mobility для IPv4

IP Mobility Support for IPv4

Статус документа

Данный документ содержит спецификацию стандартного протокола Internet, предложенного сообществу Internet, и является приглашением к дискуссии в целях развития этого протокола. Сведения о текущем состоянии стандартизации протокола вы найдёте в документе Internet Official Protocol Standards (STD 1). Документ можно распространять без ограничений.

Авторские права

Аннотация

Этот документ описывает расширение протокола, позволяющее прозрачно маршрутизировать дейтаграммы IP мобильным узлам в Internet. Каждый мобильный узел идентифицируется его домашним адресом, независимо от текущей точки подключения к Internet. Находящийся за пределами домашней сети мобильный узел имеет адрес обслуживания (care-of address), который обеспечивает информацию о текущей точке подключения к Internet. Протокол предусматривает регистрацию адреса обслуживания на домашнем агенте. Этот агент отправляет адресованные мобильному узлу дейтаграммы через туннель на адрес обслуживания. После прибытия дейтаграммы на удалённую сторону туннеля она передаётся мобильному узлу.

Оглавление

1. Введение

В IP версии 4 предполагается, что IP-адрес узла уникально идентифицирует точку подключения данного узла к сети Internet. Следовательно, узел должен размещаться в сети, указанной его адресом IP, чтобы получать адресованные ему пакеты. В противном случае дейтаграммы просто не дойдут до узла. Чтобы узлы могли менять точки подключения без потери возможности связи в настоящее время используется обычно один из перечисленных механизмов:

a) узел меняет адрес в соответствии с точкой подключения;

b) специфические маршруты к хостам распространяются через систему маршрутизации Internet.

Зачастую не приемлем ни один из этих вариантов. В первом случае при изменении местоположения узла для него становится невозможной поддержка соединений на транспортном и вышележащих уровнях. Второе решение вызывает проблемы с масштабированием, существенно усложняющиеся с ростом числа мобильных компьютеров.

Требуется новый, обеспечивающий масштабирование механизм для подключения мобильных узлов к сети Internet. В этом документе определён такой механизм, который позволяет мобильным узлам менять точку подключения к Internet без смены своего адреса IP.

Различия между этой обновлённой спецификацией Mobile IP и предшествующими спецификациями (см. [33, 32, 34, 43, 8]) подробно рассмотрены в Приложении G.

1.1. Протокольные требования

Мобильный узел должен сохранять возможность взаимодействия с другими узлами после изменения его точки подключения к Internet на канальном уровне без изменения адреса IP.

Мобильный узел должен иметь возможность коммуникаций с узлами, не поддерживающими описанные здесь функции мобильности. Не требуется расширения протоколов на хостах и маршрутизаторах, не являющихся непосредственными участниками архитектурных элементов, указанных в параграфе 1.5.

Все сообщения для обновления на других узлах в связи со сменой местоположения мобильного узла должны аутентифицироваться для предотвращения атак с перенаправлением трафика.

1.2. Цели

Для подключения мобильных узлов к Internet зачастую могут применяться беспроводные сети. Канал подключения может отличаться меньшей полосой пропускания и большей частотой ошибок по сравнению с традиционными проводными сетями. Более того, питание мобильных узлов зачастую осуществляется от внутренней батареи и вопрос снижения энергопотребления весьма важен. Следовательно, число административных сообщений через канал подключения мобильного узла к сети Internet следует минимизировать, а размер таких сообщений сделать как можно меньше.

1.3. Допущения

Протоколы, определённые в данном документе, не вносят дополнительных ограничений в распределение адресов IP. Т. е., мобильным узлам могут выделяться адреса IP из блоков владеющих этими устройствами организаций.

Этот протокол исходит из допущения, что мобильные узлы не меняют точку своего подключения к Internet чаще 1 раза в секунду.

Этот протокол исходит из допущения о том, что индивидуальные дейтаграммы IP маршрутизируются на основе адресов получателей в заголовках дейтаграмм (и не маршрутизация не зависит, например, от адресов отправителей).

1.4. Применимость

Расширение Mobile IP предназначено для обеспечения мобильным узлам возможности перехода из одной сети IP в другую. Оно одинаково подходит как для однородных, так и для разнородных сетевых сред. Т. е., Mobile IP упрощает как переход узла из одного сегмента Ethernet в другой, так и переключение из сети Ethernet в беспроводную сеть, если IP-адрес мобильного узла при таких перемещениях не меняется.

Можно рассматривать Mobile IP как решение задачи управления мобильностью на макроуровне. Для управления мобильностью на «микроуровне» (например, переключение между беспроводными точками доступа в движении) это решение подходит не столь хорошо. Если мобильный узел не просто переключается из одной сети IP в другую, а движется в процессе такого «переключения», механизмы поддержки мобильности на канальном уровне (переход из одной сети в другую - link-layer handoff) могут обеспечивать более быстрое переключение и меньшие издержки, нежели Mobile IP.

1.5. Новые архитектурные элементы

Mobile IP добавляет ряд новых функциональных элементов, перечисленных ниже.

Mobile Node - мобильный узел
Хост или маршрутизатор, который меняет точку своего подключения, переходя из одной (под)сети в другую. Мобильный узел может менять своё местоположение без смены адреса IP, он может продолжать взаимодействие с другими узлами Internet из любой точки, используя свой (постоянный) адрес IP, если обеспечивается связность с сетью на канальном уровне.

Home Agent - домашний агент
Маршрутизатор в домашней сети мобильного узла, который туннелирует дейтаграммы для доставки мобильному узлу, находящемуся за пределами домашней сети, и поддерживает информацию о текущем местоположении мобильного узла.

Foreign Agent - внешний агент
Маршрутизатор в сети, к которой подключается мобильный узел, обеспечивающий по запросу мобильного узла услуги маршрутизации. Внешний агент служит второй точкой туннеля, организуемого домашним агентом

мобильного узла. Для передаваемых зарегистрированными мобильными узлами дейтаграмм внешний агент может служить используемым по умолчанию маршрутизатором.

Мобильный узел имеет с домашней сети адрес IP с продолжительным сроком действия. Этот домашний адрес администрируется так же, как «постоянные» адреса IP на стационарных хостах. Когда мобильное устройство отключается от домашней сети и подключается к другой, оно получает «адрес обслуживания» (care-of address), который связывается с мобильным узлом и указывает его текущую точку подключения. Мобильный узел использует свой домашний адрес в качестве адреса отправителя всех передаваемых им дейтаграмм IP, за исключением описанных в этом документе дейтаграмм, служащих для некоторых функций управления (см. параграф 3.6.1.1).

1.6. Терминология

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с RFC 2119 [4].

Ниже приведены определения некоторых терминов, часто используемых в данном документе.

Authorization-enabling extension - расширение для поддержки проверки полномочий

Аутентификация, которая делает (регистрационное) сообщение приемлемым для конечного получателя. Поддерживающее проверку полномочий расширение **должно** включать SPI.

В этом документе все случаи использования поддерживающего проверку полномочий расширения относятся к аутентификационным расширениям, которые разрешают восприятие сообщения Registration Request домашним агентом. Использование дополнительных протокольных структур, не описанных в данном документе, может оказаться возможным для мобильного узла с целью обеспечить его регистрацию на домашнем агенте с помощью элемента аутентификации в сети, который приемлем для домашнего агента (см., например, RFC 2794 [6]).

Agent Advertisement - анонсирование агента

Сообщение-анонс, созданное путём присоединения к маршрутным анонсам специального расширения [10].

Authentication - аутентификация

Процесс проверки (с использованием криптографических методов для всех приложений в данной спецификации) идентификации источника сообщения.

Care-of Address - адрес обслуживания

Точка завершения туннеля в направлении мобильного узла для пересылаемых такому узлу дейтаграмм в случае его подключения за пределами домашней сети. Протокол может использовать два разных типа адресов обслуживания: foreign agent care-of address представляет собой адрес внешнего агента, на котором регистрируется мобильный узел, а co-located care-of address (совмещённый адрес) - полученный извне локальный адрес, который мобильный узел связывает с одним из своих интерфейсов.

Correspondent Node - узел-корреспондент

Партнёр, с которым взаимодействует мобильный узел. Это может быть стационарный или мобильный узел.

Foreign Network - чужая сеть

Любая сеть, не являющаяся домашней для мобильного узла.

Gratuitous ARP - беспричинный пакет

Пакет ARP, передаваемый узлом для того, чтобы побудить другие узлу к обновлению их кэша ARP [45] (см. параграф 4.6).

Home Address - домашний адрес ARP

Адрес IP, предоставленный мобильному узлу для использования в течение достаточно долгого срока. Этот адрес не зависит от точки подключения мобильного узла к сети Internet.

Home Network - домашняя сеть

Сеть (возможно, виртуальная), адресный префикс которой соответствует домашнему адресу мобильного узла. Отметим, что стандартные механизмы маршрутизации IP будут доставлять дейтаграммы для мобильного узла в его домашнюю сеть.

Link - канал, соединение

Элемент или среда, через которые узлы взаимодействуют на канальном уровне. Располагается под сетевым уровнем.

Link-Layer Address - адрес канального уровня

Адрес, служащий для идентификации конечных точек в некоторых коммуникациях через физические каналы. Обычно адресом канального уровня является MAC-адрес интерфейса.

Mobility Agent - агент мобильности

Домашний или внешний агент.

Mobility Binding - мобильная привязка

Связывание домашнего адреса с адресом обслуживания вкупе со временем существования такой привязки.

Mobility Security Association - защищённая мобильная связь

Набор защитных средств (контекстов) между парой узлов, который может быть применён к сообщениям протокола Mobile IP между этими узлами. Каждый контекст указывает алгоритм и режим аутентификации (параграф 5.1), секрет (разделяемый ключ или подходящая пара из закрытого и открытого ключей), а также стиль защиты от использования повторов (параграф 5.7).

Node - узел

Хост или маршрутизатор.

Nonce

Случайное значение, отличающееся от предыдущих, которое помещается в сообщение для защиты от повторного использования.

Security Parameter Index (SPI) - индекс параметров защиты

Индекс, идентифицирующий контекст защиты между парой узлов из числа контекстов, доступных в Mobility Security Association. Значения SPI от 0 до 255 являются резервными, **недопустимо** использовать их для Mobility SA.

Tunnel - туннель

Путь, по которому проходят инкапсулированные дейтаграммы. Инкапсулируемая дейтаграмма маршрутизируется известному агенту декапсуляции, который корректно извлекает дейтаграмму и направляет её получателю.

Virtual Network - виртуальная сеть
Сеть без физического интерфейса за пределы маршрутизатора (с физическим интерфейсом маршрутизатора в другую сеть). Маршрутизатор (например, домашний агент) обычно анонсирует доступность виртуальной сети с использованием обычных протоколов маршрутизации.

Visited Network - посещённая сеть
Сеть, к которой подключён мобильный узел, не являющаяся домашней для него.

Visitor List - список посетителей
Список мобильных узлов, посетивших внешний агент.

1.7. Обзор протокола

Ниже перечислены службы, определённые для Mobile IP.

Agent Discovery - обнаружение агента
Домашние и внешние агенты могут анонсировать свою доступность на каждом канале, через который они обеспечивают сервис. Вновь подключившийся мобильный узел может отправить в канал запрос для определения наличия там нужного агента.

Registration - регистрация
Когда мобильный узел покидает домашнюю сеть, он регистрирует свой адрес обслуживания на домашнем агенте. В зависимости от метода подключения мобильный узел может регистрироваться на домашнем агенте напрямую или через внешний агент, пересылающий регистрационные данные домашнему агенту.

silently discard - отбрасывание без уведомления
Реализация отбрасывает дейтаграммы без дальнейшей обработки и без уведомления об этом отправителя. В реализациях **следует** поддерживать возможность записи таких фактов в системный журнал (с возможностью сохранения содержимого отброшенной дейтаграммы) и учёт таких событий в статистике.

Ниже кратко описаны операции протокола Mobile IP.

- Агенты мобильности (т. е., домашние и внешние агенты) анонсируют своё присутствие с помощью сообщений Agent Advertisement (раздел 2). Мобильный узел может запросить сообщение Agent Advertisement от любого локально подключённого агента мобильности с помощью отправки сообщения Agent Solicitation.

- Мобильный узел получает эти сообщения Agent Advertisement и определяет подключён он к домашней или чужой сети.

- Когда мобильный узел определяет своё подключение к домашней сети, он не использует службы мобильности. При возвращении в домашнюю сеть после регистрации в какой-либо чужой сети мобильный узел заново регистрируется на домашнем агенте, обмениваясь с ним сообщениями Registration Request и Registration Reply.

- Когда мобильный узел определяет, что он подключён к чужой сети, он получает от этой сети адрес обслуживания. Этот адрес может быть определён из анонсов внешнего агента (адрес внешнего агента) или с помощью того или иного внешнего механизма типа DHCP [13] (совмещённый адрес обслуживания).

- Работающий за пределами домашней сети мобильный узел регистрирует адрес обслуживания на своём домашнем агенте, обмениваясь с ним сообщениями Registration Request и Registration Reply (возможно через внешнего агента - см. раздел 3).

- Дейтаграммы, передаваемые на домашний адрес мобильного узла, перехватываются домашним агентом, туннелируются на адрес обслуживания мобильного узла, принимаются в конечной точке этого туннеля (внешний агент или сам мобильный узел) и доставляются мобильному узлу (параграф 4.2.3).

- В обратном направлении дейтаграммы от мобильного узла обычно доставляются получателям с использованием стандартных механизмов маршрутизации IP (не обязательно через домашнего агента).

При работе мобильного узла вне домашней сети Mobile IP использует туннелирование для сокрытия домашнего адреса мобильного узла от промежуточных маршрутизаторов на пути между домашней сетью и текущей точкой подключения мобильного узла. Туннель завершается на адресе обслуживания мобильного узла. Адресом обслуживания должен быть тот адрес IP, на который дейтаграммы будут доставляться обычной маршрутизацией. По адресу обслуживания исходные дейтаграммы извлекаются из туннеля и доставляются мобильному узлу.

Mobile IP предлагает два варианта получения адреса обслуживания:

a) Адрес внешнего агента (foreign agent care-of address) - это адрес обслуживания, предоставляемый внешним агентом в его сообщениях Agent Advertisement. В этом случае адресом обслуживания является IP-адрес внешнего агента. В этом режиме внешний агент является конечной точкой туннеля и при получении туннелированных дейтаграмм он декапсулирует их и доставляет вложенные дейтаграммы мобильному узлу. Этот режим получения адреса является предпочтительным, поскольку он позволяет множеству мобильных узлов пользоваться одним адресом обслуживания, что весьма важно в условиях дефицита адресов IPv4.

b) Совмещённый адрес (co-located care-of address) - это адрес обслуживания, получаемый мобильным узлом, как локальный адрес IP с помощью тех или иных внешних механизмов. Полученный адрес мобильный узел связывает с одним из своих интерфейсов. Адрес может выделяться динамически (например, через DHCP [13]) или статически на все время присутствия мобильного узла в чужой сети. Конкретные способы предоставления локальных адресов мобильным узлам для использования в качестве адресов обслуживания выходят за рамки этого документа. При использовании совмещённого адреса обслуживания мобильный узел является конечной точкой туннеля и сам выполняет декапсуляцию туннелируемых дейтаграмм.

Преимуществом использования совмещённого адреса обслуживания является возможность работы мобильного узла без внешнего агента (например, в сетях, где таких агентов нет). Однако для поддержки этого режима требуется выделять дополнительный пул дефицитных адресов IPv4, которые могут использоваться мобильными узлами. Эффективная поддержка таких пулов для каждой подсети, к которой могут подключаться мобильные пользователи, является достаточно трудной задачей.

Важно различать адрес обслуживания и функции внешнего агента. Адрес обслуживания просто задаёт конечную точку туннеля. Это может быть и адрес внешнего агента (foreign agent care-of address), но может быть и адресом, временно полученным мобильным узлом (co-located care-of address). Внешний агент, с другой стороны, является агентом мобильности, обслуживающим мобильны узлы. Дополнительная информация приведена в параграфах 3.7 и 4.2.2.

На рисунке 1 показана маршрутизация дейтаграмм мобильного узла, находящегося вне домашней сети, после его регистрации на домашнем агенте. В этом примере мобильный узел использует адрес внешнего агента, а не совмещённый адрес.

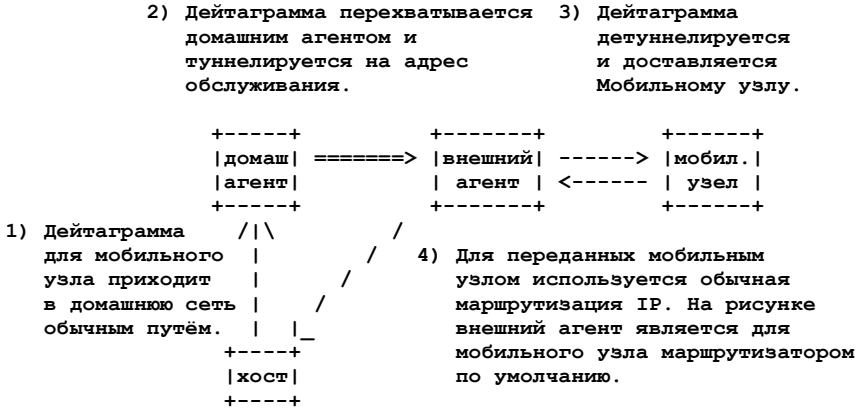


Рисунок 1. Работа Mobile IPv4.

Домашний агент **должен** быть способен перехватывать дейтаграммы, направленные любому из зарегистрированных им мобильных узлов. Использование посредника и механизмов ARP, описанных в параграфе 4.6, позволяет выполнить это требование, если домашний агент имеет интерфейс в сеть (канал), указанную домашним адресом мобильного узла. При ином расположении домашнего агента относительно домашнего местоположения мобильных узлов **могут** применяться иные механизмы для перехвата пакетов, адресованных на домашние адреса мобильных узлов. Рассмотрение этих вариантов выходит за рамки данного документа.

Аналогично, мобильный узел и текущий или будущий внешний агент **должны** быть способны обмениваться дейтаграммами без привлечения стандартных механизмов маршрутизации IP (т. е., механизмы, принимающие решение о пересылке на основе адреса получателя в заголовках IP). Это требование может быть выполнено, если внешний агент и подключившийся мобильный узел имеют интерфейсы в одну сеть (канал). В этом случае мобильный узел и внешний агент при обмене дейтаграммами могут обойтись без вовлечения обычных механизмов маршрутизации IP, адресуя пакеты канального уровня соответствующему получателю канального уровня. При других вариантах взаимного расположения мобильного узла и внешнего агента **могут** применяться иные механизмы обеспечения обмена дейтаграммами между ними, но этот вопрос выходит за рамки данного документа.

Если мобильный узел использует совмещённый адрес обслуживания (см. п (b) выше), он **должен** размещаться в сети, указанной префиксом адреса обслуживания. Иначе дейтаграммы, направленные по адресу обслуживания, не будут доставлены.

1.8. Расширяемость протокола и формата сообщений

Mobile IP определяет набор управляющих сообщений, передаваемых по протоколу UDP [37] через порт 434. В данном документе определены два типа сообщений:

1 Registration Request (запрос регистрации)

3 Registration Reply (регистрационный отклик)

Актуальные значения для типов сообщений Mobile IP указаны в документе Assigned Numbers[1] [40].

Кроме того для обнаружения агентов (Agent Discovery) Mobile IP использует сообщения Router Advertisement и Router Solicitation, определённые для ICMP Router Discovery [10].

Mobile IP определяет общий механизм расширения (Extension), позволяющий передавать дополнительную информацию в управляющих сообщениях Mobile IP и сообщениях ICMP Router Discovery. Некоторые расширения представляются в формате TLV[2], описанном в параграфе 1.9.

Расширения позволяют передавать в каждой дейтаграмме переменный объем информации. Завершение списка расширений указывается полем общего размера дейтаграммы IP.

В Mobile IP используется два набора номерных пространств для значения Extension Type:

- Первый набор включает расширения, которые могут включаться только в управляющие сообщения Mobile IP (передаются по протоколу UDP через порт 434). В этом документе определены три типа расширений для управляющих сообщений Mobile IP:

  32 Mobile-Home Authentication;

  33 Mobile-Foreign Authentication;

  34 Foreign-Home Authentication.

- Второй набор включает расширения, которые могут включаться только в сообщения ICMP Router Discovery [10]. Данный документ определяет три типа таки расширений:

  0 One-byte Padding (однобайтовое заполнение, без полей Length и Data);

[1] В настоящее время этот документ утратил силу. Информация о типах сообщений доступна по ссылке. *Прим. перев.*
[2] Type-Length-Value - тип-размер-значение.

16 Mobility Agent Advertisement (анонс мобильного агента);

19 Prefix-Lengths (размеры префиксов).

Каждое расширение подробно будет описано ниже. Актуальные значения Extension Type можно найти в свежей версии Assigned Numbers [40].

По причине разделения (ортогональности) этих множеств в будущем номера типов для расширений из разных множеств могут совпадать. Это не создаст проблем, поскольку одни расширения могут применяться только в управляющих сообщениях Mobile IP, а другие - только в сообщениях ICMP Router Discovery.

Поле типа в структуре расширения Mobile IP может поддерживать до 255 (пропускаемых и непропускаемых) уникально идентифицируемых расширений. Когда расширение из любого набора со значением типа от 0 до 127 не распознаётся, сообщение с таким расширением **должно** отбрасываться без уведомления. Если не распознаётся расширение со значением типа от 128 до 255, это конкретное расширение игнорируется, но остальные расширения и данные сообщения **должны** обрабатываться. Поле Length в Extension используется для пропуска поля Data при поиске следующего расширения.

Пока для типов расширений не используется дополнительная структура, новые разработки или дополнения к Mobile IP могут потребовать столько расширений, что доступного для типов расширения пространства окажется не достаточно. Для решения этой проблемы предложены две новых структуры расширения. Некоторые типы расширений можно агрегировать, используя подтипы для точной идентификации (например, это возможно для расширений Generic Authentication Keys [35]). Во многих случаях это позволяет снизить скорость добавления новых значений для поля типа.

Поскольку новые структуры повышают эффективность использования пространства типов расширений, рекомендуется для новых расширений Mobile IP следовать одному из двух предложенных форматов, если возможна группировка связанных расширений.

В последующих параграфах более подробно рассмотрены три разных структуры для расширений Mobile IP:

- простой формат;
- длинный формат;
- короткий формат.

1.9. Формат TLV для расширений Mobile IP

Для расширений, определённых в этом документе применяется формат TLV, показанный на рисунке 2. Поскольку эта простая структура не обеспечивает повышения эффективности использования пространства типов расширений, для новых расширений Mobile IP рекомендуется использовать один из новых форматов, описанных в параграфах 1.10 и 1.11, если расширения поддерживают группировку.

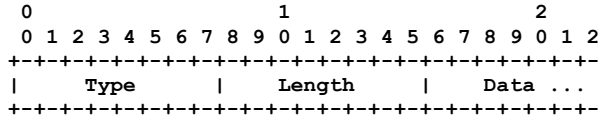


Рисунок 2. Формат TLV для расширений Mobile IPv4.

