Internet Engineering Task Force (IETF)
Request for Comments: 5944
Obsoletes: 3344
Category: Standards Track
ISSN: 2070-1721

C. Perkins, Ed.
WiChorus Inc.
November 2010

Пересмотренная поддержка IP Mobility для IPv4

IP Mobility Support for IPv4, Revised

Аннотация

В этом документе содержится спецификация расширения протокола, обеспечивающего прозрачную маршрутизацию дейтаграмм IP для мобильных узлов в сети Internet. Каждый мобильный узел всегда идентифицируется своим домашним адресом, независимо от текущей точки подключения к сети Internet. С мобильным узлом, находящимся за пределами домашней сети, связывается адрес обслуживания, обеспечивающий информацию о текущей точке подключения к сети Internet. Протокол обеспечивает регистрацию адреса обслуживания на домашнем агенте. Домашний агент передаёт дейтаграммы для мобильного узла через туннель на адрес обслуживания. После прибытия дейтаграммы на этот конец туннеля дейтаграмма доставляется мобильному узлу.

Статус документа

Этот документ содержит проект стандарта Internet (Internet Standards Track).

Документ является результатом работы IETF[1] и представляет собой согласованное мнение членов (сообщества) IETF. Документ был представлен для публичного обсуждения и одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 документа RFC 5741.

Информацию о текущем состоянии этого документа, обнаруженных ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc5944.

Оглавление

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

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. [44], [14], [15], [20], [4], [50]) подробно рассмотрены в Приложении F.

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 с целью 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 [1].

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 [2]).

Agent Advertisement - анонсирование агента
Сообщение-анонс, созданное путем присоединения к маршрутным анонсам специального расширения [5].

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 (совмещенный 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 (MSA)
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 MSA. 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] (совмещенный 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. Совмещенный 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.

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 совмещенный адрес обслуживания (см. п. b выше), он **должен** размещаться в сети, указанной префиксом этого адреса. Иначе дейтаграммы, переданные по адресу обслуживания, не будут доставлены.

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 совмещенный адрес.

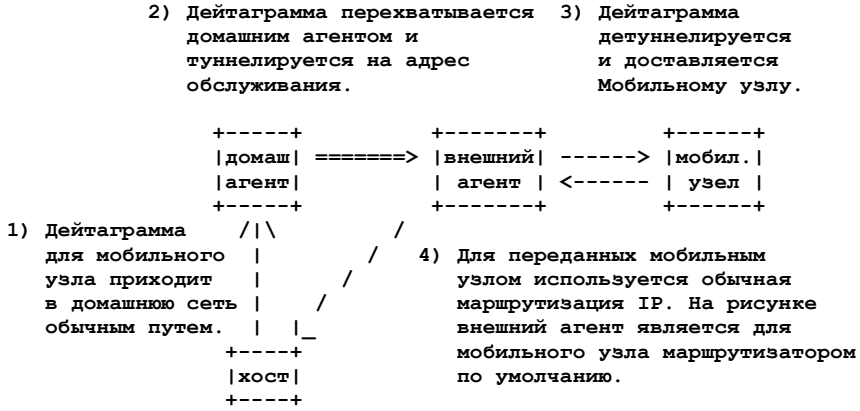


Рисунок 1. Работа Mobile IPv4.

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 базе данных IANA [48].

Кроме того для обнаружения агентов (Agent Discovery) Mobile IP использует сообщения Router Advertisement и Router Solicitation, определённые для ICMP Router Discovery [5].

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[1], 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.

[1]Type-Length-Value - тип-размер-значение.

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

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

  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 [5]. Данный документ определяет три типа таки расширений:

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

  16 Mobility Agent Advertisement (анонс мобильного агента);

  19 Prefix-Lengths (размеры префиксов).

Расширения будут подробно описаны ниже. Актуальные значения Extension Type можно найти в базе данных IANA [48].

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) однозначно 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 с типом от 128 до 255, это расширение игнорируется, но остальные расширения и данные сообщения **должны** обрабатываться. Поле Length в Extension служит 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 [46]). 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.

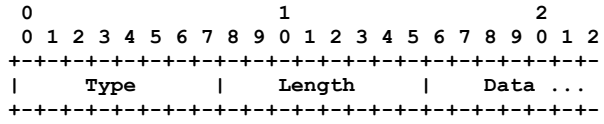


Рисунок 2. Формат TLV для расширений Mobile IPv4

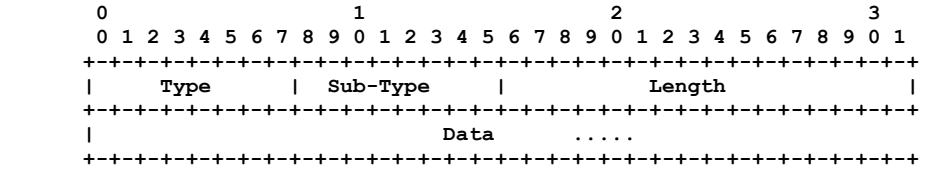
Type
Указывает конкретный тип расширения.