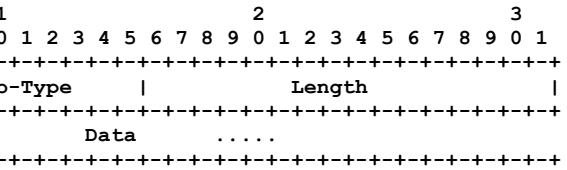
Type
Указывает конкретный тип расширения.

Length
Указывает размер поля данных расширения в байтах. Размер **не** учитывает два байта полей Type и Length.

Data
Связанные с расширением данные, формат и размер которых определяется значениями полей Type и Length.

1.10. Длинный формат расширения

Этот формат применим для непропускаемых расширений, которые могут содержать более 256 данных.



Длинный формат расширения требует наличия в начале заголовка следующих полей.

Type
Поле типа, описывающее набор однотипных расширений.

Sub-Type
Уникальный номер каждого элемента в группе расширений.

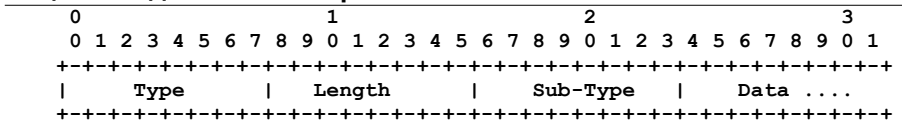
Length
Размер поля данных расширения в байтах. 4 октета полей Type, Length и Sub-Type в размере не учитываются.

Data
Данные, связанные с конкретным подтипом расширения. Структура данных в этой спецификации не задаётся.

16-битовое поле размера позволяет данным расширения превышать размер 256 байтов.

1.11. Короткий формат расширения

Этот формат совместим с пропускаемыми расширениями, которые определены в параграфе 1.9, но не применим с расширениями, включающими более 256 байтов данных (для них используется формат, описанный в параграфе 1.10).



Короткий формат требует присутствия в начале расширения перечисленных ниже полей.

Type
Поле типа, описывающее набор однотипных расширений.

Sub-Type
Уникальный номер каждого элемента в группе расширений.

Length
8-битовое целое число без знака, которое показывает размер расширения без учёта полей Type и Length (1 + размер поля Data).

Data
Данные, связанные с конкретным подтипом расширения. Структура данных в этой спецификации не задаётся.

2. Обнаружение агента

Agent Discovery является методом, с помощью которого мобильный узел определяет подключён он в данный момент к чужой или домашней сети, а также фиксирует перемещение из одной сети в другую. При подключении к чужой сети сети описанные в этом разделе методы также позволяют мобильному узлу определить адрес внешнего агента, предлагаемый им в качестве адреса обслуживания мобильных узлов.

Mobile IP расширяет механизм Router Discovery [10] для использования в целях обнаружения агента. Сообщения Agent Advertisement формируются путём включения расширений Mobility Agent Advertisement в сообщения ICMP Router Advertisement (параграф 2.1). Сообщение Agent Solicitation идентично ICMP Router Solicitation, за исключением того, что **должно** устанавливаться IP TTL = 1 (параграф 2.2). В этом разделе рассматриваются форматы сообщений и процедуры, с помощью которых мобильные узлы в кооперации с домашними и внешними агентами реализуют механизм Agent Discovery.

Сообщения Agent Advertisement и Agent Solicitation могут не требоваться для канальных уровней, где такая функциональность уже присутствует. Метод организации мобильным узлом соединений с потенциальными агентами на канальном уровне выходит за рамки данного документа (см. Приложение B). Описанные ниже процедуры предполагают наличие такого соединения на канальном уровне.

Для сообщений Agent Advertisement и Agent Solicitation не требуется аутентификации. Они **могут** быть аутентифицированы с помощью IP Authentication Header [22], но это не связано с описываемыми здесь сообщениями. Дополнительная спецификация процедур аутентификации сообщений Advertisement и Solicitation выходит за рамки данного документа.

2.1. Анонсы агента

Сообщения Agent Advertisement передаются в канал агентом мобильности для анонсирования своих услуг. Мобильные узлы используют эти анонсы для определения своей текущей точки подключения к Internet. Agent Advertisement представляет собой сообщение ICMP Router Advertisement, в которое добавлено расширение Mobility Agent Advertisement (параграф 2.1.1) и могут быть также добавлены расширения Prefix-Lengths (параграф 2.1.2), One-byte Padding (параграф 2.1.3) и другие расширения, которые будут добавлены в будущем.

В сообщении Agent Advertisement поля ICMP Router Advertisement должны соответствовать перечисленным ниже дополнительным требованиям.

- Поля канального уровня

  Destination Address

  Адрес получатель на канальном уровне в индивидуальном сообщении Agent Advertisement **должен** совпадать с канальным адресом отправителя в сообщении Agent Solicitation, вызвавшем Advertisement.

- Поля IP

  TTL

  Во всех сообщениях Agent Advertisement **должно** устанавливаться TTL = 1.

  Destination Address

  Как указано в [10] для сообщений ICMP Router Discovery, IP-адрес получателя группового сообщения Agent Advertisement **должен** быть 224.0.0.1 (все системы на канале) [11] или 255.255.255.255 (ограниченное широковещание). Широковещательный адрес подсети (subnet-directed broadcast) вида <prefix>.<-1> использовать не допустимо, поскольку мобильным узлам обычно не известен префикс чужой сети. Если сообщение Agent Advertisement передаётся индивидуально мобильному узлу, в качестве Destination Address **следует** использовать домашний IP-адрес мобильного узла.

- Поля ICMP

  Code

  Поле Code в анонсах агентов интерпретируется следующим образом:

  0 - агент мобильности обслуживает трафик общего назначения (т. е., действует в качестве маршрутизатора дейтаграмм IP не только мобильных узлов);

  16 - агент мобильности не маршрутизирует трафик общего назначения. Однако все внешние агенты **должны** (как минимум) пересылать используемому по умолчанию все дейтаграммы, полученные от зарегистрированного мобильного узла (параграф 4.2.2).

Lifetime

Максимальное время, в течение которого сообщение Advertisement считается корректным при отсутствии других анонсов.

Router Address(es)

Адреса, которые могут присутствовать в этой части Agent Advertisement, рассмотрены в параграфе 2.3.1.

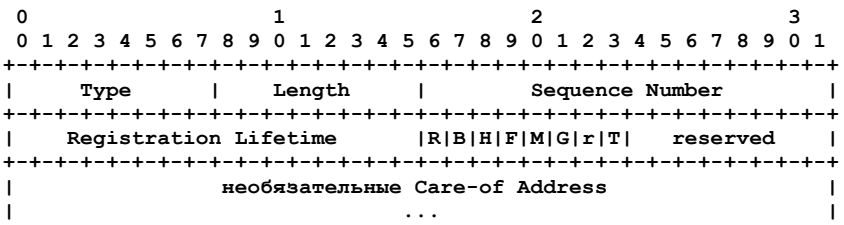
Num Addrs

Число адресов маршрутизаторов, анонсируемых в этом сообщении. Отметим, что в сообщении Agent Advertisement число адресов маршрутизаторов, заданных в ICMP Router Advertisement, **может** быть нулевым. Дополнительная информация приведена в параграфе 2.3.1.

При периодической передаче интервал между сообщениями Agent Advertisement **следует** делать не более 1/3 от анонсируемого значения Lifetime в заголовке ICMP. Этот интервал **может** быть короче 1/3 анонсируемого значения Lifetime. Это позволяет мобильному узлу не удалять агента из своего списка подходящих агентов даже при пропуске трёх анонсов подряд. Реальное время передачи каждого анонса **следует** менять на случайную величину [10] для предотвращения синхронизации и последующих конфликтов с анонсами от других агентов (или с анонсами Router Advertisement от других маршрутизаторов). Отметим, что это поле не связано с полем Registration Lifetime в определённом ниже расширении Mobility Agent Advertisement.

2.1.1. Расширение для анонсов мобильного агента

Расширение Mobility Agent Advertisement использует поля анонса ICMP Router Advertisement. Это расширение служит для индикации того, что сообщение ICMP Router Advertisement является также анонсом агента (Agent Advertisement), переданным мобильным агентом. Формат Mobility Agent Advertisement Extension показан ниже.



Type

16

Length

(6 + 4*N), где 6 учитывает число байтов в полях Sequence Number, Registration Lifetime, флагах и резервных битах, а N задаёт число анонсируемых адресов обслуживания.

Sequence Number

Число сообщений Agent Advertisement, переданных с момента инициализации агента (см. параграф 2.3.2).

Registration Lifetime

Максимальное время жизни (в секундах), которое этот агент будет принимать в запросах Registration. 0xffff задаёт бесконечное время. Это поле не связано с полем Lifetime в части ICMP Router Advertisement анонсов агента.

R

Требуется регистрация. Регистрация на данном (или другом на том же канале) внешнем агенте требуется даже при использовании совмещённого адреса обслуживания.

B

Занят. Внешний агент не принимает регистрацию для дополнительных мобильных узлов.

H

Домашний агент. Предлагает услуги домашнего агента на канале, в который передан анонс Agent Advertisement.

F

Внешний агент. Предлагает услуги внешнего агента на канале, в который передан анонс Agent Advertisement.

M

Минимальная инкапсуляция. Агент принимает туннелированные дейтаграммы с минимальной инкапсуляцией [34].

G

Инкапсуляция GRE. Агент принимает туннелированные дейтаграммы с инкапсуляцией GRE [16].

r

0 при передаче, игнорируется на приёмной стороне. **Не следует** использовать для каких-либо иных целей.

T

Внешний агент поддерживает обратное туннелирование [27].

reserved

0 при передаче, игнорируется на приёмной стороне.

Care-of Address(es)

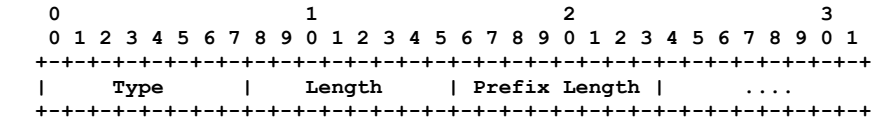
Анонсированный адрес (адреса) внешнего агента, обеспечиваемый этим агентом. Сообщение Agent Advertisement **должно** включать хотя бы один адрес обслуживания, если установлен бит F. Число представленных адресов обслуживания определяется значением поля Length в расширении.

Домашний агент **должен** быть постоянно готов к обслуживанию мобильных узлов, для которых он служит домашним агентом. Внешний агент может оказаться перегруженным и не будет способен обслуживать дополнительные узлы. В таких случаях он должен продолжать передачу сообщений Agent Advertisement, чтобы зарегистрированные мобильные узлы знали, что агент работает и продолжает их обслуживание. Внешний агент может указать свою чрезмерную загрузку (too busy), чтобы позволить регистрацию новых мобильных узлов, устанавливая бит B в своих сообщениях Agent Advertisement. В анонсах агента **недопустимо** устанавливать одновременно биты B и F. Кроме того, один из битов F или H **должен** быть установлен во всех передаваемых сообщениях Agent Advertisement.

Если внешний агент требует регистрации даже для мобильных узлов с совмещённым адресом обслуживания, он устанавливает бит R. Поскольку этот флаг применим только для внешних агентов, **не допускается** установка R при сброшенном флаге F.

2.1.2. Расширение Prefix-Lengths

Расширение Prefix-Lengths **может** следовать за расширением Mobility Agent Advertisement. Оно служит для индикации числа битов в сетевом префиксе для каждого адреса Router Address в списке ICMP Router Advertisement сообщения Agent Advertisement. Отметим, что размер префикса **не относится** к адресам обслуживания в расширении Mobility Agent Advertisement. Формат расширения Prefix-Lengths показан ниже.



Type

19 (Prefix-Lengths Extension)

Length

N, где N - значение (возможно 0) поля Num Addrs в части ICMP Router Advertisement анонса Agent Advertisement.

Prefix Length

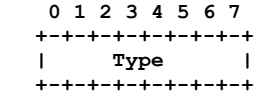
Число старших битов, определяющих номер сети для соответствующего Router Address в ICMP Router Advertisement данного сообщения. Размер префикса для каждого Router Address представляется отдельным байтом в порядке следования полей Router Address в ICMP Router Advertisement.

В параграфе 2.4.2 рассмотрено, как с помощью расширения Prefix-Lengths мобильный узел **может** определить факт своего перемещения в другую сеть. Детали использования расширения приведены в Приложении E.

2.1.3. Расширение для однобайтового заполнения

Некоторым реализациям протокола IP нужно заполнение сообщений ICMP для выравнивания по чётному размеру. Если размер ICMP в анонсе Agent Advertisement нечётный, **может** использоваться данное расширение для увеличения размера до чётного. Отметим, что это расширение **не** относится к числу расширений общего назначения для выравнивания различных полей Agent Advertisement. В анонсы Agent Advertisement **не следует** включать более одного расширения One-byte Padding Extension и при наличии этого расширения его **следует** размещать последним в Agent Advertisement.

Отметим, что в отличии от других расширений, используемых Mobile IP, расширение One-byte Padding Extension представляется одним байтом без полей Length и Data. Формат расширения One-byte Padding показан ниже.



Type

0 (One-byte Padding Extension)

2.2. Сообщение Agent Solicitation

Сообщение Agent Solicitation идентично ICMP Router Solicitation, но поле IP TTL **должно** иметь значение 1.

2.3. Внешний агент и домашний агент

Любой агент мобильности, который не может быть обнаружен протоколом канального уровня,, **должен** передавать анонсы Agent Advertisement. Анонсам, которые могут быть обнаружены протоколом канального уровня, **следует** также реализовать Agent Advertisement. Однако анонсы не требуется передавать за исключениям ситуаций, когда политика сайта требует регистрации (установлен бит R), или в качестве отклика на конкретное сообщение Agent Solicitation. Все агенты мобильности **должны** обрабатывать полученные пакеты, направленные в группу Mobile-Agents по адресу 224.0.0.11. Мобильный **узел** может отправлять сообщения Agent Solicitation по адресу 224.0.0.11. Все агентам мобильности **следует** отвечать на сообщения Agent Solicitation.

Одни и те же процедуры, параметры по умолчанию и константы используются в сообщениях Agent Advertisement и сообщениях Agent Solicitation, как указано для ICMP Router Discovery в [10], за исключением перечисленного ниже.

- Агент мобильности **должен** ограничивать скорость передачи широковещательных и групповых сообщений Agent Advertisement; максимальную скорость **следует** выбирать так, чтобы анонсы не отнимали значительную часть пропускной способности сети;

- мобильному агенту, получившему Router Solicitation, **недопустимо** требовать, чтобы в поле IP Source Address был указан адрес соседа (т. е., соответствовал подсети, связанной с одним из адресов интерфейса, через который пришло сообщение).

- Агент мобильности **может** быть настроен на передачу сообщений Agent Advertisementстолько в ответ на сообщения Agent Solicitation.

Если домашняя сеть не является виртуальной, домашний агент для любого мобильного узла **следует** размещать на канале, идентифицируемом домашним адресом мобильного узла, а передаваемые домашним агентом в этот канал сообщения Agent Advertisement **должны** иметь флаг H. Благодаря этому, мобильный узел в своей домашней сети может определить, что он находится дома. В любых сообщениях Agent Advertisement, передаваемых домашним агентом в другие каналы, к которым он подключён (если агент мобильности обслуживает более одного канала), **недопустимо** устанавливать бит H, если этот агент не является домашним и для данного канала (для других мобильных узлов). Агент мобильности **может** использовать разные установки для битов R, H и F на каждом сетевом интерфейсе.

Если домашняя сеть является виртуальной, она не имеет физической реализации, внешней по отношению к домашнему агенту. В этом случае нет физического сетевого соединения, в которое передаются сообщения Agent Advertisement, анонсирующие домашний агент. Мобильные пользователи, для которых такая сеть является домашней, всегда трактуются, как находящиеся дома.

В конкретной подсети все агенты мобильности **должны** включать расширение Prefix-Lengths Extension или все они **должны** отказаться от его использования. Иными словами, недопустимо использование данного расширения одними агентами в подсети, тогда как другие агенты в той же подсети не будут его включать. В противном случае один из алгоритмов детектирования перемещений для мобильных узлов не будет работать корректно (параграф 2.4.2).

2.3.1. Анонсируемые адреса маршрутизатора

Часть ICMP Router Advertisement анонса Agent Advertisement **может** включать один или множество адресов маршрутизаторов. Агенту **следует** помещать в анонс только свои собственные адреса (если они есть). Независимо от наличия его адреса в поле Router Address, внешний агент **должен** маршрутизировать дейтаграммы, полученные от зарегистрированных мобильных узлов (параграф 4.2.2).

2.3.2. Порядковые номера

Порядковые номера в Agent Advertisement лежат в диапазоне от 0 до 0xffff. После загрузки агент **должен** использовать в первом анонсе номер 0. В каждом последующем анонсе номер должен увеличиваться на 1, за исключением того, что после номера 0xffff **должен** следовать номер 256. Это позволяет мобильному узлу различать ситуации, когда порядковый номер меняется в результате перезагрузки агента или по причине достижения верхнего передела.

2.4. Мобильный узел

Каждый мобильный узел **должен** поддерживать сообщения Agent Solicitation. Ходатайства **следует** передавать лишь при отсутствии анонсов Agent Advertisement, если адрес обслуживания ещё не был определён через протокол канального уровня или иным способом. Мобильный узел использует те же процедуры, значения по умолчанию и константы для Agent Solicitation, что указаны для сообщений ICMP Router Solicitation в [10], за исключением того, что мобильный узел **может** ходатайствовать более часто, чем 1 раз в 3 секунды, а не подключенный к внешнему агенту мобильный узел **может** передавать больше запросов, чем задаёт MAX_SOLICITATIONS.

Скорость передачи ходатайств мобильным узлом **должна** быть ограничена этим узлом. Мобильный узел **может** передать три начальных ходатайства с максимальной скоростью 1 сообщение в секунду, пока происходит поиск агента. После этого скорость передачи ходатайств **должна** быть снижена для ограничения нагрузки на локальный канал. Последующие ходатайства **должны** передаваться с использованием механизма экспоненциального роста интервала, который обеспечивает удвоение интервала перед отправкой каждого следующего сообщения, вплоть да заданного максимума. Максимальный интервал **следует** выбирать с учётом среды, через которую подключён мобильный узел. Значение максимального интервала **следует** задавать не менее 1 минуты.

Пока продолжается поиск агента мобильному узлу **недопустимо** повышать скорость передачи ходатайств, если он не имеет подтверждения своего перехода на другой канал. После регистрации мобильному узлу также **следует** повысить скорость передачи ходатайств при начале поиска нового агента для регистрации. При увеличении скорость **может** достигнуть максимального значения, но она **должна** ограничиваться, как указано выше. Для всех случаев рекомендуемые интервалы отправки ходатайств являются номинальными значениями. Мобильные узлы **должны** вносить случайные изменений в эти номинальные интервалы, как указано для ICMP Router Discovery [10].

Мобильные узлы **должны** обрабатывать полученные анонсы Agent Advertisement. Мобильный узел может отличить сообщение Agent Advertisement от других применений сообщения ICMP Router Advertisement, проверяя число анонсируемых адресов и поле IP Total Length. Если общий размер IP показывает, что сообщение ICMP длиннее, чем требуется для указанного числа анонсируемых адресов, остальные данные интерпретируются как одно или несколько расширений. Наличие расширения Mobility Agent Advertisement Extension идентифицирует сообщение, как анонс Agent Advertisement.

Если анонсируется более одного адреса, мобильному узлу **следует** выбрать первый адрес для своей начальной попытки регистрации. Если попытка регистрации не удалась и код указывает отказ со стороны внешнего агента, мобильный узел **может** повторить попытки для каждого анонсируемого адреса.

При использовании множества методов обнаружения агента мобильному узлу **следует** сначала предпринять попытку регистрации у агентов, включивших расширения Mobility Agent Advertisement в свои анонсы и лишь после этого использовать агентов, открытых иными способами. Такая регистрация будет признана с максимальной вероятностью и это позволяет снизить число попыток.

Мобильный узел **должен** игнорировать резервные биты в анонсах Agent Advertisement, не отбрасывая самих анонсов. В этом случае даже после добавки новых битов мобильные узлы смогут пользоваться не до конца понятными им анонсами.

2.4.1. Требование регистрации

Когда мобильный узел получает анонс Agent Advertisement с установленным битом R, ему **следует** выполнять регистрацию через внешний агент даже при наличии возможности получения своего совмещённого адреса обслуживания. Это предназначено для обеспечения сайтам возможности реализации правил посещения (например, учёта), требующих проверки полномочий.

Если некоторые зарезервированные ранее биты требуют того или иного мониторинга/исполнения на внешнем канале, поддерживающие новую спецификацию внешние агенты могут устанавливать бит R. Это вынудит мобильные узлы регистрироваться через данного агента, что позволит ему контролировать/требовать выполнение правил.

2.4.2. Детектирование перемещений

Для мобильных узлов обеспечиваются два основных механизма детектирования перехода из одной подсети в другую. **Могут** использоваться также иные механизмы. Мобильному узлу, обнаружившему своё перемещение, **следует** зарегистрироваться (раздел 3) с подходящим адресом обслуживания в новой внешней сети. Однако мобильным узлам **недопустимо** регистрироваться чаще одного раза в секунду (в среднем), как указано в параграфе 3.6.3.

2.4.2.1. Алгоритм 1

Первый метод детектирования перемещений основан на использовании поля Lifetime в основном теле части ICMP Router Advertisement сообщения Agent Advertisement. Мобильному узлу **следует** сохранять значение, полученное в анонсах Agent Advertisement до истечения времени Lifetime. Если мобильный узел не получает другого анонса от того же агента в течение времени, заданного Lifetime, ему **следует** считать, что контакт с агентом потерян. Если мобильный узел при этом получил сообщение Agent Advertisement от другого агента, для которого время Lifetime ещё не истекло, он **может** незамедлительно попытаться зарегистрироваться у этого агента. В противном случае мобильному узлу **следует** предпринять попытку обнаружения нового агента для регистрации.

2.4.2.2. Алгоритм 2

Во втором методе используются сетевые префиксы. В некоторых случаях мобильные узлы **могут** использовать расширение Prefix-Lengths для определения принадлежности недавно полученного анонса Agent Advertisement к той же подсети, из которой взят адрес обслуживания мобильного узла. Если префиксы различаются, мобильный узел **может** предполагать своё перемещение. Если мобильный узел в данный момент пользуется адресом внешнего агента, ему **не следует** применять этот метод детектирования перемещений, если в анонсах нового и текущего агентов не присутствует расширение Prefix-Lengths. Аналогично при использовании мобильным узлом совмещённого адреса обслуживания узлу **не следует** применять этот метод, если новый агент не включает расширение Prefix-Lengths в свои анонсы или мобильному узлу не известен сетевой префикс для своего текущего совмещённого адреса обслуживания. При завершении срока текущей регистрации, если данный метод говорит о перемещении мобильного узла, данный узел **может** зарегистрироваться на внешнем агенте, передавшем новое сообщение Agent Advertisement с другим сетевым префиксом. **Недопустимо** в таких случаях регистрироваться с использованием сообщения Agent Advertisement, для которого истёк срок, заданный полем Lifetime.

2.4.3. Возвращение в домашнюю сеть

Мобильный узел может обнаружить свой возврат в домашнюю сеть при получении анонса Agent Advertisement от своего домашнего агента. В этом случае мобильному узлу **следует** отменить регистрацию на своём домашнем агенте (раздел 3). Перед попыткой дерегистрации мобильному узлу **следует** настроить свою таблицу маршрутизации на домашнюю сеть (параграф 4.2.1). Кроме того, если домашняя сеть использует ARP [36], мобильный узел **должен** выполнить процедуры, описанные в параграфе 4.6 применительно к ARP, proxy ARP и gratuitous (беспричинный) ARP.

2.4.4. Порядковые номера

Если мобильный узел обнаруживает два последовательных значения порядковых номеров в сообщениях Agent Advertisement от внешнего агента, где он зарегистрирован, и второй номер меньше первого и лежит в диапазоне от 0 до 255, данному узлу **следует** зарегистрироваться заново. Если второе значение меньше первого, но не меньше 256, мобильному узлу **следует** считать, что нумерация достигла максимума (0xffff) и пошла на следующий круг. Повторная регистрация в этом случае не требуется (параграф 2.3).

Регистрация Mobile IP обеспечивает мобильным узлам гибких механизм обмена текущей информацией о доступности со своим домашним агентом. Это представляет собой метод, с помощью которого мобильные узлы

- запрашивают обслуживание при подключении к чужой сети;
- информируют домашний агент о своём текущем адресе обслуживания;
- обновляют регистрацию по её завершении;
- отменяют внешнюю регистрацию при возврате домой.

Регистрационные сообщения обеспечивают обмен информацией между мобильным узлом, (опционально) внешним агентом и домашним агентом. Регистрация организует или меняет привязку мобильности на домашнем агенте, связывающую домашний адрес мобильного узла с текущим адресом его обслуживания на время, заданное Lifetime.

В регистрационной процедуре поддерживается ряд опциональных возможностей, доступных мобильному узлу:

- определение мобильным узлом своего домашнего адреса (если он не указан в конфигурации);
- поддержка множества одновременных регистраций для туннелирования копий каждой дейтаграммы по всем активным адресам обслуживания;
- дерегистрация конкретного адреса обслуживания с сохранением других привязок мобильности;
- определение адреса домашнего агента, если он не задан в настройках мобильного узла.

3.1. Обзор регистрации

Mobile IP определяет две разных процедуры регистрации. Одна из процедур использует внешний агент, который транслирует регистрацию домашнему агенту мобильного узла, а во второй регистрация происходит напрямую на домашнем агенте. Приведённые ниже правила определяют выбор конкретной процедуры для тех или иных условий:

- если мобильный узел регистрирует адрес внешнего агента, он **должен** делать это через данного агента;
- если мобильный узел использует совмещённый адрес обслуживания и получил анонс Agent Advertisement от внешнего агента на канале, где он использует данный адрес обслуживания, мобильному узлу **следует** регистрироваться через данный внешний агент (или другой внешний агент на данном канале), если в полученном анонсе был установлен бит R;
- в остальных случаях при использовании совмещённого адреса обслуживания мобильный узел **должен** регистрироваться непосредственно на своём домашнем агенте;
- если мобильный узел вернулся в свою домашнюю сеть, он **должен** регистрироваться непосредственно на своём домашнем агенте.

Обе процедуры регистрации включают обмен сообщениями Registration Request и Registration Reply (параграфы 3.3 и 3.4). При регистрации через внешний агент процедура требует использования четырёх сообщений:

a) мобильный узел передаёт Registration Request подходящему внешнему агенту для начала процесса;

b) внешний агент обрабатывает запрос и транслирует его домашнему агенту;

c) домашний агент передаёт Registration Reply внешнему агенту, принимая или отвергая полученный запрос;

d) внешний агент обрабатывает Registration Reply и транслирует его мобильному узлу для информирования того о результате рассмотрения запроса.

При регистрации непосредственно на домашнем агенте процедура требует двух сообщений:

a) мобильный узел передаёт Registration Request домашнему агенту;

b) домашний агент передаёт мобильному узлу Registration Reply, принимая или отвергая запрос.

Регистрационные сообщения, определённые в параграфах 3.3 и 3.4, используют протокол UDP[1] [37]. В заголовок **следует** включать отличную от нуля контрольную сумму UDP, а получатель **должен** проверять эту сумму. Получателям **следует** воспринимать пакеты с нулевой контрольной суммой UDP. Поведение мобильного узла и домашнего агента в части восприятия пакетов с нулевым значением контрольной суммы UDP **следует** согласовывать в рамках связи Mobility Security Association между сторонами.

3.2. Аутентификация

Каждый мобильный узел, домашний и внешний агент **должны** обеспечивать поддержку связей Mobility Security Association для мобильных узлов, индексируемых по их SPI и адресам IP. Для мобильного узла должна использоваться индексация по его домашнему адресу. Требования по поддержке алгоритмов аутентификации приведены в параграфе 5.1. Регистрационные сообщения между мобильным узлом и его домашним агентом **должны** аутентифицироваться с поддерживающим проверку полномочий расширением (см., например, Mobile-Home Authentication Extension в параграфе 3.5.2). Это расширение **должно** быть первым аутентификационным расширением. В сообщение **могут** добавляться другие расширения, специфичные для внешнего агента, после того, как аутентификация завершится.

3.3. Запрос регистрации

Мобильный узел регистрируется на своём домашнем агенте, используя сообщения Registration Request, чтобы домашний агент мог создать или изменить привязку мобильности для этого узла (например, скорректировать Lifetime). Запрос может быть оттранслирован домашнему агенту внешним агентом, через который регистрируется мобильный узел, или передан напрямую при регистрации мобильным узлом совмещённого адреса обслуживания.

Поля IP

Source Address - обычно адрес интерфейса, с которого передаётся сообщение.

Destination Address - обычно адрес домашнего или внешнего агента.

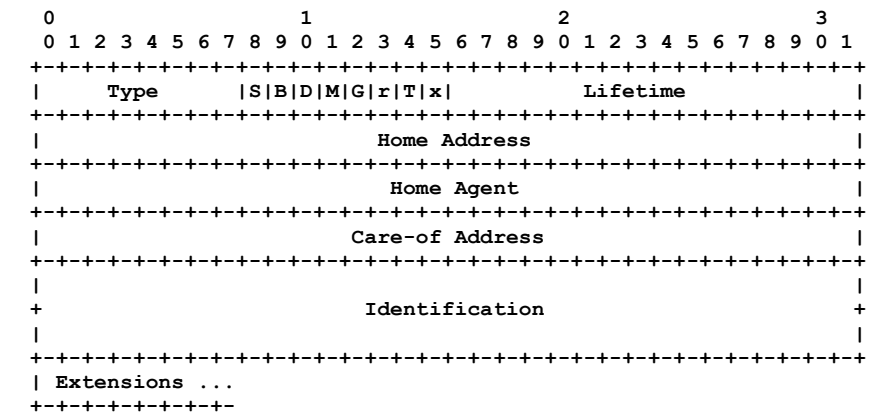
Дополнительная информация приведена в параграфах 3.6.1.1 и 3.7.2.2.

Поля UDP

Source Port - переменное.

Destination Port - 434.

Заголовок UDP, следующий за полями Mobile IP, показан ниже.



Type

1 (Registration Request)

S

Одновременные (Simultaneous) привязки. Если бит S установлен, мобильный узел запрашивает у домашнего агента сохранение имеющихся привязок мобильности, как описано в параграфе 3.6.1.2.

B

Широковещательные (Broadcast) дейтаграммы. Установленный бит B показывает запрос мобильного узла к домашнему агенту на пересылку в туннель всех широковещательных дейтаграмм из домашней сети, как описано в параграфе 4.3.

[1]User Datagram Protocol - протокол пользовательских дейтаграмм.

D

Декапсуляция (Decapsulation) мобильным узлом. Установленный флаг D показывает, что мобильный узел желает самостоятельно декапсулировать дейтаграммы, направленные по адресу обслуживания. Это говорит об использовании мобильным узлом совмещённого адреса обслуживания.

M

Минимальная (Minimal) инкапсуляция. Установленный бит M означает, что домашний агент использует минимальную инкапсуляцию [34] для туннелируемых мобильному узлу дейтаграмм.

G

Инкапсуляция GRE. Установленный бит G говорит о том, что мобильный узел запрашивает у своего домашнего агента использование инкапсуляции GRE [16] для туннелируемых мобильному узлу дейтаграмм.

r

На передающей стороне устанавливается 0, при получении игнорируется. Не **следует** использовать этот бит для каких-либо целей.

T

Запрошено обратное туннелирование (см. [27]).

x

На передающей стороне устанавливается 0, при получении игнорируется.

Lifetime

Число секунд, остающихся до завершения срока действия регистрации. Нулевое значение указывает запрос отмены регистрации, значение 0xffff показывает неограниченный срок регистрации.

Home Address

IP-адрес мобильного узла.

Home Agent

IP-адрес домашнего агента мобильного узла.

Care-of Address

IP-адрес точки завершения туннеля (к мобильному узлу).

Identification

64-битовое число, создаваемое мобильным узлом и служащее для сопоставления запросов и откликов на них, а также защиту от атак с повторным использованием регистрационных сообщений (см. параграфы 5.4 и 5.7).

Extensions

За фиксированной частью Registration Request может следовать одно или несколько расширений, описанных в параграфе 3.5. В запросы **должно** включаться расширение для проверки полномочий. Порядок, в котором **должны** следовать расширения при их включении в запросы регистрации описан в параграфах 3.6.1.3 и 3.7.2.2.

3.4. Регистрационный отклик

Агент мобильности обычно возвращает сообщение Registration Reply мобильному узлу, передавшему Registration Request. Если мобильный узел запрашивает обслуживание у внешнего агента, этот агент обычно получает отклик от домашнего агента этого мобильного узла и пересылает его мобильному узлу. Отклики содержат коды, требуемые для информирования мобильного узла о состоянии его запроса и выделенном домашним агенте сроке регистрации, который может оказаться меньше запрошенного.

Внешнему агенту **недопустимо** увеличивать значение Lifetime, указанное мобильным узлом в сообщении Registration Request, поскольку поле Lifetime учитывается аутентификационным расширением, которое включает проверку полномочий на домашнем агенте. Такие расширения содержат аутентификационные данные, которые внешний агент не может корректно рассчитать. Домашнему агенту также **недопустимо** увеличивать значение Lifetime, указанное мобильным узлом в Registration Request, поскольку это может привести к выходу срока регистрации за пределы максимального значения Registration Lifetime, разрешаемого вешним агентом. Если значение Lifetime в полученном сообщении Registration Reply превышает значение в отправленном сообщении Registration Request, **должно** использоваться значение Lifetime из запроса. Если значение Lifetime в отклике меньше значения этого поля в запросе, **должно** использоваться значение Lifetime из сообщения Registration Reply.

Поля IP

Source Address - обычно копируется из поля Destination Address сообщения Registration Request, на которое агент отвечает. Дополнительная информация приведена в параграфах 3.7.2.3 и 3.8.3.1.

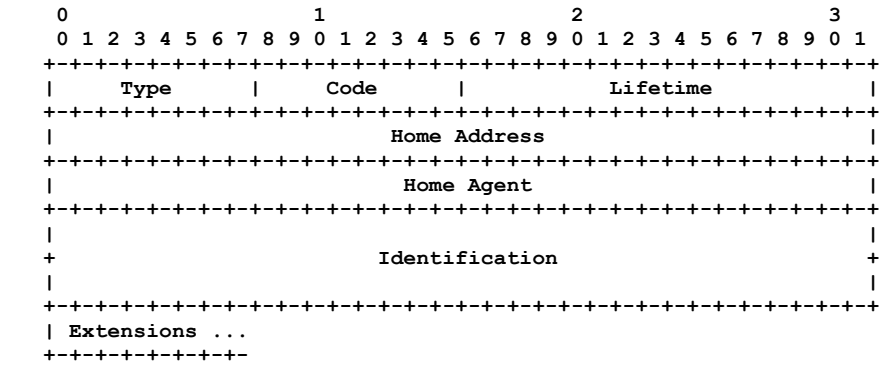
Destination Address - копируется из поля Source Address сообщения Registration Request, на которое агент отвечает.

Поля UDP

Source Port - переменный.

Destination Port - копируется из поля UDP Source Port соответствующего запроса (параграф 3.7.1).

Заголовок UDP, следующий за полями Mobile IP, показан ниже.



Type
3 (Registration Reply)

Code
Значение, показывающее результат обработки Registration Request. Значения кодов приведены ниже.

Lifetime
Если поле Code говорит, что регистрация была воспринята, в поле Lifetime указывается число секунд, оставшихся до завершения срока регистрации. Нулевое значение указывает отмену регистрации мобильного узла, значение 0xffff показывает неограниченный срок регистрации. Если значение Code говорит об отказе в регистрации, содержимое поля Lifetime не задаётся. и **должно** игнорироваться при получении.

Home Address
IP-адрес мобильного узла.

Home Agent
IP-адрес домашнего агента мобильного узла.

Identification
64-битовое число, создаваемое мобильным узлом и служащее для сопоставления запросов и откликов на них, а также защиту от атак с повторным использованием регистрационных сообщений. Значение определяется значением поля Identification из сообщения Registration Request от мобильного узла и стилем защиты от повторного использования пакетов в контексте защиты между мобильным узлом и домашним агентом (определяется Mobility Security Association и значением SPI в разрешающем проверку полномочий расширении). См. параграфы 5.4 и 5.7.

Extensions
За фиксированной частью запроса Registration Request может следовать одно или несколько расширений, описанных в параграфе 3.5. Разрешающее проверку полномочий расширение **должно** включаться во все регистрационные отклики, возвращаемые домашним агентом. Правила размещения расширений в откликах приведены в параграфах 3.7.2.2 и 3.8.3.3.

Ниже приведены значения, определённые для поля Code.

Успешная регистрация

0 регистрация принята;

1 регистрация принята, но одновременные привязки мобильности не поддерживаются.

Регистрация отвергнута внешним агентом

64 причина отказа не указана;

65 административный запрет;

66 недостаточно ресурсов;

67 отказ при аутентификации мобильного узла;

68 отказ при аутентификации домашнего агента;

69 запрошенное значение Lifetime слишком велико;

70 некорректный формат сообщения Request;

71 некорректный формат сообщения Reply;

72 запрошенная инкапсуляция не поддерживается;

73 резерв (не используется);

77 недопустимый адрес обслуживания;

78 тайм-аут при регистрации;

80 домашняя сеть недоступна (получена ошибка ICMP);

81 хост домашнего агента недоступен (получена ошибка ICMP);

82 порт домашнего агента недоступен (получена ошибка ICMP);

88 домашний агент недоступен (получена другая ошибка ICMP).

Регистрация отвергнута домашним агентом

128 причина не указана;

129 административный запрет;

130 недостаточно ресурсов;

131 отказ при аутентификации мобильного узла;

132 отказ при аутентификации внешнего агента;

133 несоответствие Identification;

134 некорректный формат сообщения Request;

135 слишком много одновременных привязок мобильности;

136 не известен адрес домашнего агента.

Актуальные значения кодов приведены в свежей редакции документа Assigned Numbers [40].

3.5. Регистрационные расширения

3.5.1. Расчёт значений аутентификационного расширения

Значение Authenticator, рассчитываемое для каждого аутентификационного расширения, **должно** защищать следующие поля регистрационного сообщения:

- данные UDP (т. е., данные Registration Request или Registration Reply);
- все предшествующие расширения целиком;
- поля Type, Length и SPI данного расширения.

По умолчанию используется алгоритм HMAC-MD5 [23] для расчёта 128-битовой цифровой подписи регистрационного сообщения. При расчёте HMAC учитываются следующие данные:

- данные UDP (т. е., данные Registration Request или Registration Reply);
- все предшествующие расширения целиком;
- поля Type, Length и SPI данного расширения.

Отметим, что само поле Authenticator и заголовок UDP **не** включаются по умолчанию в расчёт значения Authenticator. В параграфе 5.1 приведена информация о требованиях к поддержке для кодов аутентификации, которые применяются в различных аутентификационных расширениях.

Индекс параметров защиты (SPI[1]) в любом аутентификационном расширении определяет контекст защиты, который применяется для расчёта значения Authenticator и **должен** использоваться получателем для проверки принятого значения. В частности, SPI выбирает алгоритм и режим аутентификации (параграф 5.1), а также секрет (разделяемый ключ или подходящую пару из открытого и закрытого ключей), применяемый при расчёте значения Authenticator. Для обеспечения совместимости реализаций Mobile IP каждая реализация должна быть способна связать любое значение SPI с любым поддерживаемым алгоритмом и режимом аутентификации. Кроме того, все реализации Mobile IP **должны** поддерживать используемый по умолчанию алгоритм аутентификации HMAC-MD5, указанный выше.

3.5.2. Расширение Mobile-Home Authentication

Во всех сообщениях Registration Request, а также генерируемых домашним агентом сообщениях Registration Reply **должно** присутствовать в точности одно разрешающее аутентификацию расширение. Mobile-Home Authentication Extension всегда является разрешающим аутентификацию расширением для описанных в этом документе регистрационных сообщений. Это требование обусловлено необходимостью предотвращения проблем [2], возникающих в результате неконтролируемого распространения удалённых перенаправлений в Internet. Местоположение разрешающего аутентификацию расширения указывает окончание аутентифицируемых данных.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length    |          SPI  ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       ... SPI (cont.)           |       Authenticator ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type
32

Length
4 + число байтов в поле Authenticator.

SPI
Индекс параметров защиты (4 байта). Неразбираемый идентификатор (см. параграф 1.6).

Authenticator
(переменный размер) (см. параграф 3.5.1.)

3.5.3. Расширение Mobile-Foreign Authentication

Это расширение **может** включаться в регистрационные запросы и отклики при существовании между мобильным узлом и внешним агентом защищённой связи. Требования поддержки для кодов аутентификации сообщений описаны в параграфе 5.1.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length    |          SPI  ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       ... SPI (cont.)           |       Authenticator ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type
33

Length
4 + число байтов в поле Authenticator.

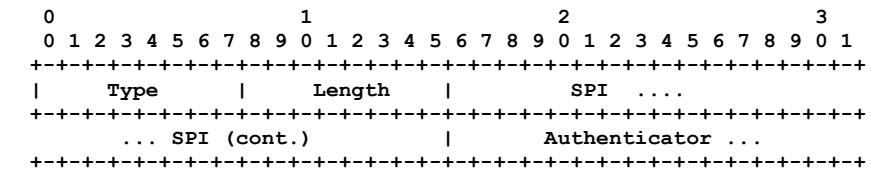
SPI
Индекс параметров защиты (4 байта). Неразбираемый идентификатор (см. параграф 1.6).

Authenticator
(переменный размер) (см. параграф 3.5.1.)

[1] Security Parameter Index.

3.5.4. Расширение Foreign-Home Authentication

Это расширение **может** включаться в регистрационные запросы и отклики при существовании между мобильным узлом и внешним агентом защищённой связи. Требования поддержки для кодов аутентификации сообщений описаны в параграфе 5.1.



Type

34

Length

4 + число байтов в поле Authenticator.

SPI

Индекс параметров защиты (4 байта). Неразбираемый идентификатор (см. параграф 1.6).

Authenticator

(переменный размер) (см. параграф 3.5.1.)

3.6. Мобильные узлы

На мобильном узле **должна** быть (статически или динамически) задана маска сети и Mobility Security Association для каждого из его домашних агентов. В дополнение к этому на мобильном узле **может** быть установлен домашний адрес и IP-адреса одного или нескольких домашних агентов. Если этого не сделано, мобильный узел **может** определить адрес домашнего агента, используя процедуры, описанные в параграфе 3.6.1.2.

Если на мобильном узле не настроен домашний адрес, он **может** использовать расширение Mobile Node Network Access (NAI) [6] для самоидентификации и установить в поле Home Address сообщения Registration Request значение 0.0.0.0. В таких случаях мобильный узел **должен** быть способен присвоить себе домашний адрес после извлечения нужной информации из сообщения Registration Reply от домашнего агента.

Для каждой ожидающей регистрации мобильный узел поддерживает следующую информацию:

- адрес канального уровня внешнего агента, которому было отправлено сообщение Registration Request (если такой адрес имеется),
- IP Destination Address из сообщения Registration Request,
- адрес обслуживания, используемый при регистрации,
- значение Identification, переданное при регистрации,
- запрошенное изначально значение Lifetime,
- оставшееся время Lifetime для ожидающей регистрации.

Мобильному узлу **следует** инициировать регистрацию при обнаружении смены своего подключения к сети. Методы, с помощью которых мобильный узел **может** это обнаружить, описаны в параграфе 2.4.2. При выходе мобильного узла из домашней сети сообщение Registration Request от такого узла позволяет домашнему агенту создать или изменить для этого узла привязку мобильности. Для находящегося в домашней сети мобильного узла такое сообщение позволяет домашнему агенту удалить существующие мобильные привязки для этого узла. В домашней сети мобильный узел работает без использования функций мобильности.

Есть ещё два случая, когда мобильному узлу **следует** (де)регистрироваться на домашнем агенте, - обнаружение мобильным узлом перезагрузки внешнего агента (как описано в параграфе 2.4.4) и истекающее время Lifetime для текущей регистрации.

При отсутствии на канальном уровне индикации смены точки подключения анонсам Agent Advertisement от новых агентов **не следует** инициировать на мобильном узле попытки новой регистрации, если срок действия текущей ещё не истёк и от внешнего агента текущей регистрации продолжают приходить анонсы Agent Advertisement. При отсутствии индикации канального уровня мобильному узлу **недопустимо** пытаться зарегистрироваться более 1 раза в секунду.

Мобильный узел **может** зарегистрироваться у другого агента, если протоколы транспортного уровня показывают слишком много повторов передачи. Мобильному узлу **недопустимо** трактовать получение ICMP Redirect от обеспечивающего текущее обслуживание внешнего агента, как основание для регистрации у другого агента. При выполнении указанных ограничений мобильный узел **может** снова зарегистрироваться в любой момент.

В Приложении D даны примеры заполнения полей регистрационных сообщений и типовые варианты регистрации.

3.6.1. Отправка регистрационных запросов

В последующих параграфах приведено подробное описание значений, которые мобильный узел **должен** представлять в полях сообщений Registration Request.

3.6.1.1. Поля IP

В этом параграфе описаны правила, в соответствии с которыми мобильные узлы заполняют поля заголовков IP для сообщений Registration Request.

IP Source

- при регистрации в чужой сети с совмещённым адресом обслуживания в поле IP source **должен** указываться этот адрес;

- в остальных случаях, если у мобильного узла нет домашнего адреса, поле IP source **должно** быть 0.0.0.0;
- при прочих обстоятельствах в поле IP source **должен** указываться домашний адрес мобильного узла.