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. Пропускаемые расширения не могут использовать длинный формат, поскольку получатель не обязан поддерживать код для разбора и будет, очевидно, трактовать 8 битов, следующих непосредственно за полем Type, как поле Length.



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.

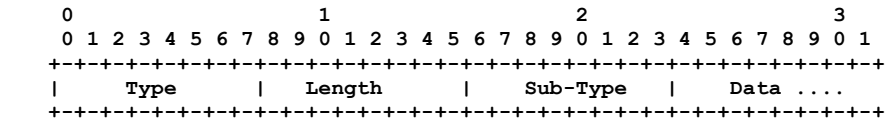
Length
Размер поля данных расширения в байтах. 4 октета полей Type, Length и Sub-Type в размере **не** учитываются.

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 [5] для использования в целях обнаружения агента. Сообщения Agent Advertisement формируются путем 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 A). 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 [9], 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) [6] 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.

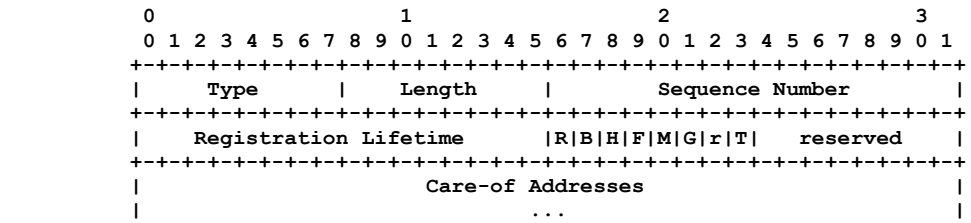
Num Addrs

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 [5] 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 [15].

G
Инкапсуляция GRE. Агент принимает туннелированные дейтаграммы с инкапсуляцией GRE [13].

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

T
Внешний агент поддерживает обратное туннелирование [12].

Агент мобильности поддерживает туннелирование UDP в соответствии с [27].

X

Агент мобильности поддерживает отзыв регистрации в соответствии с [28].

I

Внешний агент поддерживает региональную регистрацию в соответствии с [29].

reserved

0 при передаче, игнорируется на приёмной стороне.

Care-of Address(es)

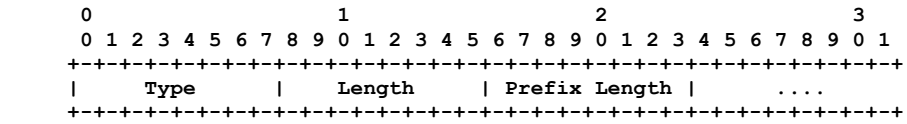
Анонсированный адрес (адреса) внешнего агента, обеспечиваемый этим агентом. Сообщение Agent Advertisement **должно** включать хотя бы один адрес обслуживания, если установлен бит F. Число представленных адресов обслуживания определяется значением поля Length в расширении.

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

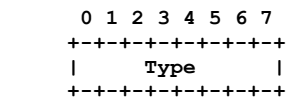
Число старших битов, определяющих номер сети для соответствующего Router Address в ICMP Router Advertisement данного сообщения. Размер префикса для каждого Router Address представляется отдельным байтом в порядке следования полей Router Addresses в ICMP Router Advertisement.

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 D.

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 [5], 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 Advertisements только 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 Addresses, внешний агент **должен** маршрутизировать дейтаграммы, полученные от зарегистрированных мобильных узлов (параграф 3.7).

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 [5], 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 [5].

Мобильные узлы **должны** обрабатывать полученные анонсы агентов. 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 нужно для указанного числа анонсируемых адресов, остальные данные интерпретируются как одно или несколько расширений. Наличие расширения Mobility Agent Advertisement 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 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 [16], мобильный узел **должен** выполнить процедуры, описанные в параграфе 4.6 применительно к ARP, proxy ARP и gratuitous 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).

3. Регистрация

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 совмещенный 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] [17]. 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 MSA между сторонами.

3.2. Аутентификация

Каждый мобильный узел, домашний и внешний агент **должны** обеспечивать поддержку связей MSA 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.

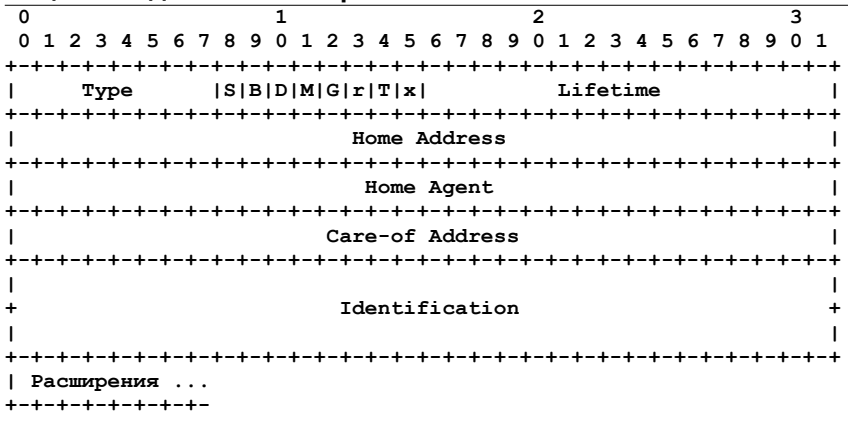
Поля UDP

Source Port - переменное.