IP Destination

- Когда мобильный узел нашёл агента, на котором зарегистрирован тем или иным способом, не сообщающим IP-адрес агента (например, на канальном уровне), **должен** указываться адрес получателя All Mobility Agents (224.0.0.11). В этом случае мобильный узел **должен** использовать индивидуальный адрес канального уровня для доставки дейтаграммы нужному агенту.
- Когда при регистрации у внешнего агента, **должен** указываться его адрес, взятый из поля IP source соответствующего анонса Agent Advertisement. Это **может** оказаться адресом, который не анонсируется в качестве адреса обслуживания в Agent Advertisement. Кроме того, при передаче этого сообщения Registration Request мобильный узел **должен** использовать адрес получателя на канальном уровне, взятый из соответствующего поля анонса Agent Advertisement, где был найден IP-адрес внешнего агента.
- Когда мобильный узел регистрируется напрямую у своего домашнего агента и знает его (индивидуальный) адрес IP, это адрес **должен** указываться в поле IP Destination.
- Если мобильный узел напрямую регистрируется у домашнего агента, но не знает его адреса IP, он может использовать динамическое преобразование для автоматического определения нужного адреса IP (параграф 3.6.1.2). В этом случае в поле IP Destination помещается широковещательный адрес (subnet-directed) домашней сети мобильного узла. Такой адрес **недопустимо** использовать в качестве адреса получателя, если мобильный узел регистрируется через внешний агент, хотя этот адрес **можно** указывать в теле сообщения Registration Request при такой регистрации.

IP TTL

- В поле IP TTL **должно** указываться значение 1, если в качестве адреса получателя используется All Mobility Agents, как указано выше. В остальных случаях задаётся. подходящее значение в соответствии с обычной практикой IP [38].

3.6.1.2. Поля регистрационного запроса

В этом параграфе представлены специфические правила, в соответствии с которыми мобильные узлы устанавливают значения полей в фиксированной части сообщений Registration Request.

Мобильный узел **может** установить бит S для того, чтобы запросить у домашнего агента поддержку предыдущих привязок мобильности. Без этого домашний агент будет удалять все прежние привязки, заменяя их новой привязкой, которая задана в Registration Request. Множество одновременных привязок полезно в тех случаях, когда мобильный узел, использующий хотя бы одну беспроводную сеть, перемещается в области покрытия обслуживаемой несколькими внешними агентами. IP явно разрешает дублирование дейтаграмм. Если домашний агент разрешает множественные привязки, он будет туннелировать копии каждой прибывающей дейтаграммы на все адреса обслуживания и мобильный узел будет получать множество таких копий.

Мобильному узлу **следует** устанавливать бит D при регистрации с совмещённым адресом обслуживания. В остальных случаях установка этого флага **недопустима**.

Мобильный узел **может** устанавливать бит B для запроса у своего домашнего агента пересылки копий всех широковещательных дейтаграмм, получаемых агентом из домашней сети. Метод, используемый домашним агентом для пересылки широковещательных дейтаграмм, зависит от типа адреса обслуживания, зарегистрированного мобильным узлом (как указано битом D в регистрационном запросе мобильного узла).

- Установленный бит D показывает, что мобильный узел будет самостоятельно декапсулировать все дейтаграммы, туннелированные на этот адрес обслуживания (совмещённый). В этом случае для пересылки мобильному узлу полученных широковещательных дейтаграмм домашний агент **должен** туннелировать их на адрес обслуживания. Мобильный узел детуннелирует такие дейтаграммы так же, как он делает это с дейтаграммами, адресованными непосредственно ему.
- Сброшенный бит D показывает, что мобильный узел использует для обслуживания адрес внешнего агента, который будет декапсулировать дейтаграммы до их пересылки мобильному узлу. В этом случае для пересылки полученных широковещательных дейтаграмм мобильному узлу домашний агент **должен** инкапсулировать их в unicast-дейтаграммы, направленные по домашнему адресу мобильного узла, а потом **должен** туннелировать их на адрес обслуживания мобильного узла.

  После декапсуляции внешним агентом внутренняя дейтаграмма будет обычной (unicast) дейтаграммой IP, адресованной мобильному узлу, что показывает внешнему агенту направление её пересылки. Доставка её мобильному узлу осуществляется так же, как доставляются тому обычные дейтаграммы. Мобильному узлу **недопустимо** декапсулировать вложенные широковещательные дейтаграммы и **недопустимо** для их пересылки мобильному узлу использовать локальное широковещание. Мобильный узел **должен** декапсулировать широковещательную дейтаграмму самостоятельно. Следовательно, для мобильного узла в таких случаях **недопустима** установка бита B в Registration Request, если он не способен декапсулировать дейтаграммы.

Мобильный узел **может** запрашивать дополнительные формы инкапсуляции, устанавливая бит M и/или G, но только в тех случаях, когда он самостоятельно декапсулирует дейтаграммы (использует совмещённый адрес обслуживания) или внешний агент указал поддержку этих форм инкапсуляции, установив соответствующие биты в расширении Mobility Agent Advertisement анонса Agent Advertisement, полученного мобильным узлом. В остальных случаях для мобильного узла установка этих битов **недопустима**.

Выбор значения поля Lifetime показан ниже:

- Если мобильный узел регистрируется с внешним агентом, значение поля Lifetime **не следует** делать больше значения поля Registration Lifetime в сообщении Agent Advertisement, полученном от внешнего агента. Когда метод определения адреса обслуживания не включает Lifetime, **может** использоваться принятое по умолчанию значение ICMP Router Advertisement Lifetime (1800 секунд).

- Мобильный узел **может** попросить домашнего агента удалить конкретную привязку мобильности, отправив тому сообщение Registration Request с адресом обслуживания этой привязки и Lifetime = 0 (параграф 3.8.2).

- Аналогично с помощью Lifetime = 0 мобильный узел может отменить регистрацию всех адресов обслуживания при возвращении в домашнюю сеть.

В поле Home Address **должен** указываться домашний адрес мобильного узла, если он известен, или 0 в противном случае.

В поле Home Agent **должен** указываться адрес домашнего агента мобильного узла, если этот адрес известен. В противном случае мобильный узел **может** использовать динамическое определение адреса домашнего агента. Для этого мобильный узел **должен** установить в поле Home Agent широковещательный адрес subnet-directed своей домашней сети. Каждый домашний агент, получив сообщение Registration Request с широковещательным адресом получателя, **должен** отвергнуть регистрацию мобильного узла, которому **следует** возвратить сообщение Registration Reply, показывающее индивидуальный адрес IP для использования при последующей попытке регистрации.

В поле Care-of Address **должен** указываться конкретный адрес обслуживания, который мобильный узел хочет (де)регистрировать. Если мобильный узел хочет отменить регистрацию всех своих адресом обслуживания, он **должен** указать в этом поле свой домашний адрес.

Мобильный узел выбирает значение поля Identification в зависимости от способа защиты от повторного использования пакетов, который применяется для его домашнего агента. Это является частью защищённой мобильной связи между мобильным узлом и его домашним агентом. Метод расчёта поля Identification описан в параграфе 5.7.

3.6.1.3. Расширения

В этом параграфе описан порядок всех обязательных и необязательных расширений, которые мобильный узел добавляет в конце сообщения Registration Request. Расширения должны указываться в приведённом ниже порядке.

a) После заголовка IP следует заголовок UDP, а за ним фиксированная часть Registration Request, после которой

b) могут присутствовать какие-либо, не связанные с аутентификацией расширения, которые могут использоваться домашним агентом (и могут оказаться полезны внешнему агенту), а за ними

c) разрешающее аутентификацию расширение, после которого

d) могут присутствовать любые, не относящиеся к аутентификации расширения, используемые только внешним агентом, а затем

e) может следовать расширение Mobile-Foreign Authentication.

Отметим, что элементы a) и c) **должны** присутствовать в каждом сообщении Registration Request от мобильного узла. Элементы b), d) и e) не обязательны. Однако элемент e) **должен** включаться в сообщения при использовании мобильным узлом и внешним агентом общей защищённой связи.

3.6.2. Получение регистрационных откликов

Сообщения Registration Reply мобильный узел получает в ответ на свои сообщения Registration Request. Отклики при регистрации обычно делятся на три категории:

- запрос был принят;

- запрос был отклонён внешним агентом;

- регистрация была отвергнута домашним агентом.

- В оставшейся части этого раздела рассматривается обработка мобильным узлом сообщений Registration Reply каждой из трёх категорий.

3.6.2.1. Проверка применимости

Отклики Registration Reply с ненулевой некорректной контрольной суммой UDP **должны** отбрасываться без уведомления.

Кроме того, 32 младших бита поля Identification в Registration Reply **должны** сравниваться с 32 младшими битами поля Identification в последнем сообщении Registration Request, отправленном отвечающему агенту. При несоответствии отклик **должен** отбрасываться без уведомления.

В дополнение к этому сообщения Registration Reply **должны** проверяться на предмет наличия разрешающего аутентификацию расширения. Для всех сообщений Registration Reply, содержащих Status Code с кодом статуса от домашнего агента, мобильный узел **должен** проверять наличие разрешающего аутентификацию расширения и действовать с соответствии со значением поля Code в отклике. Правила приведены ниже.

a) Если мобильный узел и внешний агент используют защищённую связь Mobility Security Association, в отклике Registration Reply **должно** присутствовать в точности одно расширение Mobile-Foreign Authentication и мобильный узел **должен** проверить значение Authenticator в этом расширении. Если расширения Mobile-Foreign Authentication не найдено, присутствует несколько таких расширений или значение Authenticator неприемлемо, мобильный узел **должен** отбросить отклик без уведомления (**следует** также сделать запись в системном журнале о нарушении безопасности).

b) Если поле Code указывает, что обслуживание было отвергнуто домашним агентом или регистрация была воспринята им, в сообщении Registration Reply **должно** присутствовать в точности одно расширение Mobile-

Home Authentication и мобильный узел **должен** проверить значение Authenticator в этом расширении. Если отклик был создан домашним агентом, но расширения Mobile-Home Authentication в нем не найдено, присутствует несколько таких расширений или значение Authenticator неприемлемо, мобильный узел **должен** отбросить отклик без уведомления (**следует** также сделать запись в системном журнале о нарушении безопасности).

Если значение Code говорит об отказе при аутентификации со стороны домашнего или внешнего агента, вполне возможно наличие ошибок в полях Authenticator сообщения Registration Reply. Это может произойти, например, при некорректной настройке совместно используемого мобильным узлом и домашним агентом секрета. Мобильному узлу **следует** занести в системный журнал запись о нарушении безопасности.

3.6.2.2. Регистрационный запрос принят

Если поле Code указывает, что запрос был воспринят, мобильному узлу **следует** настроить свою таблицу маршрутизации в соответствии с текущей точкой подключения (параграф 4.2.1).

Если мобильный узел возвращается в домашнюю сеть и в этой сети поддерживается ARP, мобильный узел **должен** следовать описанным в параграфе 4.6 процедурам в части ARP, proxy ARP, беспричинный ARP.

Если мобильный узел зарегистрирован в чужой сети, ему **следует** возобновлять регистрацию до того, как завершится срок действия (Lifetime) текущей регистрации. Как указано в параграфе 3.6, для каждого ожидающего сообщения Registration Request, мобильный узел **должен** поддерживать информацию об оставшемся сроке регистрации, а также исходное значение Lifetime из сообщения Registration Request. При получении мобильным узлом приемлемого сообщения Registration Reply, он **должен** уменьшить значение оставшегося срока регистрации в соответствии с указанным домашним агентом в отклике значением Lifetime. Это равносильно началу отсчёта таймера в момент отправки регистрационного запроса со значения Lifetime в отклике, хотя значение Lifetime из отклика домашнего агента заранее не известно. Поскольку регистрационный запрос передаётся несколько раньше того, как домашний агент начнёт отсчёт срока регистрации (указываемое в отклике значение Lifetime), эта процедура обеспечивает мобильному узлу возможность своевременно возобновить регистрацию с учётом возможных задержек при передаче регистрационного запроса и отклика на него.

3.6.2.3. Регистрационный запрос отвергнут

Если поле Code показывает, что запрос на обслуживание был отвергнут, мобильному узлу **следует** занести в системный журнал запись об ошибке. В некоторых случаях мобильный узел может решить проблему сам. К таким случаям относятся:

Code 69: (отвергнуто внешним агентом, запрошенное значение Lifetime слишком велико)

В этом случае поле Lifetime в сообщении Registration Reply будет показывать максимальное значение Lifetime, которое внешний агент согласен принимать в сообщениях Registration Request. Мобильный узел **может** повторить попытку регистрации у того же внешнего агента, установив для поля Lifetime в сообщении Registration Request значение, которое **должно** быть не больше указанного в отклике времени.

Code 133: (отвергнуто домашним агентом, несоответствие Identification)

В этом случае поле Identification в сообщении Registration Reply будет содержать значение, которое позволит мобильному узлу синхронизироваться с домашним агентом с учётом используемой модели защиты от повторного использования пакетов (параграф 5.7). Мобильный узел **должен** скорректировать параметры, используемые при расчёте поля Identification в соответствии с информацией из сообщения Registration Reply, прежде, чем вводить новые запросы на регистрацию.

Code 136: (отвергнуто домашним агентом, неизвестный адрес домашнего агента)

Этот код может возвращаться домашним агентом в тех случаях, когда мобильный узел определяет адрес домашнего агента динамически, как описано в параграфах 3.6.1.1 и 3.6.1.2. В таких случаях поле Home Agent в отклике будет содержать индивидуальный IP-адрес передающего отклик домашнего агента. Мобильный узел **может** повторить попытку регистрации, указав полученный адрес в последующем сообщении Registration Request. Кроме того, мобильному узлу **следует** до новой попытки регистрации настроить параметры, используемые для расчёта поля Identification с учётом значений соответствующих полей из полученного сообщения Registration Reply.

3.6.3. Повтор передачи при регистрации

При отсутствии отклика Registration Reply в течение достаточно продолжительного времени, **возможна** повторная передача сообщения Registration Request. При использовании временных меток для каждого повтора используется новое значение Identification и каждое сообщение, по сути, является новой регистрацией. При использовании маркеров nonce запросы передаются повторно без изменений и повтор не учитывается, как новая регистрация (параграф 5.7). За счёт этого повторная передача не будет требовать от домашнего агента повторной синхронизации с мобильным узлом за счёт использования другого маркера nonce, как происходит в случае потери исходного сообщения Registration Request (с меньшей вероятностью, Registration Reply) в сети.

Максимальное время до повтора передачи Registration Request **следует** делать не больше значения Lifetime, указанного в Registration Request. Минимальный интервал до повтора **следует** делать достаточно большим, принимая во внимание размер сообщений - подойдёт двойное время кругового обхода между мобильным узлом и домашним агентом, к которому добавлено по крайней мере 100 мсек на обработку сообщения перед откликом. Время кругового обхода для передачи домашнему агенту будет не меньше времени, требуемого для передачи сообщения через канал в текущей точке подключения мобильного узла. Некоторые устройства добавляют ещё 200 мсек задержки при передаче домашнему агенту с учётом возможности наличия на пути спутникового канала. Минимальное время между повторами сообщений Registration Request **недопустимо** делать меньше 1 секунды. Каждый последующий интервал до повтора **следует** увеличивать по крайней мере вдвое по сравнению с предыдущим, пока не будет достигнуто максимальное значение, рассмотренное выше.

3.7. Внешний агент

Роль внешнего агента в процессе регистрации Mobile IP в основном пассивна. Он транслирует регистрационные запросы между мобильными узлами и их домашними агентами и, в случае предоставления своего адреса для обслуживания мобильных клиентов, декапсулирует дейтаграммы для доставки мобильному узлу. Внешним агентам **следует** периодически отправлять сообщения Agent Advertisement для анонсирования своего присутствия, как описано в параграфе 2.3, если агент не может быть обнаружен средствами канального уровня.

Внешним агентам **недопустимо** передавать сообщения Registration Request, за исключением пересылки регистрационных запросов мобильных узлов к своим домашним агентам. Внешним агентам **недопустимо** передавать сообщения Registration Reply, за исключением пересылки регистрационных откликов домашних агентов или ответов на регистрационные запросы в случае отказа от обслуживания мобильного узла. В частности, внешним агентам **недопустимо** генерировать регистрационные запросы и/или отклик по истечении срока регистрации (Lifetime) мобильного узла. Внешним агентам **недопустимо** генерировать сообщения Registration Request для запроса отмены регистрации мобильных узлов, однако они **должны** транслировать корректные запросы мобильных узлов на регистрацию или её отмену.

3.7.1. Таблицы конфигурации и регистрации

В конфигурации каждого внешнего агента **должен** быть задан адрес обслуживания. Кроме того, для каждой ожидающей и действующей регистрации внешний агент **должен** поддерживать запись в списке посетителей, включающую сведения из сообщений Registration Request от мобильных узлов:

- адрес мобильного узла на канальном уровне;
- домашний IP-адрес мобильного узла или его совмещённый адрес обслуживания (см. описание бита R в параграфе 2.1.1);
- IP-адрес получателя (см. параграф 3.6.1.1);
- UDP-порт источника;
- адрес домашнего агента;
- значение поля Identification;
- запрошенное значение Lifetime;
- остающееся время ожидающей или действующей регистрации.

Если в регистрационном указано нулевое значение Home Address, внешний агент **должен** следовать процедурам, описанным в RFC 2794 [6]. В частности, если внешний агент не может управлять записями для ожидающих сообщений Registration Request с нулевым значением Home Address, этот агент **должен** возвращать мобильному узлу сообщение Registration Reply с кодом NONZERO_HOMEADDR_REQD (см. [6]).

Конфигурация внешнего агента **может** ограничивать число ожидающих регистраций, которые она готова поддерживать (обычно 5). В этом случае внешнему агенту **следует** отвергать дополнительные попытки регистрации с кодом 66. Внешний агент **может** удалить любой регистрационный запрос, ожидающий более 7 секунд; в этом случае внешнему агенту **следует** отвергнуть запрос с кодом 78 (тайм-аут при регистрации).

Как любой узел в сети Internet, внешний агент может организовывать защищённые связи Mobility Security Association с другими узлами. При трансляции сообщений Registration Request от мобильного узла его домашнему агенту, если у внешнего агента имеется Mobility Security Association с этим домашним агентом, он **должен** добавлять в запрос расширение Foreign-Home Authentication. В таких случаях, когда сообщение Registration Reply включает отличное от 0 значение Lifetime, внешний агент **должен** проверить наличие требуемого расширения Foreign-Home Authentication в сообщении Registration Reply от домашнего агента (параграфы 3.3 и 3.4). Аналогично, при получении Registration Request от мобильного узла и наличии Mobility Security Association с этим узлом внешний агент **должен** проверить наличие требуемого расширения Mobile-Foreign Authentication в запросе и **должен** добавлять в отклики для этого узла расширение Mobile-Foreign Authentication.

3.7.2. Получение регистрационных запросов

Если внешний агент воспринимает сообщение Registration Request от мобильного узла, он убеждается в том, что указанный там домашний агент не подключён к какому-либо из сетевых интерфейсов внешнего агента. Если такого подключения не обнаружено, внешний агент **должен** транслировать запрос указанному домашнему агенту. В противном случае, если внешний агент отвергает запрос, он **должен** передать мобильному узлу сообщение Registration Reply с подходящим кодом отказа, но частота передачи таких сообщений не должна превышать 1 сообщения в секунду для данного мобильного узла. Этот вопрос более подробно рассматривается в последующих параграфах.

Если на одном из интерфейсов внешнего агента установлен адрес IP, который указан мобильным узлом в качестве адреса домашнего агента, внешнему агенту **недопустимо** пересылать такой запрос. Если внешний агент обслуживает мобильный узел в качестве домашнего агента, он должен следовать процедурам, описанным в параграфе 3.8.2. В противном случае (если внешний агент не обслуживает мобильный узел в качестве домашнего агента) внешний агент отвергает запрос с возвратом кода ошибки 136 (неизвестный адрес домашнего агента).

Если внешний агент получает сообщение Registration Request от мобильного узла из своего списка посетителей, существующую в этом списке запись **не следует** удалять или изменять, пока внешний агент не получит от домашнего агента сообщение Registration Reply с кодом успешной регистрации. Внешний агент **должен** записать новый ожидающий запрос в отдельную запись списка посетителей. Если сообщение запрашивает отмену регистрации, имеющуюся в списке посетителей запись для мобильного узла **не следует** удалять до получения Registration Reply с кодом успешного выполнения. Если сообщение Registration Reply говорит об отвергнутом запросе (регистрации или дерегистрации), имеющуюся в списке запись **недопустимо** изменять в результате получения такого Registration Reply.

3.7.2.1. Проверка применимости

Сообщения Registration Request с некорректной, отличной от нуля контрольной суммой UDP **должны** отбрасываться без уведомления. Запросы с отличными от 0 резервными полями **должны** отвергаться с кодом 70 (некорректный формат запроса). Запросы со сброшенным флагом D и отличным от нуля полем Lifetime, указывающие адрес обслуживания, не являющийся адресом внешнего агента, **должны** отвергаться с кодом 77 (недопустимый адрес обслуживания).

В сообщениях Registration Request **должна** проверяться аутентификация. Если между мобильным узлом и внешним агентом имеется защищённая связь Mobility Security Association, в запросе **должно** присутствовать в точности одно расширение Mobile-Foreign Authentication и внешний агент **должен** проверять значение Authenticator в таком расширении. Если расширение не найдено, обнаружено несколько расширений или значение Authenticator не приемлемо, внешний агент **должен** отбросить запрос без уведомления. **Следует** также записать информацию о таком запросе в системный журнал. Внешнему агенту **следует** также передать мобильному узлу сообщение Registration Reply с кодом 67.

3.7.2.2. Пересылка применимых запросов домашнему агенту

Если внешний агент принимает регистрационный запрос мобильного узла, он должен транслировать этот запрос домашнему агенту данного узла, указанному в поле Home Agent сообщения Registration Request. Внешнему агенту **недопустимо** менять какие-либо поля, начиная с фиксированной части сообщения Registration Request и заканчивая Mobile-Home Authentication Extension (включая его) или другим аутентификационным расширением, представленным мобильным узлом в качестве разрешающего аутентификацию расширения для домашнего агента. В противном случае с высокой вероятностью аутентификация на домашнем агенте завершится отказом. Кроме того, внешний агент выполняет следующие операции:

- **должен** обработать и удалить любые расширения, кроме предшествующих расширению, разрешающему проверку полномочий;
- **может** добавить любое из своих не относящихся к аутентификации расширений для домашнего агента;
- **должен** добавить в конце расширение Foreign-Home Authentication, если имеется защищённая связь с домашним агентом.

Поля заголовков IP и UDP в транслируемых сообщениях Registration Request **должны** устанавливаться в соответствии с приведёнными ниже правилами.

IP Source Address
Адрес внешнего агента на интерфейсе, через который будет передано сообщение.

IP Destination Address
Копируется из поля Home Agent в сообщении Registration Request.

UDP Source Port
<переменный>

UDP Destination Port
434

После пересылки корректного сообщения Registration Request домашнему агенту внешний агент **должен** начать отсчёт оставшегося времени для ожидающей регистрации со значения поля Lifetime в Registration Request. Если отсчёт таймера завершится до получения приемлемого сообщения Registration Reply, внешний агент **должен** удалить запись для ожидающей регистрации из своего списка посетителей.

3.7.2.3. Отказы для недопустимых запросов

Если внешний агент по какой-либо причине отвергает регистрационный запрос мобильного узла, ему **следует** возвратить сообщение Registration Reply с подходящим кодом отказа. В таких случаях поля Home Address, Home Agent, и Identification копируются в сообщение Registration Reply из соответствующих полей Registration Request.

Если значение поля Reserved отлично от 0, внешний агент **должен** отвергнуть запрос и мобильному узлу **следует** отправить сообщение Registration Reply с кодом 70. Если запрос отвергается по причине слишком большого значения Lifetime в запросе, внешний агент устанавливает в поле Lifetime возвращаемого отклика максимальное значение срока регистрации, которое может быть принято для регистрационного запроса и помещает в поле Code значение 69. В остальных случаях значение Lifetime **следует** копировать из одноимённого поля в запросе.

Ниже показаны значения, которые **должны** помещаться в поля заголовков IP и UDP для сообщений Registration Reply.

IP Source Address
Копируется из поля IP Destination Address сообщения Registration Request, если там не был указан адрес All Agents Multicast. В последнем случае **должен** использоваться адрес интерфейса внешнего агента, через который сообщение передаётся.

IP Destination Address
Если сообщение Registration Reply генерируется внешним агентом для отказа от регистрации мобильного узла и в поле Home Address регистрационного запроса указано значение, отличное от 0.0.0.0, значение поля IP Destination Address копируется из поля Home Address в сообщении Registration Request. В противном случае, если сообщение Registration Reply получено от домашнего агента и содержит отличное от 0.0.0.0 поле Home Address, значение IP Destination Address копируется из поля Home Address сообщения Registration Reply. В остальных случаях для поля IP Destination Address в Registration Reply устанавливается значение 255.255.255.255.

UDP Source Port
434

UDP Destination Port
Копируется из поля UDP Source Port регистрационного запроса.

3.7.3. Получение регистрационных откликов

Внешний агент обновляет свой список посетителей при получении приемлемого сообщения Registration Reply от домашнего агента. Полученное сообщение транслируется мобильному узлу. Более подробное описание этого приведено в последующих параграфах.

Если при трансляции сообщения Registration Request домашнему агенту внешний агент получает сообщение ICMP об ошибке вместо Registration Reply, тогда этому агенту **следует** отправить мобильному узлу сообщение Registration Reply с подходящим кодом отказа (домашний агент недоступен) из диапазона кодов 80-95. Создание сообщений Registration Reply описано в параграфе 3.7.2.3.

3.7.3.1. Проверка применимости

Сообщения Registration Reply с некорректно, отличной от 0 контрольной суммой UDP **должны** отбрасываться без уведомления.

При получении внешним агентом сообщения Registration Reply он **должен** просмотреть свой список посетителей на предмет ожидающих сообщений Registration Request с тем же домашним адресом мобильного узла, какой указан в полученном отклике. Если для этого адреса найдено множество записей и в сообщении Registration Reply имеется расширение Mobile Node NAI [2], внешний агент **должен** использовать NAI для устранения неоднозначности с ожидающими регистрационными запросами. Если соответствующего запроса в списке не найдено и сообщение Registration Reply не соответствует ни одному из ожидающих регистрационных запросов с нулевым домашним адресом мобильного узла (см. параграф 3.7.1), внешний агент **должен** отбросить отклик без уведомления. Отклики также **должны** отбрасываться без уведомления, если младшие 32 бита поля Identification не соответствуют таким же битам в запросе.

Должна также проверяться аутентификация в Registration Reply. Если между внешним и домашним агентом имеется защищённая связь Mobility Security Association, в сообщении **должно** присутствовать в точности одно расширение Foreign-Home Authentication и внешний агент **должен** проверять значение Authenticator в нем. Если расширения Foreign-Home Authentication не найдено, обнаружено несколько таких расширений или значение Authenticator неприемлемо, внешний агент **должен** отбросить отклик без уведомления и ему также **следует** сделать запись о нарушении безопасности в системный журнал. Внешний агент в этом случае **должен** также отвергать регистрацию мобильного узла, которому **следует** отправить сообщение Registration Reply с кодом 68.

3.7.3.2. Пересылка откликов мобильному узлу

Сообщения Registration Reply, прошедшие проверки из параграфа 3.8.2.1, транслируются мобильному узлу. Внешний агент в этом случае **должен** обновить свой список посетителей с учётом результата регистрационного запроса, указанного полем Code в отклике. Если код показывает восприятие запроса домашним агентом и значение поля Lifetime отлично от 0, внешнему агенту **следует** установить в поле Lifetime своего списка посетителей меньшее из:

- значение поля Lifetime в сообщении Registration Reply;
- максимально допускаемое внешним агентом значение Lifetime.

Если вместо этого отклик содержит значение Code, показывающее, что Lifetime = 0, внешний агент **должен** удалить запись для мобильного узла из своего списка посетителей. Если же код в отклике указывает на отказ домашнего агента от регистрации мобильного узла, внешний агент **должен** удалить из своего списка ожидающую регистрацию, сохранив запись для мобильного узла в списке посетителей.

Внешнему агенту **недопустимо** менять какие-либо поля, начиная с фиксированной части Registration Reply и заканчивая расширением Mobile-Home Authentication (включительно). В противном случае на стороне мобильного узла с высокой вероятностью возникнет отказ аутентификации.

В дополнение к этому внешнему агенту **следует** выполнять перечисленные ниже процедуры:

- он **должен** обработать и удалить все расширения, не относящиеся к аутентификационным;
- он **может** добавить в конец свои, не относящиеся к аутентификации расширения, передающие информацию мобильному узлу;
- он **должен** добавить в коней расширение Mobile-Foreign Authentication, если имеется защищённая связь Mobility Security Association с мобильным узлом.

Поля заголовков IP и UDP в транслируемых сообщениях Registration Reply устанавливаются в соответствии с правилами, приведёнными в параграфе 3.7.2.3.

После пересылки приемлемого сообщения Registration Reply мобильному узлу внешний агент **должен** обновить для этой регистрации запись в списке посетителей. Если сообщение Registration Reply указывает восприятие регистрации домашним агентом, внешний агент устанавливает для таймера срока регистрации значение поля Lifetime из сообщения Registration Reply. В отличии от мобильного узла, отсчитывающего срок регистрации в соответствии с параграфом 3.6.2.2, внешний агент начинает свой отсчёт с момента пересылки сообщения Registration Reply - это гарантирует, что отсчёт срока регистрации на внешнем агенте не завершится раньше, нежели на мобильном узле. Если же сообщение Registration Reply показывает, что регистрация была отвергнута домашним агентом, внешний агент удаляет из списка посетителей запись для этой попытки регистрации.

3.8. Домашний агент

Домашний агент в процессе регистрации играет реактивную роль. Он получает сообщения Registration Request от мобильного узла (возможно, транслируемые внешним агентом), обновляет свою запись привязки мобильности и возвращает подходящее сообщение Registration Reply в ответ на каждый запрос.

Домашнему агенту **недопустимо** передавать сообщения Registration Reply за исключением случаев ответа на сообщения Registration Request от мобильного узла. В частности, домашнему агенту **недопустимо** генерировать сообщения Registration Reply для индикации завершения срока регистрации (Lifetime).

3.8.1. Таблицы конфигурации и регистрации

На каждом домашнем агенте **должен** быть задан адрес IP и размер префикса для домашней сети. На домашнем агенте **должна** быть настроена защищённая связь Mobility Security Association с каждым уполномоченным мобильным узлом, который он обслуживает.

Когда домашний агент воспринимает корректное сообщение Registration Request от мобильного узла, который он обслуживает, этот агент **должен** создать или изменить для этого узла привязку мобильности, содержащую:

- домашний адрес мобильного узла;
- адрес обслуживания мобильного узла;
- поле Identification из сообщения Registration Reply;
- остающийся срок регистрации (Lifetime).

Домашний агент **может** предлагать динамическое выделение домашнего адреса мобильному узлу при получении от того сообщения Registration Request. Методы выделения динамических адресов выходят за рамки данного документа и рассмотрены в работе [6]. После того, как домашний агент свяжет с мобильным узлом домашний адрес, агент **должен** поместить этот адрес в поле Home Address сообщения Registration Reply.

Домашний агент **может** также поддерживать защищённые связи с разными внешними агентами. При получении сообщения Registration Request от внешнего агента, с которым имеется защищённая связь, домашний агент **должен** проверить значение Authenticator в обязательном расширении Foreign-Home Authentication данного сообщения, основываясь на своей защищённой связи. Аналогично, при передаче сообщения Registration Reply внешнему агенту, с которым домашний агент имеет защищённую связь, домашний агент **должен** включить в сообщение расширение Foreign-Home Authentication на основе этой защищённой связи.

3.8.2. Получение регистрационных запросов

Если домашний агент воспринимает входящее сообщение Registration Request, он **должен** обновить свою запись для привязки мобильности данного узла. В ответ **следует** отправить сообщение Registration Reply с подходящим кодом. В противном случае (домашний агент отвергает запрос) **следует** в большинстве случаев отправить сообщение Registration Reply с кодом, указывающим причину отказа в регистрации. Эта ситуация рассматривается более подробно в последующих параграфах. Если домашний агент не поддерживает широковещания (см. параграф 4.3), он **должен** игнорировать флаг B (не отвергая Registration Request).

3.8.2.1. Проверка применимости

Сообщения Registration Request с отличной от 0 и некорректной контрольной суммой UDP **должны** отбрасываться домашним агентом без уведомления отправителя.

Должна выполняться аутентификация сообщений Registration Request, включающая перечисленные ниже операции.

a) Домашний агент **должен** проверить наличие разрешающего аутентификацию расширения и провести указанную им аутентификацию. В сообщении Registration Request **должно** присутствовать в точности одно расширение, разрешающее аутентификацию, и домашний агент **должен** проверить значение Authenticator в этом расширении или убедиться, что оно проверено другим агентом, с которым у него имеется защищённая связь. Если разрешающего аутентификацию расширения нет или значение Authenticator не приемлемо, домашний агент **должен** отвергнуть регистрацию мобильного узла. **Следует** также отправить этому узлу сообщение Registration Reply с кодом 131. После этого домашний агент **должен** отбросить сообщение с запросом, о чем **следует** сделать запись в системном журнале.

b) Домашний агент **должен** проверять корректность поля Identification с использованием контекста, выбранного SPI в разрешающем аутентификацию расширении. Описание такой проверки приведено в параграфе 5.7. При некорректном значении поля домашний агент **должен** отвергнуть регистрационный запрос, а мобильному узлу **следует** отправить сообщение Registration Reply с кодом 133, включающее поле Identification, рассчитанное в соответствии с правилами параграфа 5.7. Домашний агент **должен** прекратить обработку регистрационного запроса, хотя **следует** сделать запись об ошибке в системный журнал.

c) Если у домашнего агента организована защищённая связь с внешним агентом, домашний агент **должен** проверить наличие подходящего расширения Foreign-Home Authentication. В этом случае в сообщении Registration Request **должно** присутствовать в точности одно расширение Foreign-Home Authentication и домашний агент **должен** проверить значение Authenticator в этом расширении. Если расширение Foreign-Home Authentication не найдено, указано несколько таких расширений или значение Authenticator не приемлемо, домашний агент **должен** отвергнуть регистрацию мобильного узла, которому **следует** вернуть сообщение Registration Reply с кодом 132. Домашний агент **должен** отбросить запрос, а в системный журнал **следует** внести запись о нарушении безопасности.

В дополнение к выполнению аутентификации для сообщений Registration Request домашний агент **должен** отвергать регистрационные запросы, которые отправлены по широковещательному адресу subnet-directed домашней сети (вместо индивидуального адреса домашнего агента). Домашний агент **должен** отбросить запрос, а мобильному узлу **следует** отправить сообщение Registration Reply с кодом 136. В этом случае Registration Reply будет содержать индивидуальный адрес домашнего агента, по которому мобильный узел может передать новое сообщение Registration Request.

Отметим, что некоторые маршрутизаторы меняют поле IP Destination Address в дейтаграммах с широковещательным адресом subnet-directed на 255.255.255.255 до их передачи в сеть адресата. В таких случаях домашний агент, который пытается «подобрать» запросы динамического обнаружения домашнего агента путём явной привязки к широковещательному адресу subnet-directed, не увидит таких пакетов. Разработчикам домашних агентов следует быть готовыми к приёму пакетов, направленных по широковещательным адресам subnet-directed и 255.255.255.255, если они хотят поддерживать динамическое обнаружение домашнего агента.

3.8.2.2. Восприятие приемлемого запроса

Если сообщение Registration Request успешно прошло проверки, описанные в параграфе 3.8.2.1, и домашний агент может воспринять запрос на регистрацию, этот агент **должен** обновить свой список мобильных привязок для данного мобильного узла и **должен** вернуть этому узлу сообщение Registration Reply.

В этом случае сообщение Registration Reply будет включать код 0, если домашний агент поддерживает одновременные мобильные привязки, или 1, если такие привязки не поддерживаются. Описание построения регистрационных откликов дано в параграфе 3.8.3.

Домашний агент обновляет свою запись мобильной привязки для данного узла на основе полей сообщения Registration Request:

- Если Lifetime = 0 и Care-of Address совпадает с домашним адресом мобильного узла, домашний агент удаляет для этого узла все записи из своего списка мобильных привязок, как будто мобильный узел попросил у домашнего агента прекратить обслуживание мобильности для него.
- Если Lifetime = 0, а Care-of Address отличается от домашнего адреса мобильного узла, домашний агент удаляет из списка привязок мобильности только запись, содержащую указанный Care-of Address для данного мобильного узла. Все прочие активные записи для других адресов обслуживания останутся активными.
- Если значение Lifetime отлично от 0, домашний агент добавляет в свой список мобильных привязок для данного мобильного узла значение Care-of Address из запроса. Если установлен бит S и домашний агент поддерживает одновременные мобильные привязки, имеющиеся в списке записи для этого узла сохраняются. В остальных случаях домашний агент удаляет из списка все имеющиеся для данного мобильного узла записи.

Во всех случаях домашний агент **должен** отправить сообщение Registration Reply источнику сообщения Registration Request, который на деле может быть не тем внешним агентом для чьего адреса обслуживания запрошена (де)регистрация. Если у домашнего агента есть защищённая связь с внешним агентом, для адреса которого запрошена отмена регистрации и этот агент отличается от того, который транслировал сообщение Registration Request, домашний агент **может** дополнительно передать сообщение Registration Reply внешнему агенту, чей адрес обслуживания дерегистрируется. Домашнему агенту **недопустимо** передавать такой отклик, если у него нет защищённой связи с внешним агентом. Если отклик не передаётся, срок действия записи в списке посетителей внешнего агента завершается естественным путём по истечении времени Lifetime.

Домашнему агенту **недопустимо** увеличивать значение Lifetime сверх указанного мобильным узлом в сообщении Registration Request. Однако запрос мобильным узлом значения Lifetime, превышающего то, которое позволяет домашний агент, не является ошибкой. В таком случае домашний агент просто уменьшает Lifetime до приемлемого значения и возвращает его в отклике Registration Reply. Значение Lifetime в сообщении Registration Reply информирует мобильный узел об установленном сроке регистрации, показывая тому, когда **следует** повторно зарегистрироваться для продолжения обслуживания. По истечении срока регистрации домашний агент **должен** удалить свою запись для данной регистрации из списка привязок мобильности.

Если сообщение Registration Request дублирует воспринятый текущий регистрационный запрос, **недопустимо** выделять срок регистрации, превышающий выданное ранее значение Lifetime. Сообщение Registration Request считается дубликатом при совпадении домашнего адреса, адреса обслуживания и поля Identification с такими же полями имеющейся регистрации.

Кроме того, если в домашней сети поддерживается ARP [36] и сообщение Registration Request просит у домашнего агента создать мобильную привязку для узла, который ранее такой привязки не имел (узел предполагался домашним), домашний агент должен следовать процедурам, описанным в параграфе 4.6, в части ARP, proxy ARP и беспричинный ARP. Если для мобильного узла есть предшествующая привязка, домашний агент должен по прежнему следовать правилам для proxy ARP из параграфа 4.6.

3.8.2.3. Отказ при недопустимом запросе

Если регистрационный запрос не проходит всех проверок, указанных в параграфе 3.8.2.1, или домашний агент не способен его воспринять, домашнему агенту **следует** направить мобильному узлу сообщение Registration Reply с кодом причины отказа. Если запрос транслировался внешним агентом, такое сообщение позволяет этому агенту удалить запись из списка ожидающих посетителей. Кроме того, информация о причине отказа может помочь мобильному узлу в его попытках исправить ошибку перед отправкой следующего запроса на регистрацию.

В этом разделе описано множество причин, по которым домашний агент может отвергнуть регистрационный запрос, и приведены коды, которые следует использовать в каждом случае. Построение откликов Registration Reply подробно описано в разделе 3.8.3.

Многие из причин отказа при регистрации являются по своей природе административными. Например, домашний агент может ограничивать для мобильного узла число одновременных регистраций, отвергая выходящие за этот предел попытки с возвратом кода 135. Домашний агент может также отвергать запросы на регистрацию для мобильных узлов, подключённым к недоверенным областям обслуживания (сетям), возвращая отклик с кодом 129.

Запросы с отличными от 0 битами резервных полей **должны** отвергаться с возвратом кода 134 (неверный формат).

3.8.3. Передача регистрационных откликов

Если домашний агент воспринимает сообщение Registration Request, он **должен** обновить свою запись привязок для мобильного узла и ему также **следует** отправить отклик Registration Reply с соответствующим значением Code. В противном случае (домашний агент отвергает запрос) **следует** отправить сообщение Registration Reply с полем Code, указывающим причину отказа. В последующих параграфах приведены описания значений, которые домашний агент **должен** устанавливать в полях сообщений Registration Reply.

3.8.3.1. Поля IP/UDP

В этом параграфе приведены правила, в соответствии с которыми домашний агент устанавливает значения полей заголовков IP и UDP в сообщениях Registration Reply.

IP Source Address

Копируется из поля IP Destination Address сообщения Registration Request, если там не указан групповой или широковещательный адрес. При групповом или широковещательном адресе в заголовке Registration Request в поле IP Source Address **должен** указываться (индивидуальный) IP-адрес домашнего агента.

IP Destination Address

Копируется из поля IP Source Address в сообщении Registration Request.

UDP Source Port

Копируется из поля UDP Destination Port в сообщении Registration Request.

UDP Destination Port

Копируется из поля UDP Source Port в сообщении Registration Request.

При передаче Registration Reply в ответ на Registration Request с запросом дерегистрации мобильного узла (Lifetime = 0 и Care-of Address совпадает с домашним адресом мобильного узла), в котором поле IP Source Address содержит домашний адрес мобильного узла (это обычный метод дерегистрации при возвращении в домашнюю сеть), в поле IP Destination Address передаваемого отклика указывается домашний адрес мобильного узла путём копирования поля IP Source Address из запроса.

В этом случае при передаче Registration Reply домашний агент **должен** передать отклик непосредственно в домашнюю сеть, обходя список мобильных привязок. В частности для возвращающегося в домашнюю сеть мобильного узла если его новое сообщение Registration Request не воспринято домашним агентом, имеющаяся в списке мобильных привязок запись для этого узла будет указывать на зарегистрированный ранее адрес обслуживания. При передаче сообщения Registration Reply, указывающего на отказ при обработке данного запроса, эта привязка **должна** игнорироваться и домашний агент **должен** передать этот отклик как для мобильного узла, находящегося в домашней сети.

3.8.3.2. Поля регистрационного отклика

В этом параграфе описаны конкретные правила, в соответствии с которыми домашний агент устанавливает значения полей в фиксированной части сообщений Registration Reply.

Значение поля Code в сообщении Registration Reply выбирается в соответствии с правилами, описанными в предыдущих параграфах. При ответах на воспринятую регистрацию домашнему агенту **следует** возвращать код 1, если он не поддерживает одновременных регистраций.

Значение поля Lifetime **должно** копироваться из соответствующего поля сообщения Registration Request, если запрошенное значение не превышает максимальное время регистрации, на которое согласен домашний агент. Если запрошенное время регистрации превышает максимум, в поле Lifetime **должно** указываться реальное время, в течение которого домашний агент согласен выполнять обслуживание. В этом случае в поле Lifetime **следует** указывать максимальное время регистрации, допускаемое домашним агентом (для данного мобильного узла и адреса обслуживания).

Если поле Home Address в сообщении Registration Request отлично от 0, оно **должно** копироваться в поле Home Address сообщения Registration Reply. В противном случае, если поле Home Address в Registration Request равно 0, как указано в параграфе 3.6, домашнему агенту **следует** определиться с выделением домашнего адреса для мобильного узла и поместить выбранный адрес в поле Home Address сообщения Registration Reply. Ситуации, когда мобильный узел представляется значением NAI вместо домашнего адреса IP, описаны в документе [6].

Если поле Home Agent в Registration Request содержит индивидуальный адрес домашнего агента, значение этого поля **должно** копироваться в поле Home Agent сообщения Registration Reply. В противном случае домашний агент **должен** установить в поле Home Agent сообщения Registration Reply свой индивидуальный адрес. В этом последнем случае домашний агент **должен** отвергнуть регистрацию с возвратом подходящего кода (например, 136) для предотвращения одновременной регистрации мобильного узла на нескольких домашних агентах.

3.8.3.3. Расширения

В этом параграфе описан порядок всех обязательных и необязательных расширений, которые мобильный узел добавляет в конце сообщения Registration Reply. Расширения должны указываться в приведённом ниже порядке.

f) После заголовка IP следует заголовок UDP, а за ним фиксированная часть Registration Reply, после которой

g) могут присутствовать какие-либо, не связанные с аутентификацией расширения, которые могут использоваться домашним агентом (и могут оказаться полезны внешнему агенту), а за ними

h) расширение Mobile-Home Authentication, после которого

i) могут присутствовать любые, не относящиеся к аутентификации расширения, используемые только внешним агентом, а затем

j) может следовать расширение Foreign-Home Authentication.

Отметим, что элементы a) и c) **должны** присутствовать в каждом сообщении Registration Reply от домашнего агента. Элементы b), d) и e) не обязательны. Однако элемент e) **должен** включаться в сообщения при использовании мобильным узлом и внешним агентом общей защищённой связи.

4. Вопросы маршрутизации

В этом разделе описано взаимодействие мобильных узлов, домашних и (необязательно) внешних агентов в части маршрутизации дейтаграмм мобильного узла, подключённого к чужой сети. Мобильный узел информирует домашнего агента о своём текущем подключении, используя процедуру регистрации, описанную в разделе 3. В параграфе 1.7 приведён обзор протокола для разных вариантов расположения (адресации) мобильного узла относительно домашнего и внешнего агентов.

4.1. Типы инкапсуляции

Домашние и внешние агенты **должны** поддерживать туннелирование дейтаграмм с использованием инкапсуляции IP-in-IP [32]. Все мобильные узлы, использующие совмещённые адреса обслуживания, **должны** поддерживать приём

дейтаграмм, туннелированных с использованием такой инкапсуляции IP-in-IP. Минимальная инкапсуляция [34] и GRE [16] также **могут** поддерживаться агентами мобильности и мобильными узлами в качестве опции. Использование этих дополнительных форм инкапсуляции по запросам мобильных узлов осуществляется по усмотрению домашнего агента.

4.2. Маршрутизация индивидуальных дейтаграмм

4.2.1. Мобильный узел

При подключении к домашней сети мобильный узел не использует услуг поддержки мобильности. Т. е., он работает так же, как все прочие (стационарные) хосты и маршрутизаторы. Метод выбора используемого по умолчанию маршрутизатора в домашней сети или при подключении к чужой сети и использовании совмещённого адреса обслуживания выходит за рамки данного документа. Одним из таких методов является ICMP Router Advertisement [10].

При регистрации в чужой сети мобильный узел для выбора маршрутизатора по умолчанию использует правила, перечисленные ниже.

- Если мобильный узел регистрируется с использованием адреса внешнего агента, он **может** применять этот адрес в качестве адреса первого маршрутизатора. MAC-адрес внешнего агента можно узнать из сообщения Agent Advertisement. В остальных случаях мобильный узел **должен** выбрать используемый по умолчанию маршрутизатор из числа Router Address, анонсируемых в разделе ICMP Router Advertisement сообщений Agent Advertisement.
- Если мобильный узел регистрируется у домашнего агента, используя совмещённый адрес обслуживания, ему **следует** выбрать используемый по умолчанию маршрутизатор из числа анонсируемых в принятых им сообщениях ICMP Router Advertisement тот адрес, который будет соответствовать полученному извне адресу обслуживания и Router Address по префиксам. Если полученный мобильный узлом извне адрес обслуживания соответствует по префиксу адресу отправителя Agent Advertisement, мобильный узел **может** рассмотреть этот адрес при выборе маршрутизатора по умолчанию. Префикс сети **может** быть получен из Prefix-Lengths Extension в сообщении Router Advertisement (если оно используется). Префикс **можно** также получить с использованием иных механизмов, не рассматриваемых в данном документе.

При выходе из домашней сети мобильному узлу **недопустимо** передавать широковещательные пакеты ARP для определения MAC-адреса другого узла Internet. Таким образом, список (возможно пустой) Router Address из раздела ICMP Router Advertisement не принесёт пользы при выборе маршрутизатора по умолчанию, если у мобильного узла нет возможности какого-либо метода, не включающего широковещания ARP, и не указывается в данном документе, как средство получения MAC-адреса одного из маршрутизаторов в списке. Аналогично, при отсутствии не заданных механизмов получения MAC-адресов чужой сети, мобильный узел **должен** игнорировать перенаправления на другие маршрутизаторы чужих сетей.

4.2.2. Внешний агент

При получении инкапсулированной дейтаграммы, отправленной на анонсируемый внешним агентом адрес обслуживания он **должен** сравнить внутренний адрес получателя со своим списком посетителей. Если внутренний адрес не соответствует ни одному из адресов в списке посетителей, внешнему агенту **недопустимо** пересылать дейтаграмму без изменения исходного заголовка IP, поскольку в противном случае может возникнуть маршрутная петля. Такую дейтаграмму **следует** отбросить без уведомления. Внешнему агенту **недопустимо** передавать сообщения ICMP Destination Unreachable, когда он не способен переслать входящую туннелированную дейтаграмму. В остальных случаях внешний агент пересылает декапсулированную дейтаграмму мобильному узлу.

Внешнему агенту **недопустимо** анонсировать другим маршрутизаторам в своём домене или другим мобильным узлам присутствие в его списке посетителей мобильного маршрутизатора (параграф 4.5) или мобильного узла.

Внешний агент **должен** маршрутизировать дейтаграммы, полученные от зарегистрированных мобильных узлов. Как минимум, мобильный агент должен проверять контрольную сумму заголовка IP, уменьшать значение IP TTL, заново рассчитывать контрольную сумму заголовка IP и пересылать дейтаграммы используемому по умолчанию маршрутизатору.

Внешнему агенту **недопустимо** использовать широковещание ARP для определения MAC-адреса мобильного узла. Он может получить MAC-адрес, копируя данные из сообщений Agent Solicitation или Registration Request, передаваемых мобильным узлом. Для записей в кэше ARP с IP-адресами мобильных узлов **недопустимо** устанавливать время жизни меньше срока регистрации соответствующего узла в списке посетителей, если у внешнего агента нет способа обновления MAC-адреса, связанного с IP-адресом мобильного узла, без применения широковещания ARP.

Каждому внешнему агенту **следует** поддерживать функции, обязательные для реверсного туннелирования [27].

4.2.3. Домашний агент

Домашний агент **должен** быть способен перехватывать в домашней сети любые дейтаграммы, адресованные находящемуся за пределами домашней сети мобильному узлу. Для организации такого перехвата **можно** использовать proxy ARP и беспричинный ARP, как описано в параграфе 4.6.

Домашний агент должен проверять IP-адрес получателя во всех прибывающих дейтаграммах на предмет его соответствия какому-либо из мобильных узлов, находящихся за пределами домашней сети. При обнаружении пакета с таким адресом домашний агент туннелирует дейтаграммы на текущий адрес (адреса) обслуживания мобильного агента. Если домашний агент поддерживает множество одновременных привязок для мобильного узла, он туннелирует копии дейтаграммы по все адресам обслуживания мобильного узла из своего списка привязок. Если мобильный узел в данный момент не имеет привязки, домашнему агенту **недопустимо** пытаться перехватывать адресованные этому мобильному узлу дейтаграммы и, таким образом, он в общем случае не будет их получать. Однако, если домашний агент является также маршрутизатором, обслуживающим общий трафик IP, он может получать такие дейтаграммы для пересылки в домашнюю сеть. В этом случае домашний агент **должен** предполагать, что мобильный узел подключён к домашней сети и просто пересылать дейтаграммы напрямую в домашнюю сеть.

Для многодомных домашних агентом адресом отправителя во внешнем заголовке IP инкапсулированной дейтаграммы **должен** быть адрес, отправленный мобильному узлу в поле Home Agent регистрационного отклика. Т. е., домашний агент не может использовать адрес какого-либо иного сетевого интерфейса в качестве адреса отправителя.

В параграфе 4.1 рассмотрены методы инкапсуляции, которые могут применяться для туннелирования. Узлам, реализующим туннелирование, **следует** также поддерживать механизм tunnel soft state [32], позволяющий возвращать из туннеля сообщения ICMP об ошибках отправителям вызвавших ошибку дейтаграмм.

Домашний агент **должен** декапсулировать адресованные ему пакеты, инкапсулированные мобильным узлом с целью сокрытия своего реального местоположения, как описано в параграфе 5.5. Эта функция требуется также для поддержки реверсного туннелирования [27].

Если время Lifetime для данной мобильной привязки завершается до того, как домашний агент получает другое подходящее сообщение Registration Request для данного мобильного узла, такая привязка удаляется из списка. Домашнему агенту **недопустимо** передавать какие-либо сообщения Registration Reply, основываясь лишь на том, что срок привязки мобильного узла истекает. Запись для мобильного узла в списке посетителей внешнего агента будет устаревать естественным путём, возможно в одно время с завершением срока действия мобильной привязки у домашнего агента. Когда срок действия мобильной привязки у домашнего агента завершается, этот агент **должен** удалить привязку, но он **должен** сохранять все остальные (с незавершённым сроком) привязки, которые имеются у него для мобильного узла.

При получении дейтаграммы, направленной одному из зарегистрированных у домашнего агента мобильных узлов, агент **должен** проверить, не является ли эта дейтаграмму уже инкапсулированной. Если дейтаграмма уже инкапсулирована, она пересылается мобильному узлу с использованием приведённых ниже правил.

- Если внутренний (инкапсулированный) адрес получателя совпадает с внешним (мобильный узел), домашний агент **должен** также проверить внешний адрес отправителя инкапсулированной дейтаграммы (исходная точка туннеля). Если этот адрес совпадает с текущим адресом обслуживания мобильного узла, домашний агент **должен** отбросить эту дейтаграмму без уведомления для предотвращения маршрутной петли. Если адреса **не** совпадают, домашнему агенту **следует** переслать дейтаграмму мобильному узлу. В этом случае для пересылки домашний агент **может** просто сменить внешний адрес получателя на адрес обслуживания мобильного узла, не инкапсулируя дейтаграмму ещё раз.
- Если внутренний адрес в дейтаграмме **не** совпадает с внешним, домашнему агенту **следует** инкапсулировать дейтаграмму ещё паз, установив в качестве внешнего адреса получателя текущий адрес обслуживания мобильного узла. Т. е., домашний агент пересылает инкапсулированную дейтаграмму мобильному точно так же, как это делается для остальных дейтаграмм.

4.3. Широковещательные дейтаграммы

При получении домашним агентом широковещательной дейтаграммы **недопустимо** пересылать их каким-либо мобильным узлам из списка привязок, за исключением мобильных узлов, явно запросивших такую пересылку. Мобильный узел **может** запросить пересылку широковещательных дейтаграмм, установив флаг B в своём сообщении Registration Request (параграф 3.3). Каждому из таких мобильных узлов домашнему агенту **следует** пересылать полученные широковещательные дейтаграммы, при этом режим пересылки конкретных категорий широковещательных пакетов может устанавливаться в настройках конфигурации домашнего агента.

Если в регистрационном запросе мобильного узла был установлен бит D, указывающий на использование данным узлом совмещённого адреса обслуживания, домашний агент просто туннелирует соответствующие широковещательные дейтаграммы IP на адрес обслуживания мобильного узла. Если флаг D не установлен, домашний агент сначала инкапсулирует широковещательные дейтаграммы в дейтаграммы на индивидуальный домашний адрес мобильного узла и потом туннелирует их внешнему агенту. Дополнительная инкапсуляция нужна для того, чтобы внешний агент мог определить, какому из мобильных узлов следует переслать дейтаграмму после её декапсуляции. При получении дейтаграммы внешним агентом инкапсулированная дейтаграмма извлекается из туннеля и доставляется мобильному узлу, как обычные дейтаграммы. Мобильный узел должен сам декапсулировать полученную дейтаграмму для извлечения исходной широковещательной дейтаграммы.

4.4. Маршрутизация групповых дейтаграмм

Как было отмечено выше, мобильный узел, подключенный к своей домашней сети, функционирует так же, как обычный (не мобильный) хост или маршрутизатор. Таким образом, в домашней сети функции мобильного узла идентичны функциям других групповых отправителей и получателей. По этой причине в данном параграфе рассматривается лишь обработка групповых дейтаграмм для случая подключения мобильного узла к чужой сети.

Для получения группового трафика мобильный узел **должен** присоединиться к multicast-группе одним из двух способов. В первом варианте мобильный узел **может** присоединиться к группе через (локальный) групповой маршрутизатор сети, к которой он подключён. Этот вариант предполагает наличие группового маршрутизатора в чужой сети. Если мобильный узел использует совмещённый адрес обслуживания, ему **следует** указывать этот адрес в качестве адреса отправителя сообщений IGMP [11]. В противном случае он **может** использовать свой домашний адрес.

Кроме того, желающий получать групповой трафик мобильный узел **может** присоединиться к группе через двухсторонний туннель со своим домашним агентом (а предположении, что этот агент является групповым маршрутизатором). Мобильный узел туннелирует сообщения IGMP своему домашнему агенту, а тот пересылает групповые дейтаграммы в туннель к мобильному узлу. В туннелируемых домашнему агенту пакетах в качестве адреса отправителя **следует** указывать домашний IP-адрес мобильного узла.

Правила доставки групповых дейтаграмм мобильному узлу в этом случае идентичны правилам доставки широковещательных дейтаграмм (параграф 4.3). Если мобильный узел использует совмещённый адрес обслуживания (был установлен флаг D в регистрационном запросе мобильного узла), домашнему агенту **следует** туннелировать дейтаграммы на этот адрес обслуживания. В противном случае домашний агент **должен** сначала инкапсулировать дейтаграмму в индивидуальную дейтаграмму на домашний адрес мобильного узла, а затем **должен** дополнительно инкапсулировать полученную дейтаграмму (вложенное туннелирование) на адрес обслуживания мобильного узла. По

этой причине мобильный узел **должен** быть способен декапсулировать пакеты, отправленные на его домашний адрес для извлечения исходной групповой дейтаграммы.

Для мобильных узлов, желающих передавать дейтаграммы в multicast-группы также есть два варианта: (1) передача напрямую в чужую сеть или (2) передача через туннель к домашнему агенту. Поскольку групповая маршрутизация в общем случае зависит от IP-адреса отправителя, мобильный узел, напрямую передающий дейтаграммы в чужую сеть должен использовать в качестве IP-адреса отправителя совмещённый адрес обслуживания. Мобильный узел, использующий туннель к домашнему агенту, **должен** указывать свой домашний адрес в поле отправителя как групповой (внутренней), так и инкапсулированной (внешней) дейтаграммы. Для этого варианта домашний агент должен выполнять также функции группового маршрутизатора.

4.5. Мобильные маршрутизаторы

Мобильный узел может быть маршрутизатором, отвечающим за мобильность одной или множества сетей, которые перемещаются как единые объекты (возможно, на самолёте, корабле, поезде, автомобиле, велосипеде или каяке). Узлы, подключённые к обслуживаемой мобильным маршрутизатором сети, сами по себе могут быть стационарными узлами или мобильными узлами или маршрутизаторами. В этом документе такие сети называются «мобильными сетями».

Мобильный маршрутизатор может служить в качестве внешнего агента и предоставлять свой адрес для обслуживания мобильных узлов, подключённых к мобильной сети. Типичный пример маршрутизации для мобильных узлов через мобильный маршрутизатор приведён ниже.

a) Переносный компьютер отключается от домашней сети и позднее подключается к сети на борту самолёта. Этот компьютер использует Mobile IP для регистрации в чужой сети, используя для обслуживания адрес внешнего агента, найденный из сообщения Agent Advertisement от внешнего агента на борту самолёта.

b) Сеть самолёта. сама по себе является мобильной. Предположим, что узел, являющийся бортовым внешним агентом, служит также используемым по умолчанию маршрутизатором, который соединяет бортовую сеть с сетью Internet. Когда самолёт находится «дома», этот маршрутизатор подключается к некой стационарной сети в аэропорту, которая для этого маршрутизатора является домашней. Когда самолёт находится в воздухе, маршрутизатор время от времени регистрируется через радиоканал на внешних агентах, расположенных на земле по маршруту полёта. Домашний агент этого мобильного маршрутизатора располагается в стационарной сети «домашнего» аэропорта.

c) Некий узел-корреспондент отправляет дейтаграмму на переносный компьютер, адресуя её на домашний адрес этого компьютера. Изначально эта дейтаграмма маршрутизируется в домашнюю сеть переносного компьютера.

d) Домашний агент переносного компьютера перехватывает дейтаграмму в домашней сети и туннелирует её на адрес обслуживания переносного компьютера, которым в данном случае является адрес узла, служащего маршрутизатором и внешним агентом на борту самолёта. Обычная маршрутизация IP будет направлять дейтаграмму в стационарную сеть авиакомпании.

e) Домашний агент бортового маршрутизатора и внешнего агента перехватывает дейтаграмму и туннелирует её на текущий адрес обслуживания, которым в этом примере является некий внешний агент в наземной сети под самолётом. Исходная дейтаграмма будет инкапсулирована дважды - домашним агентом переносного компьютера и домашним агентом бортового маршрутизатора.

f) Внешний агент в наземной сети декапсулирует дейтаграмму, сохраняя инкапсуляцию домашнего агента переносного компьютера (внутреннюю) и получателем декапсулированной дейтаграммы будет адрес обслуживания переносного компьютера. Полученная в результате дейтаграмма будет передана по радиоканалу на борт самолёта.

g) Внешний агент на борту декапсулирует дейтаграмму, извлекая из неё исходную дейтаграмму от узла-корреспондента, направленную по домашнему адресу переносного компьютера. Внешний агент бортовой сети самолёта. доставит эту дейтаграмму через бортовую сеть по адресу канального уровня в переносной компьютер.

Этот пример иллюстрирует ситуацию с подключением мобильного узла к мобильной же сети. Т. е., мобильный узел мобилен по отношению к сети, которая сама является мобильной (по отношению к земле). Если узел фиксирован по отношению к мобильной сети (мобильная сеть является домашней для него), можно использовать любой из двух описанных ниже методов для того, чтобы дейтаграммы от узлов-корреспондентов маршрутизировались фиксированному узлу.

На домашнем агенте **можно** настроить для стационарного узла перманентную регистрацию, которая будет указывать адрес мобильного маршрутизатора в качестве адреса обслуживания стационарного компьютера. Для этого обычно используется домашний агент мобильного маршрутизатора. В этом случае домашний агент отвечает за анонсирование связности со стационарным узлом в мобильной сети с использованием обычных протоколов маршрутизации. Все дейтаграммы, направленные фиксированному узлу будут использовать описанную выше двойную инкапсуляцию.

В другом варианте мобильный маршрутизатор **может** анонсировать связность со всей мобильной сетью по обычным протоколам маршрутизации IP через двухсторонний туннель со своим домашним агентом. Этот метод не требует двойной инкапсуляции.

4.6. ARP, Proxy ARP и беспричинный ARP

Использование ARP [36] требует специальных правил для корректной работы с мобильными и беспроводными узлами. Изложенные в этом параграфе требования применимы ко всем домашним сетям, где используется преобразование адресов ARP.

В дополнение к обычному использования ARP для сопоставления адресов канального уровня с адресами IP в этом документе рассматриваются два специальных применения ARP, описанных ниже.

- Proxy ARP [39] представляет собой отклик ARP, передаваемый узлом от имени другого узла, который не способен или не хочет сам отвечать на запросы ARP. Отправитель Proxy ARP меняет местами поля Sender и Target Protocol Address, как описано в [36], и подставляет некий заданный в конфигурации (обычно, свой) адрес канального уровня в поле Sender Hardware Address. Получатель такого отклика будет связывать указанный в нем адрес канального уровня с IP-адресом исходного искомого узла, что приведёт к отправке в будущем адресованных целевому узлу пакетов на узел с указанным в отклике адресом канального уровня.

- Беспричинный (Gratuitous) ARP [45] представляет собой пакет ARP, переданный узлом для того, чтобы спонтанно вызвать на других узлах обновление записи в их кэше ARP. Для беспричинного ARP **могут** использоваться пакеты ARP Request или ARP Reply. В любом случае в полях ARP Sender Protocol Address и ARP Target Protocol Address устанавливается IP-адрес, для которого нужно обновить запись, а в поле ARP Sender Hardware Address - адрес канального уровня, который следует указать в обновлённой записи. При использовании пакетов ARP Reply в поле Target Hardware Address также устанавливается адрес канального уровня, для которого следует обновить запись в кэше (это поле не используется в пакетах ARP Request).

  В любом случае для беспричинного ARP пакеты ARP **должны** передаваться, как локальные широковещательные пакеты на локальном канале. Как указано в [36], любой узел, получивший пакет ARP (Request или Reply), **должен** обновить свой локальный кэш ARP, взяв аппаратный и протокольный адрес из пакета ARP, если в кэше имеется запись для указанного в пакете адреса IP. Это требование в протоколе ARP применяется даже для пакетов ARP Request и пакетов ARP Reply, не соответствующих каким-либо отправленным этим узлом пакетам ARP Request [36].

Когда мобильный узел регистрируется в чужой сети, его домашний агент использует proxy ARP [39] для ответа на получаемые им сообщения ARP Request, в которых запрашивается адрес мобильного узла на канальном уровне. При получении ARP Request домашний агент **должен** проверить искомый адрес IP из запроса и, если этот адрес соответствует IP-адресу какого-либо из мобильных узлов, зарегистрировавших свои мобильные привязки, агент **должен** передать сообщение ARP Reply от имени этого мобильного узла. После смены адресов отправителя и получателя в пакете [39] домашний агент **должен** установить в качестве адреса отправителя на канальном уровне соответствующий адрес интерфейса, через который будет отправлен пакет Reply.

Когда мобильный узел покидает домашнюю сеть и регистрирует привязку к чужой сети, его домашний агент использует беспричинный запрос ARP для обновления кэшей ARP на узлах домашней сети. Это побуждает узлы связать адрес домашнего агента на канальном уровне с домашним IP-адресом мобильного узла. При регистрации привязки мобильного узла, для которого раньше у домашнего агента не было мобильной привязки (агент предполагал нахождение мобильного узла в домашней сети) домашний агент **должен** передать беспричинный запрос ARP от имени мобильного узла. Этот беспричинный пакет ARP **должен** передаваться, как широковещательный для канала, на котором размещается домашний адрес мобильного узла. Поскольку для широковещательный пакетов на локальном канале (типа Ethernet) доставка обычно не гарантируется, беспричинный пакет ARP **следует** передать несколько раз в целях повышения вероятности доставки.

Когда мобильный узел возвращается в свою домашнюю сеть, он и его домашний агент используют беспричинные пакеты ARP для того, чтобы стимулировать на узлах домашней сети обновление кэшей ARP для восстановления привязки адреса мобильного узла на канальном уровне с его домашним адресом IP. Перед отправкой своему домашнему агенту запроса на (де)регистрацию мобильный узел **должен** передать беспричинный пакет ARP в свою домашнюю сеть, используя локальный широковещательный адрес для данного канала. Беспричинный пакет ARP **следует** передать несколько раз для повышения вероятности его доставки; процедуру повтора **следует** выполнять параллельно с передачей и обработкой (де)регистрационного запроса.

Когда домашний агент мобильного узла получает и воспринимает такой запрос на (де)регистрацию, он также должен передать беспричинный пакет ARP в домашнюю сеть мобильного узла. Этот беспричинный пакет ARP используется также для связывания домашнего адреса мобильного узла с его адресом на канальном уровне. Беспричинный пакет ARP передаётся мобильным узлом и его домашним агентом, поскольку в случае беспроводных сетей области приёма пакетов от них могут различаться. Пакет ARP от домашнего агента **должен** передаваться, как локальный широковещательный пакет для домашнего канала мобильного узла и передачу **следует** повторять несколько раз для повышения вероятности доставки; повтор передачи **следует** выполнять параллельно с передачей и обработкой (де)регистрационного отклика.

Пока мобильный узел находится за пределами домашней сети, ему **недопустимо** передавать какие-либо широковещательные сообщения ARP Request или ARP Reply. Более того, в этом случае ему **недопустимо** отвечать на сообщения ARP Request, в которых в качестве целевого указан его домашний адрес IP, если сообщение ARP Request не было направлено по индивидуальному адресу внешним агентом, на котором у мобильного узла имеется действующая регистрация. В последнем случае мобильный узел **должен** передавать индивидуальное сообщение ARP Reply этому внешнему агенту. Отметим, что мобильному узлу, использующему совмещённый адрес обслуживания при получении ARP Request, в котором целевым адресом IP указан его адрес обслуживания, **следует** отвечать на такой запрос. Отметим также, что при передаче Registration Request в чужую сеть мобильный узел может определить адрес внешнего агента на канальном уровне из полученного от этого агента сообщения Agent Advertisement без передачи широковещательного сообщения ARP Request.

Порядок применения рассмотренных выше требований по применению ARP, proxy ARP и беспричинных ARP относительно передачи и обработки мобильным узлом сообщений Registration Request и Registration Reply при выходе из домашней сети и возвращении в неё имеет важное значение для работы протокола.

При выходе мобильного узла из домашней сети **должны** выполняться перечисленные ниже шаги в указанном порядке:

- Мобильный принимает решение о регистрации за пределами домашней сети (возможно в результате приёма Agent Advertisement от внешнего агента и отсутствие свежих анонсов от домашнего агента).

- Перед отправкой Registration Request отключает у себя обработку будущих сообщений ARP Request, которые могут запрашивать адрес канального уровня для его домашнего адреса, за исключением тех, которые нужны для взаимодействия с внешними агентами в чужой сети.

- Мобильный узел передаёт Registration Request.

- Когда домашний агент мобильного узла получает и воспринимает Registration Request, он отправляет беспричинный пакет ARP от имени мобильного узла и начинает использование proxy ARP для ответа на сообщения ARP Request, запрашивающие адрес канального уровня мобильного узла. В беспричинных пакетах ARP поле ARP Sender Hardware Address содержит адрес домашнего агента на канальном уровне. Если же домашний агент отвергает сообщение Registration Request, он не выполняет какой-либо обработки ARP (беспричинных или proxy).

При возвращении мобильного узла в домашнюю сеть **должны** выполняться перечисленные ниже шаги в указанном порядке:

- Мобильный принимает решение о регистрации в домашней сети (возможно в результате приёма Agent Advertisement от домашнего агента).
- Перед отправкой Registration Request включает у себя обработку будущих сообщений ARP Request, которые могут запрашивать адрес канального уровня для его домашнего адреса.
- Мобильный узел передаёт беспричинный пакет ARP, указывая в поле ARP Sender Hardware Address свой адрес канального уровня.
- Мобильный узел передаёт Registration Request.
- Когда домашний агент мобильного узла получает и воспринимает Registration Request, он прекращает использование proxy ARP для ответа на сообщения ARP Request с запросом адреса канального уровня для мобильного узла и передаёт беспричинный пакет ARP от имени мобильного узла, указывая в поле ARP Sender Hardware Address адрес канального уровня этого узла. Если домашний агент отвергает Registration Request, ему **недопустимо** вносить какие-либо изменения в обработку ARP (беспричинных или proxy) для этого узла. В этом последнем случае домашнему агенту следует вести себя, как будто мобильный узел не возвращался в домашнюю сеть и продолжать использование proxy ARP от имени мобильного узла.

5. Вопросы безопасности

Мобильные компьютерные среды могут очень существенно отличаться от обычных компьютерных сред. Во многих случаях для подключения мобильных узлов используются беспроводные соединения. Такие соединения потенциально уязвимы для пассивного перехвата, активных атак с использованием перехваченных ранее пакетов и других методов.

5.1. Коды аутентификации сообщений

Домашние агенты и мобильные узлы **должны** поддерживать аутентификацию. По умолчанию используется алгоритм HMAC-MD5 [23] с размером ключей 128 битов. Внешние агенты также **должны** поддерживать аутентификацию с использованием алгоритма HMAC-MD5 и ключами размером не меньше 128 битов, распространяемыми вручную. **Должны** поддерживаться ключи с произвольными двоичными значениями.

Защита данных и общего секрета на основе префикса и суффикса с использованием MD5 специалистами по криптографии признана уязвимой. В тех случаях, где требуется совместимость со старыми версиями Mobile IP, использующими этот режим, новым реализациям **следует** включать MD5 с ключом [41] в качестве дополнительного алгоритма аутентификации для использования при создании и проверке аутентификационных данных в регистрационных сообщениях Mobile IP (например, в расширениях, описанных в параграфах 3.5.2, 3.5.3, 3.5.4).

Для всех этих расширений **могут** также поддерживаться дополнительные алгоритмы аутентификации и режимы, а также методы распространения ключей и размеры ключей.

5.2. Вопросы безопасности, связанные с этим протоколом

Протокол регистрации, описанный в данном документе, обеспечивает туннелирование трафика мобильного узла на его адрес обслуживания. Такое туннелирование может создавать существенную уязвимость, если регистрация не была аутентифицирована. Удалённое перенаправление, выполняемое протоколом мобильной регистрации, порождает широко известную проблему безопасности в современной сети Internet, если при регистрации не применяется аутентификация сторон [2]. Более того, использование протокола преобразования адресов (ARP) без аутентификации позволяет организовать «кражу» трафика другими хостами. Использование Gratuitous ARP (параграф 4.6) снимает риски, связанные с применением ARP.

5.3. Управление ключами

Эта спецификация требует поддержки строгого механизма аутентификации (MD5 с ключом), который предотвратит множество атак, основанный на протоколе регистрации Mobile IP. Однако по причине сложности распространения ключей в отсутствие сетевого протокола управления ключами обмен сообщениями с внешними агентами разрешается выполнять без аутентификации. В коммерческих средах может стать важной аутентификация всех сообщений между внешним и домашним агентами, поскольку это может быть связано с оплатой услуг сервис провайдера за подключение мобильного узла.

5.4. Выбор случайных чисел

Стойкость любого механизма аутентификации зависит от ряда факторов, включая стойкость используемого алгоритма, защищенность и стойкость используемых ключей, а также качество конкретной реализации. Данная спецификация требует от реализаций использовать для аутентификации MD5 с ключом, но не исключает применения других алгоритмов и режимов. Для обеспечения эффективности MD5 с ключом 128-битовые ключи должны быть секретными (известными только уполномоченным сторонам) и псевдослучайными. При использовании nonce вкупе с защитой от повторного использования, значения nonce также должны выбираться с осторожностью. Eastlake и др. в работе [14] приводят более подробную информацию о создании псевдослучайных значений.

5.5. Конфиденциальность

Пользователям, работающим с данными, которые они не желают раскрывать другим, следует использовать для защиты дополнительные механизмы (типа шифрования), рассмотрение которых выходит за рамки данного документа. Пользователям, озабоченным возможностью анализа трафика, следует применять шифрование на канальном уровне. Если требуется скрывать реальное местоположение мобильных узлов, они могут создавать туннели со своими домашними агентами. В этом случае дейтаграммы для узлов-корреспондентов будут выглядеть исходящими из домашней сети и определить реальное местоположение мобильного узла будет сложнее. Эти механизмы выходят за рамки данного документа.

5.6. Фильтрация на входе

Многие маршрутизаторы поддерживают политику безопасности на базе входной фильтрации (ingress filtering) [15], которая не позволяет пересылать пакеты с топологически некорректными адресами отправителей. В средах, где такая фильтрация вызывает проблемы, мобильные узлы могут использовать реверсное туннелирование [27] с использованием предоставленного внешним агентом адреса обслуживания в качестве Source Address. Пакеты мобильных узлов в таких туннелях будут нормально проходить через маршрутизаторы с входной фильтрацией, поскольку эти пакеты не будут с точки зрения топологии отличаться от пакетов узлов, не являющихся мобильными.

5.7. Защита от повторного использования для Registration Request

Поле Identification позволяет домашнему агенту убедиться в том, что регистрационное сообщение недавно создано мобильным узлом и не является повторно используемым атакующим сообщением, которое было перехвачено в предшествующей регистрации. В этом параграфе описаны два метода защиты от повторного использования - с помощью временных меток (обязательный) и с помощью nonce (необязательный). Все мобильные узлы и домашние агенты **должны** поддерживать защиту от повторов с помощью временных меток. Узлы **могут** также поддерживать защиту на основе nonce (см. Приложение A).

Стиль защиты от повторного использования между мобильным узлом и его домашним агентом устанавливается при организации защищённой связи между ними. Мобильный узел и домашний агент **должны** согласовать используемый для защиты от повторов метод. Интерпретация поля Identification зависит от выбранного метода защиты, как описано ниже.

Для любого из используемых методов младшие 32 бита поля Identification **должны** копироваться из Registration Request в Registration Reply. Внешний агент использует эти биты (и домашний адрес мобильного узла) для сопоставления регистрационных запросов с откликами на них. Мобильный узел **должен** убедиться, что 32 младших бита поля идентификации в любом сообщении Registration Reply совпадают с аналогичными битами, переданными им в сообщении Registration Request.

В новом сообщении Registration Request **недопустимо** использовать значение Identification из непосредственно предшествовавшего ему запроса и **не следует** использовать одно и то же значение поля более одного раза в рамках одного защищённого контекста между мобильным узлом и домашним агентом. Разрешается повтор, описанный в параграфе 3.6.3.

5.7.1. Защита от повторного использования с помощью временных меток

Базовым принципом защиты от повторов с помощью временных меток является включение узлом текущего времени в генерируемые сообщения и проверка на приёмной стороне близости этого значения к текущему времени у получателя. Если между сторонами при создании защищённой связи явно не согласовано иное, допустимым **можно** считать расхождение времени до 7 секунд. **Следует** во всех случаях использовать предел допустимого расхождения более 3 секунд. Очевидно, что часы на узлах должны быть подобающим образом синхронизированы. Сообщения синхронизации, как и все прочие сообщения, могут быть защищены от несанкционированного доступа с помощью механизма аутентификации, определённого при создании между парой узлов защищённого контекста.

При использовании временный меток мобильный узел **должен** помещать в поле Identification 64-битовое значение времени в формате NTP[1] [26]. 32 младших бита в формате NTP представляют доли секунды и эти биты, которые недоступны для синхронизации через сеть, **следует** заполнять случайными значениями с использованием хорошего генератора случайных чисел. Следует отметить, что при использовании временных меток 64-битовое значение Identification в сообщении Registration Request от мобильного узла **должно** быть больше, нежели в предыдущем сообщении Registration Request, поскольку домашние агенты используют это поле также в качестве порядкового номера. Без использования такой нумерации возможны случаи, когда прибывший с задержкой дубликат более раннего регистрационного запроса (в пределах допустимого расхождения по времени) будет применён с нарушением порядка, ошибочно меняя текущий зарегистрированный адрес обслуживания мобильного узла.

При получении Registration Request с разрешающим аутентификацию расширением домашний агент **должен** проверить корректность поля Identification. Корректное значение временной метки в поле Identification **должно** быть достаточно близко к текущему времени по часам домашнего агента и **должно** быть больше воспринятых ранее для этого мобильного узла временных меток. Детали возможной рассинхронизации часов зависят от конкретной защищённой связи.

Если значение временной метки приемлемо, домашний агент копирует целиком поле Identification в сообщение Registration Reply и возвращает отклик мобильному узлу. В случае неприемлемого значения временной метки домашний агент копирует только младшие 32 бита в сообщение Registration Reply, а в старшие 32 бита помещает значение времени по своим часам. В этом случае домашний агент **должен** отвергнуть регистрацию, возвращая в сообщении Registration Reply код 133.

Как описано в параграфе 3.6.2.1, мобильный узел **должен** убедиться, что младшие 32 бита поля Identification в сообщении Registration Reply битам отвергнутого регистрационного запроса, прежде чем использовать старшие биты для корректировки своих часов.

[1] Network Time Protocol - протокол сетевого времени.

5.7.2. Защита от повторного использования с помощью Nonce

Базовый принцип защиты от повторного использования с помощью nonce заключается в том, что узел A включает новое случайное значение в каждое сообщение для узла B и проверяет наличие этого значения в отправленных ему сообщениях узла B. В обоих сообщениях используется код аутентификации для защиты от изменения значений nonce. Одновременно узел B может помещать свои значения nonce во все сообщения узлу A (которые узел A будет возвращать) и этого вполне достаточно для проверки свежести получаемых сообщений.

Можно ожидать у домашних агентов наличия ресурсов, достаточных для расчёта псевдослучайных значений [14]. Домашний агент помещает новое значение nonce в 32 старших бита поля Identification каждого сообщения Registration Reply. Младшие 32 бита поля Identification домашний агент копирует из сообщения Registration Request в идентичные биты сообщения Registration Reply. Мобильный узел, получая от домашнего агента аутентифицированное сообщение Registration Reply, сохраняет старшие 32 бита поля Identification для использования в качестве 32 старших битов поля идентификации в следующем сообщении Registration Request.

Мобильный узел отвечает за генерацию младших 32 битов поля Identification в каждом сообщении Registration Request. В идеальном варианте для этого следует использовать сгенерированные узлом случайные значения nonce. Однако допускается использование других методов, включая дублирование случайного значения, полученного от домашнего агента. Выбор метода определяется только самим мобильным узлом, поскольку именно он проверяет корректность значения в полученном отклике Registration Reply. Старшие и младшие 32-битовые компоненты поля Identification **следует** делать отличными от предыдущих значений. Домашний агент использует новое значение для старших битов, а мобильный узел - новое значение младших битов в каждом регистрационном сообщении. Внешний агент использует значение младших битов (и домашний адрес мобильного узла) для корректного сопоставления регистрационных откликов с ожидающими запросами (параграф 3.7.1).

Если регистрационное сообщение отвергается по причине некорректности значения nonce, в отклике мобильному узлу всегда передаётся новое значение nonce для использования при следующей регистрации. Таким образом обеспечивается самосинхронизация протокола nonce.

6. Согласование с IANA

Протокол Mobile IP задаёт несколько новых числовых пространств для использования в различных полях сообщений. Эти пространства включают:

- Сообщения Mobile IP разных типов, передаваемые в порт UDP 434, как указано в параграфе 1.8.
- Типы расширений для сообщений Registration Request и Registration Reply (см. параграфы 3.3 и 3.4, а также [27, 29, 6, 7, 12]).
- Значения кодов (Code) для сообщений Registration Reply (см. параграф 3.4, а также [27, 29, 6, 7, 12]).
- В Mobile IP определены сообщения Agent Solicitation и Agent Advertisement. Фактически они относятся к сообщениям Router Discovery [10], дополненным специфическими расширениями Mobile IP. Таким образом, для этих сообщений не требуется новое пространство имён, но нужно определить расширения для Router Discovery, как описано ниже в параграфе 6.2 (см. параграф 2.1 и работы [7, 12].

Дополнительные пространства значений для Mobile IP указаны в [7].

Информацию о выделении значений для Mobile IP взятых из внешних по отношению к данному документу спецификаций можно найти в реестрах IANA по ссылке http://www.iana.org/numbers.html. Открыв указанную ссылкой страницу, следует выбрать ссылку [M] в Directory of General Assigned Numbers и далее найти раздел Mobile IP Numbers.

6.1. Типы сообщений Mobile IP

Сообщения Mobile IP в соответствии с их определением передаются получателю в порт 434 (UDP или TCP). Пространство номеров для сообщений Mobile IP задано в параграфе 1.8. Одобрение новых номеров для сообщений выполняется по процедуре Expert Review и требует их спецификации [30]. Стандартизованные к настоящему времени типы сообщений указаны в таблице вместе с номерами параграфов, где они определены.

Тип	*Название*	*Описание*
1	Registration Request	3.3
3	Registration Reply	3.4

6.2. Расширения для RFC 1256 Router Advertisement

В RFC 1256 определены два типа сообщений ICMP - Router Advertisement и Router Solicitation. Mobile IP определяет пространство номеров для расширений Router Advertisement, которые могут использоваться протоколами, отличными от Mobile IP. Стандартизованные к настоящему времени расширения указаны в таблице вместе с параграфами, где эти расширения определены.

Тип	*Название*	*Описание*
0	One-byte Padding	2.1.3
16	Mobility Agent Advertisement	2.1.1
19	Prefix-Lengths	2.1.2

Одобрение новых номеров для расширений, используемых Mobile IP, выполняется по процедуре Expert Review и требует спецификации таких расширений [30].

6.3. Расширения для регистрационных сообщений Mobile IP

Сообщения Mobile IP, определённые в этом документе и перечисленные в параграфах 1.8 и 6.1, могут включать расширения. Расширения для сообщений Mobile IP используют общее пространство номеров, даже если расширения относятся к разным сообщениям Mobile IP. Пространство номеров для расширений Mobile IP задан в настоящем документе. Добавление расширений выполняется по процедуре Expert Review, для новых расширений нужны спецификации [30].

Тип	*Название*	*Описание*
0	One-byte Padding	
32	Mobile-Home Authentication	3.5.2
33	Mobile-Foreign Authentication	3.5.3
34	Foreign-Home Authentication	3.5.4

6.4. Коды для регистрационных откликов Mobile IP

В сообщениях Mobile IP Registration Reply, описанных в параграфе 3.4, имеется поле Code. Пространство значений для кодов также определено в параграфе 3.4. Пространство значений Code структурировано по результатам обработки регистрационных запросов, как показано в таблице.

0-8	Коды успешного завершения
09-63	В настоящее время нет рекомендаций по распределению
64-127	Коды ошибок от внешнего агента
128-192	Коды ошибок от домашнего агента
193-255	В настоящее время нет рекомендаций по распределению

Выделение новых значений для кодов происходит по процедуре Expert Review [30].

7. Благодарности

Особая благодарность Steve Deering (Xerox PARC) вместе с Dan Duchamp и John Ioannidis (JI) (Columbia University) за формирование рабочей группы, руководство ею и значительный вклад в работу на её начальном этапе. Ранние работы университета Columbia по Mobile IP опубликованы в [18, 19, 17].

Благодарим также Kannan Alaggapan, Greg Minshall, Tony Li, Jim Solomon, Erik Nordmark, Basavaraj Patil и Phil Roberts за их вклад в работу группы в качестве председателей, а также за их полезные комментарии.

Спасибо активным участникам рабочей группы Mobile IP, особенно тем, кто готовил тексты документов, включая (в алфавитном порядке):

- Ran Atkinson (Naval Research Lab),
- Samita Chakrabarti (Sun Microsystems)
- Ken Imboden (Candlestick Networks, Inc.)
- Dave Johnson (Carnegie Mellon University),
- Frank Kastenholz (FTP Software),
- Anders Klemets (KTH),
- Chip Maguire (KTH),
- Alison Mankin (ISI)
- Andrew Myles (Macquarie University),
- Thomas Narten (IBM)
- Al Quirt (Bell Northern Research),
- Yakov Rekhter (IBM),
- Fumio Teraoka (Sony),
- Alper Yegin (NTT DoCoMo).

Спасибо Charlie Kunzinger и Bill Simpson - редакторам, подготовившим первый вариант этого документа, где были отражены дискуссии в рабочей группе. Значительная часть текста, добавленного в последние версии RFC 2002, обязана своим появлением Jim Solomon и Dave Johnson.

Спасибо Greg Minshall (Novell), Phil Karn (Qualcomm), Frank Kastenholz (FTP Software) и Pat Calhoun (Sun Microsystems) за их поддержку при организации встреч рабочей группы.

Параграфы 1.10 и 1.11, задающие спецификации новых форматов расширений для использования с агрегируемыми типами расширений, были включены из спецификации (Mobile IP Extensions Rationalization (MIER)), подготовленной:

- Mohamed M.Khalil, Nortel Networks
- Raja Narayanan, nVisible Networks
- Haseeb Akhtar, Nortel Networks
- Emad Qaddoura, Nortel Networks

Спасибо этим авторам, а также другим участникам работы по MIER, включая Basavaraj Patil, Pat Calhoun, Neil Justusson, N. Asokan и Jouni Malinen.

A. Патенты

никаких усилий в части идентификации таких прав. Информацию о процедурах IETF, связанных с правами в проектах стандартов и связанных со стандартами документах можно найти в BCP-11. Копии заявлений о правах, доступных для публикации, и все заверения лицензий, которые должны быть доступными, а также результаты попыток получить общую лицензию или право на использование таких прав разработчиками или пользователями данной спецификации могут быть получены в секретариате IETF.

IETF приглашает все заинтересованные стороны заявить о всех авторских правах, патентах или заявках на патенты, а также иных правах собственности, которые могут быть связаны с описанной здесь технологией и могут потребоваться при практической реализации данного стандарта. Информацию следует направлять исполнительному директору IETF.

B. Канальный уровень

Мобильный узел **может** использовать механизмы канального уровня для принятия решения о смене своей точки подключения к сети. К таким индикаторам относятся состояние интерфейса (Down/Testing/Up) [24], смена «ячейки» или администрирования. Механизмы зависят от применяемой технологии канального уровня и выходят за рамки документа.

Протокол PPP [42] и его протокол управления IPCP [25] согласуют использование адресов IP. Мобильному узлу **следует** сначала попытаться использовать свой домашний адрес - в этом случае при подключении к домашней сети немаршрутизируемый канал будет работать корректно. Если домашний адрес не будет восприниматься партнёром и мобильному узлу будет динамически выделен временный адрес IP, а данный мобильный узел способен работать с совмещённым адресом обслуживания, он **может** зарегистрировать полученный адрес в качестве совмещённого адреса обслуживания. Когда партнёр задаёт свой адрес IP, **недопустимо** считать его адресом обслуживания на внешнем агенте или IP-адресом домашнего агента.

Расширения PPP для Mobile IP заданы в RFC 2290 [44]. В этом документе содержатся дополнительные сведения в части более эффективного присвоения адресов от PPP.

C. Вопросы, связанные с TCP

C.1. Таймеры TCP

При работе по каналам с большими задержками (например, SATCOM) или малой скоростью (например, радиоканалы) некоторые реализации TCP могут использовать недостаточно эффективные (нестандартные) значения тайм-аута повторной передачи. В таких случаях могут возникать тайм-ауты даже при корректной работе сети и канала просто в результате продолжительной задержки в используемой среде передачи. Это может приводить к отказам при организации и поддержке соединений TCP через такие каналы, а также приводить к ненужным повторам передачи, потребляющим доступную полосу канала. Разработчикам рекомендуется при реализации механизма тайм-аутов TCP следовать алгоритмам, описанным в 2988 [31]. Разработчикам систем, предназначенных для узкополосных каналов с большими задержками следует пользоваться рекомендациями RFC 2757 и RFC 2488 [28, 1]. Разработчикам мобильных узлов следует принимать во внимание возможность возникновения упомянутых здесь проблем.

C.2. Контроль насыщения TCP

Мобильные узлы зачастую используют среды с достаточно высокой частотой ошибок, что приводит к потере большого числа пакетов. Это приводит к возникновению конфликтов с механизмами контроля насыщения в современных реализациях [21]. Однако при отбрасывании пакетов реализация TCP на узле-корреспонденте будет, скорей всего, реагировать как на возникновение перегрузки и запускать механизмы замедленного старта (slow-start) [21], предназначенные для решения этой проблемы. Однако такие механизмы не подходят для каналов, которые сами по себе порождают множество ошибок, и на практике усиливает негативное воздействие от потери пакетов. Данная проблема была проанализирована Caceres и др. в работе [5]. Решения проблемы для методов обработки ошибок TCP, которые могут конфликтовать с механизмами контроля насыщения, рассмотрены в документах [3, 9] рабочей группы [pilc]. Хотя такие решения выходят за рамки данного документа, они показывают, что обеспечение прозрачной работы мобильных узлов включает механизмы, лежащие за пределами сетевого уровня. Проблемы, вызываемые большим числом ошибок в среде передачи, указывают на необходимость избегать решений с систематическим отбрасыванием пакетов, что следует принимать во внимание при выборе инженерных решений.

D. Примеры

В этом приложении приведены примеры сообщений Registration Request для нескольких типичных случаев.

D.1. Регистрация с адресом обслуживания от внешнего агента

Мобильный узел получает сообщение Agent Advertisement от внешнего агента и принимает решение зарегистрироваться у него с использованием анонсированного агентом адреса обслуживания. Мобильный узел желает использовать лишь инкапсуляцию IP-in-IP, ему не нужна поддержка широковещания и одновременные мобильные привязки:

Поля IP

Source Address = домашний адрес мобильного узла;

Destination Address = копируется адрес отправителя из сообщения Agent Advertisement;

Time to Live = 1.

Поля UDP

Source Port = <любой>;

Destination Port = 434;

Поля Registration Request

Type = 1;

S=0,B=0,D=0,M=0,G=0;

Lifetime = значение Registration Lifetime копируется из Mobility Agent Advertisement Extension сообщения Router Advertisement;

Home Address = домашний адрес мобильного узла;

Home Agent = IP-адрес домашнего агента мобильного узла;

Care-of Address = копируется из Mobility Agent Advertisement Extension сообщения Router Advertisement;

Identification = временная метка NTP или Nonce.

Расширения

Разрешающее проверку полномочий расширение (например, Mobile-Home Authentication Extension).

D.2. Регистрация с совмещённым адресом обслуживания

Мобильный узел подключается к чужой сети, где нет внешних агентов. Он получает адрес от сервера DHCP [13] для использования в качестве совмещённого адреса обслуживания. Мобильный узел поддерживает все формы инкапсуляции (IP-in-IP, минимальная, GRE), хочет получать копии широковещательных дейтаграмм из домашней сети и не требует одновременных привязок мобильности.

Поля IP

Source Address = адрес обслуживания, полученный от сервера DHCP;

Destination Address = IP-адрес домашнего агента;

Time to Live = 64.

Поля UDP

Source Port = <любой>;

Destination Port = 434.

Поля Registration Request

Type = 1;

S=0,B=1,D=1,M=1,G=1;

Lifetime = 1800 (секунд);

Home Address = домашний адрес мобильного узла;

Home Agent = IP-адрес домашнего агента мобильного узла;

Care-of Address = адрес обслуживания, полученный от сервера DHCP;

Identification = временная метка NTP или Nonce.

Расширения

Mobile-Home Authentication Extension.

D.3. Дерегистрация

Мобильный узел возвращается в домашнюю сеть и хочет отменить регистрацию всех адресов обслуживания.

Поля IP

Source Address = домашний адрес мобильного узла;

Destination Address = IP-адрес домашнего агента мобильного узла;

Time to Live = 1.

Поля UDP

Source Port = <любой>;

Destination Port = 434.

Поля Registration Request

Type = 1:

S=0,B=0,D=0,M=0,G=0;

Lifetime = 0;

Home Address = домашний адрес мобильного узла;

Home Agent = IP-адрес домашнего агента мобильного узла;

Care-of Address = домашний адрес мобильного узла;

Identification = временная метка NTP или Nonce.

Разрешающее проверку полномочий расширение (например, Mobile-Home Authentication Extension).

E. Применимость расширения Prefix-Lengths

Расширение Prefix-Lengths следует с осторожностью применять в беспроводных сетях по причине неравномерности радиопокрытия. Эта неравномерность может приводить к тому, что два внешних агента, анонсирующие один и тот же префикс, будут предлагать мобильным узлам два разных соединения. Расширение Prefix-Lengths **не следует** включать в анонсы, передаваемые агентами в таких конфигурациях.

Внешние агенты с разными беспроводными интерфейсами должны кооперироваться с помощью специальных протоколов для обеспечения идентичного покрытия в пространстве, чтобы заявлять наличие беспроводных интерфейсов в одну и ту же подсеть. В случае проводных интерфейсов при отключении мобильного узла и его последующем подключении к другой точке этот узел может передавать новое сообщение Registration Request даже в тех случаях, когда новая точка подключения относится к той же среде, к которой относился предшествующий зафиксированный анонс. В сетях с высокой плотностью внешних агентов не представляется разумным требовать распространения через протоколы маршрутизации префиксов подсетей, связанных с каждым беспроводным внешним агентом, поскольку это могло бы приводить к быстрому переполнению таблиц маршрутизации, неоправданным расходам времени на обработку маршрутных обновлений и значительным задержкам при выборе маршрута, если сохранять маршруты для беспроводных сетей (обычно этого не требуется).

F. Вопросы совместимости

Этот документ является пересмотром RFC 2002 с целью повышения уровня совместимости решений путём устранения неоднозначностей. Реализации, которые выполняют аутентификацию в соответствии с новым, заданным более точно, алгоритмом, будут совместимы с более старыми реализациями, которые создают аутентификационные данные в соответствии с изначальными представлениями. Это было раньше основной причиной несовместимости.

Однако данная спецификация не включает новых функций, использование которых будет вызывать проблемы взаимодействия с более старыми реализациями. Все функции, указанные в RFC 2002 будут работать с новыми реализациями, за исключением сжатия V-J [20]. В приведённом ниже списке более подробно указаны возможные проблемы совместимости, которые могут возникать на узлах, соответствующих новой спецификации, при взаимодействии с реализациями RFC 2002.

- клиент, ожидающий той или иной из ставших в новой спецификации обязательными функций (например, реверсного туннелирования) от внешнего агента, не будет сталкиваться с проблемами взаимодействия, если он принимает во внимание значение флага T;
- мобильные узлы, использующие для идентификации самих себя расширение NAI, не смогут взаимодействовать со старыми агентами мобильности;
- мобильные узлы, использующие нулевое значение для домашнего адреса и желающие получить свой домашний адрес в сообщении Registration Reply, не смогут взаимодействовать со старыми агентами мобильности;
- мобильные узлы, пытающиеся аутентифицировать себя без использования расширения Mobile-Home, не смогут зарегистрироваться у своего домашнего агента.

Во всех указанных случаях отказоустойчивый и правильно настроенный мобильный узел с высокой вероятностью будет способен восстановить работу, выполнив подобающие действия при получении Registration Reply с кодом ошибки, указывающим причину отказа в регистрации. Например, если мобильный узел передаёт регистрационный запрос, который отвергается по причине указания в нем неприемлемого аутентификационного расширения, этот узел повторить попытку регистрации с использованием расширения Mobile-Home Authentication, поскольку внешний и/или домашний агент в этом случае не был настроен на использование других аутентификационых данных.

G. Отличия от RFC 2002

В этом приложении рассматриваются отличия исходной базовой спецификации Mobile IP (RFC 2002 и последующие документы), которые были внесены в процессе обновления спецификации Mobile IP.

G.1. Основные изменения

- Спецификация для адреса Destination IP в сообщениях Registration Reply от внешнего агента для предотвращения возможности передачи IP-адреса 0.0.0.0.
- Спецификация двух новых типов расширений Mobile IP в соответствии с идеями MIER.
- Указано использование SPI аутентификационного расширения MN-HA, как части данных, к которым должен применяться алгоритм аутентификации.
- Отказ от поддержки сжатия Van-Jacobson.
- Указание, что внешние агенты **могут** передавать анонсы чаще одного раза в секунду при условии, что они не будут занимать слишком большую часть полосы локального канала. Для простоты принимается, что внешний агент **может** передавать анонсы с интервалом в 1/3 анонсируемого значения ICMP Lifetime.
- Указание, что внешним агентам **следует** поддерживать реверсное туннелирование, а домашние агенты **должны** поддерживать декапсуляцию таких туннелей.
- Изменены требования параграфа 3.6 для мобильных узлов с целью отражения определённой в RFC 2794 [6] возможности мобильного узла идентифицировать самого себя с использованием NAI и получить домашний адрес из сообщения Registration Reply.

- В параграф 3.7.3.1 внесены изменения, в соответствии с которыми от внешнего агента не требуется отбрасывать сообщения Registration Reply, где поле Home Address не соответствует ни одному из ожидающих сообщений Registration Request.
- Разрешена аутентификация регистрации с использованием защищённых связей между мобильным узлом и подходящим агентом аутентификации, приемлемым для домашнего агента. Определено расширение Authorization-enabling для аутентификации, которое делает регистрационное сообщение воспринимаемым для получателя. Это требуется в соответствии со спецификацией [6].
- Задано обязательное использование HMAC-MD5 взамен режима MD5 prefix+suffix, указанного в RFC 2002.
- Указано, что мобильному узлу **следует** брать первый адрес из упорядоченного списка, предложенного внешним агентом, и **можно** пробовать все последующие анонсированные адреса, если попытка регистрации была отвергнута внешним агентом.
- Разъяснено, что агентам мобильности **следует** помещать только свой собственный адрес с начальный (не связанный с мобильностью) список маршрутизаторов в анонсах мобильности. RFC 2002 разрешал агентам мобильности анонсировать другие маршрутизаторы для использования по умолчанию.
- Указано, что мобильный узел **должен** игнорировать резервные биты в сообщениях Agent Advertisement, не отбрасывая самих сообщений. В этом случае, определённые позднее биты не помешают мобильным узлам использовать анонсы, несмотря на наличие непонятных битов. Кроме того, внешние агенты могут устанавливать бит R для указания того, что они сами обрабатывают новые биты, вместо не понимающих эти биты агентов мобильности.
- Указано, что внешний агент проверяет указанный адрес домашнего агента на предмет (не)принадлежности к какому-либо из интерфейсов внешнего агента до трансляции сообщения Registration Request. Если указанный адрес относится к одной из сетей внешнего агента и этот агент не является домашним для мобильного узла, запрос отвергается с возвратом кода 136 (неизвестный адрес домашнего агента).
- Указано, что находящемуся вне домашней сети мобильному узлу **недопустимо** передавать широковещательные пакеты ARP для определения MAC-адреса другого узла Internet. Таким образом, список (возможно пустой) Router Addressesиз компоненты ICMP Router Advertisement в сообщении бесполезен для выбора используемого по умолчанию маршрутизатора, если у мобильного узла нет какого-либо способа получить MAC-адрес одного из маршрутизаторов в этом списке без применения широковещательных пакетов. Аналогично, в отсутствие механизмов определения MAC-адресов в чужой сети мобильный узел **должен** игнорировать все другие маршрутизаторы в чужой сети.
- Указано, что внешнему агенту **недопустимо** использовать широковещательные пакеты ARP для MAC-адреса мобильного узла в чужой сети. Он может получить этот адрес, копируя информацию из сообщения Agent Solicitation или Registration Request переданного мобильным узлом.
- Указано, что запись в кэше ARP внешнего агента для IP-адреса мобильного узла **недопустимо** считать устаревшей, пока у внешнего агента нет какого-либо способа обновить связанный с IP-адресом мобильного узла MAC-адрес без использования широковещания ARP.
- В конце параграфа 4.6 разъяснено, что домашнему агенту **недопустимо** как-то изменять способ выполнения им proxy ARP после того, как он отверг неприемлемый запрос на отмену регистрации.
- В параграфе 4.2.3 указано, что многодомные домашние агенты **должны** использовать адрес, переданный мобильному узлу в поле Home Agent регистрационного отклика, должен использоваться в качестве адреса отправителя во внешнем заголовке IP инкапсулированных дейтаграмм.
- Добавлен бит T в соответствующую позицию сообщений Registration Request (параграф 3.3).

G.2. Второстепенные изменения

- Мобильным узлам разрешена обработка регистрационных откликов даже при отсутствии расширения Mobile-Home Authentication, если в отклике содержится код отказа от внешнего агента.
- Указано, что внешний агент **может** задавать максимальное число ожидающих регистраций, которые он готов поддерживать (обычно 5). В этом случае агенту **следует** отвергать избыточные регистрации с возвратом кода 66. Внешний агент **может** удалять любые ожидающие сообщения Registration Request, ожидающие регистрации более 7 секунд; в этом случае агенту **следует** возвращать код 78 (тайм-аут при регистрации).
- Ослаблено требование, по котором мобильный узел **должен** был использовать свой домашний адрес в поле отправителя в заголовке IP для групповых пакетов при участии мобильного узла в multicast-группе на маршрутизаторе чужой сети.
- Отмечено, что агент мобильности **может** использовать разные наборы битов R, H и F для разных сетевых интерфейсов.
- Термин «рекурсивное туннелирование» заменён термином «вложенное туннелирование».
- Указано, что мобильный узел **может** использовать адрес отправителя из анонса агента в качестве маршрута по умолчанию.
- Отмечено, что ключи с произвольными двоичными значениями **должны** поддерживаться для защищённых связей.
- Указано, что в качестве значения по умолчанию можно выбирать 7 секунд для того, чтобы скомпенсировать рассогласование часов домашнего агента и мобильного узла при использовании временных меток для защиты

от повторного использования. Дополнительно указано, что для этого параметра **следует** выбирать значение более 3 секунд.

- Указано, что сообщения Registration Request с битом D=0, задающие адрес обслуживания, который не предлагается внешним агентом, должны отвергаться с возвратом кода 77 (неприемлемый адрес обслуживания).
- Отмечено, что внешним агентам **следует** принимать во внимание своё максимальное значение при обработке полей Lifetime в сообщениях Registration Reply.
- Отмечено, что домашний агент **должен** игнорировать бит B (а не отвергать сообщение Registration Request), если он не поддерживает широковещания.
- Выяснение (не)возможности использования динамического обнаружения домашнего агента в случаях, когда маршрутизаторы меняют IP-адрес получателя дейтаграмм с широковещания в масштабе подсети (subnet-directed broadcast) на 255.255.255.255 до передачи дейтаграммы в подсеть получателя.
- Разъяснено, что сообщение Agent Advertisement адресовано индивидуально мобильному узлу, конкретный домашний IP-адрес мобильного узла **может** использоваться в качестве IP-адреса получателя.
- Включена ссылка на RFC 2290 с Приложением B, где рассмотрена работа с PPP.
- Добавлен раздел согласование с IANA (IANA Considerations).
- В параграфе 3.8.3 пояснено, что домашнему агенту **следует** организовать выбор домашнего адреса для мобильного узла в тех случаях, когда сообщение Registration Reply содержит нулевое значение Home Address.

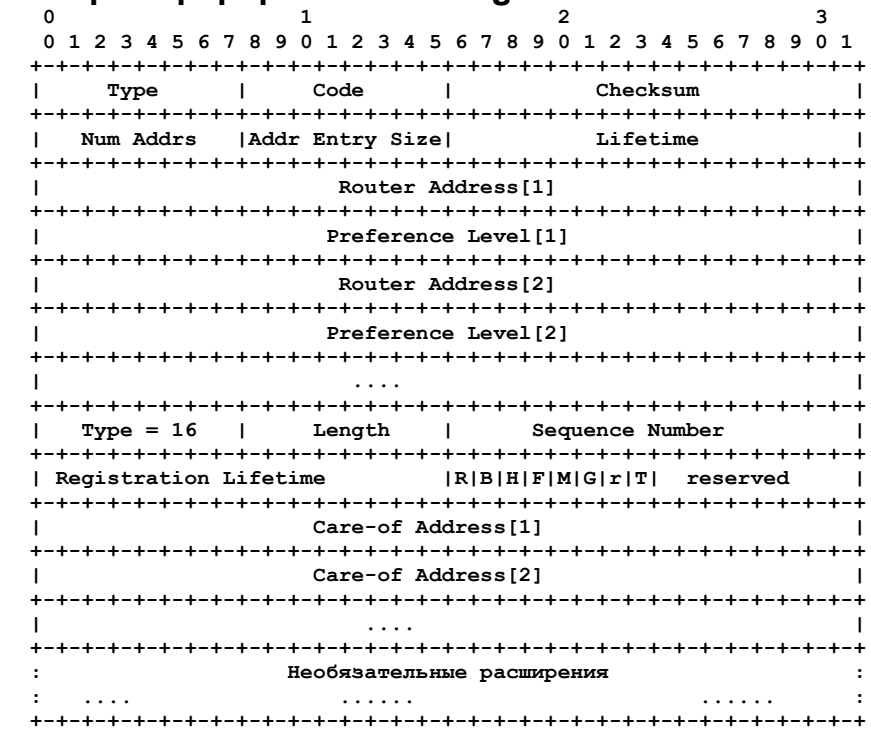
G.3. Отличия от варианта 04 RFC2002bis

В этом параграфе перечислены отличия данной версии (...-06.txt) этого документа от предыдущей (...-04.txt). Параграф может быть удалён редактором RFC.

- отмечено, что следует рассмотреть использование HMAC-MD5 взамен режима «prefix+suffix» MD5, изначально заявленного в RFC 2002;
- включена ссылка на RFC 2290 с Приложением B, где рассмотрена работа с PPP;
- переписан раздел Согласование с IANA;
- переписан раздел Обновления;
- раздел Патенты (Patents) заменён в соответствии с RFC 2026;
- обновлены цитаты.

H. Примеры сообщений

H.1. Пример формата ICMP Agent Advertisement

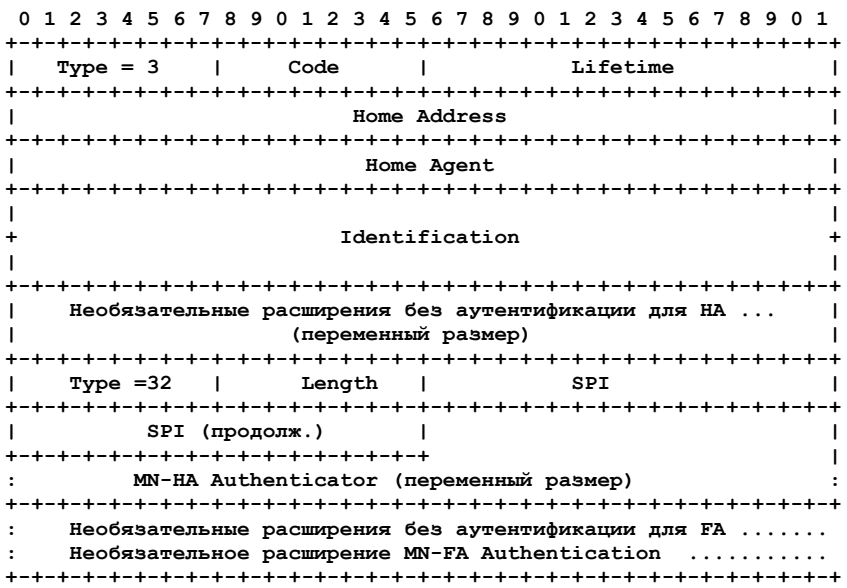


H.2. Пример формата Registration Request

После заголовка UDP следуют поля Mobile IP, как показано ниже.

H.3. Пример формата сообщения Registration Reply

После заголовка UDP следуют поля Mobile IP, как показано ниже.



Литература

[1] Allman, M., Glover, D. and L. Sanchez, "Enhancing TCP Over Satellite Channels using Standard Mechanisms", BCP 28, RFC 2488, January 1999.

[2] S. M. Bellovin. Security Problems in the TCP/IP Protocol Suite. ACM Computer Communications Review, 19(2), March 1989.

[3] Border, J., Kojo, M., Griner, J., Montenegro, G. and Z. Shelby, "Performance Enhancing Proxies", RFC 3135, June 2001.

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

[5] Ramon Caceres and Liviu Iftode. Improving the Performance of Reliable Transport Protocols in Mobile Computing Environments. IEEE Journal on Selected Areas in Communications, 13(5):850--857, June 1995.

[6] Calhoun P. and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, January 2000.

[7] Calhoun, P. and C. Perkins, "Mobile IP Foreign Agent Challenge/Response Extension", RFC 3012, December 2000.

[8] Cong, D., Hamlen, M. and C. Perkins, "The Definitions of Managed Objects for IP Mobility Support using SMIv2", RFC 2006, October 1996.

[9] Dawkins, S., Montenegro, G., Kojo, M., Magret, V. and N. Vaidya, "End-to-end Performance Implications of Links with Errors", BCP 50, RFC 3155, August 2001.

[10] Deering, S., "ICMP Router Discovery Messages", RFC 1256, September 1991.

[11] Deering, S., "Host Extensions for IP Multicasting", STD 5, RFC 1112, August 1989.

[12] Dommety, G. and K. Leung, "Mobile IP Vendor/Organization-Specific Extensions", RFC 3115, April 2001.

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

[14] Eastlake, D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[15] 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.

[16] Hanks, S., Li, T., Farinacci, D. and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994.

[17] J. Ioannidis. Protocols for Mobile Internetworking. PhD Dissertation - Columbia University in the City of New York, July 1993.

[18] John Ioannidis, Dan Duchamp, and Gerald Q. Maguire Jr. IP-Based Protocols for Mobile Internetworking. In Proceedings of the SIGCOMM '91 Conference: Communications Architectures & Protocols, pages 235--245, September 1991.

[19] John Ioannidis and Gerald Q. Maguire Jr. The Design and Implementation of a Mobile Internetworking Architecture. In Proceedings of the Winter USENIX Technical Conference, pages 489--500, January 1993.

[20] Jacobson, V., "Compressing TCP/IP headers for low-speed serial links", RFC 1144, February 1990.

[21] Jacobson, V., "Congestion Avoidance and Control. In Proceedings, SIGCOMM '88 Workshop, pages 314--329. ACM Press, August 1988. Stanford, CA.

[22] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

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

[24] McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB", RFC 2863, June 2000.

[25] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", RFC 1332, May 1992.

[26] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

[27] Montenegro, G., "Reverse Tunneling for Mobile IP (revised)", RFC 3024, January 2001.

[28] Montenegro, G., Dawkins, S., Kojo, M., Magret, V. and N. Vaidya, "Long Thin Networks", RFC 2757, January 2000.

[29] Montenegro, G. and V. Gupta, "Sun's SKIP Firewall Traversal for Mobile IP", RFC 2356, June 1998.

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

[31] Paxson, V. and M. Allman, "Computing TCP's Retransmission Timer", RFC 2988, November 2000.

[32] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[33] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

[34] Perkins, C., "Minimal Encapsulation within IP", RFC 2004, October 1996.

[35] Perkins, C. and P. Calhoun, "AAA Registration Keys for Mobile IP", Work in Progress[1], July 2001.

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

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

[38] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[39] Postel, J., "Multi-LAN Address Resolution", RFC 925, October 1984.

[40] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994.

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

[42] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[43] Solomon, J., "Applicability Statement for IP Mobility Support" RFC 2005, October 1996.

[44] Solomon J. and S. Glass, "Mobile-IPv4 Configuration Option for PPP IPCP", RFC 2290, February 1998.

[45] Stevens, W., "TCP/IP Illustrated, Volume 1: The Protocols" Addison-Wesley, Reading, Massachusetts, 1994.

Адреса авторов

Контактные данные рабочей группы приведены ниже.

Basavaraj Patil

Nokia

6000 Connection Dr.

Irving, TX. 75039

USA

Phone: +1 972-894-6709

EMail: Basavaraj.Patil@nokia.com

Phil Roberts

Megisto Corp. Suite 120

[1]Работа опубликована в RFC 3957. *Прим. перев.*

20251 Century Blvd

Germantown MD 20874

USA

Phone: +1 847-202-9314

EMail: PRoberts@MEGISTO.com

Вопросы, связанные с этим документом, можно направлять редактору, указанному ниже.

Charles E. Perkins

Communications Systems Lab

Nokia Research Center

313 Fairchild Drive

Mountain View, California 94043

USA

Phone: +1-650 625-2986

EMail: charliep@iprg.nokia.com

Fax: +1 650 625-2502

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.