Destination Port - 434.

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

[1] User Datagram Protocol - протокол пользовательских дейтаграмм.



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.

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 [16] 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 [13] 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. [12]).

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 запроса 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 3.8.3.2.

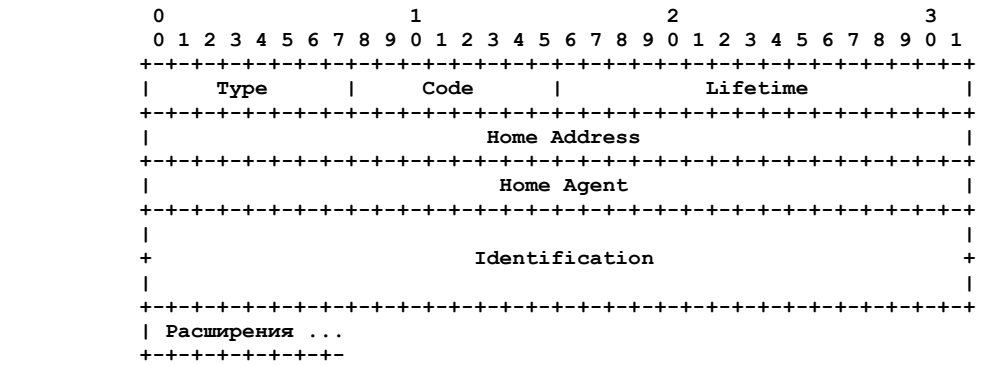
Destination Address - копируется из поля Source Address сообщения Registration Request, на которое агент отвечает.

Поля UDP

Source Port - копируется из поля UDP Destination Port соответствующего запроса.

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 Requests от мобильного узла и стилем защиты от повторного использования пакетов в контексте защиты между мобильным узлом и домашним агентом (определяется MSA 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);

194 недопустимый адрес домашнего агента.

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 указываются в базе данных IANA [48].

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 [10] для расчёта 128-битовой цифровой подписи регистрационного сообщения. При расчёте HMAC учитываются следующие данные:

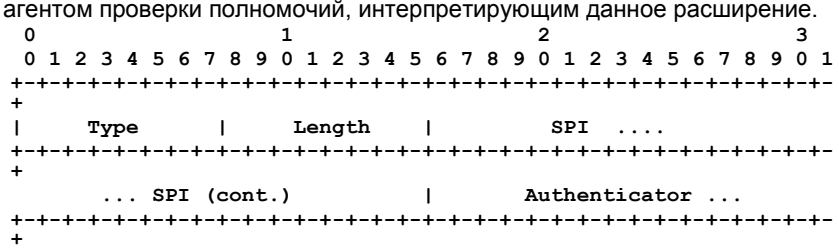
- данные UDP (т. е., данные Registration Request или Registration Reply);
- все предшествующие расширения целиком;
- поля Type, Length и SPI данного расширения.

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 взаимодействия 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 хотя бы 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 [30], возникающих в результате неконтролируемого распространения удалённых перенаправлений в Internet. Местоположение разрешающего аутентификацию расширения указывает окончание данных, которые будут аутентифицироваться агентом проверки полномочий, интерпретирующим данное расширение.



Type

32

[1]Security Parameter Index.

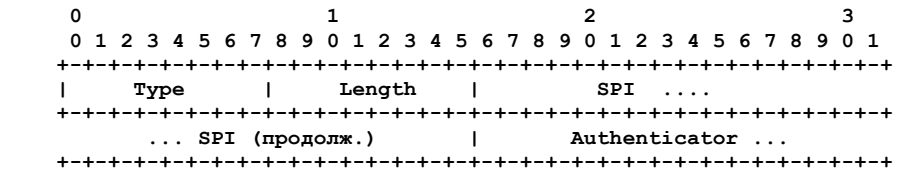
Length
4 + число байтов в поле Authenticator.

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 MSA. Требования поддержки для кодов аутентификации сообщений описаны в параграфе 5.1.



Type
33

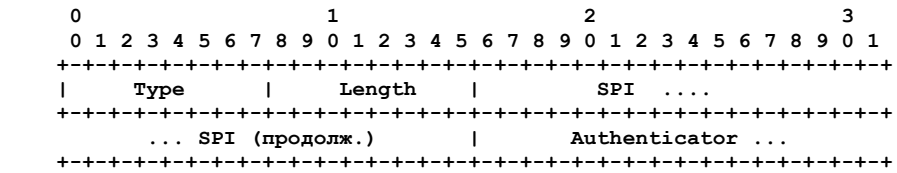
Length
4 + число байтов в поле Authenticator.

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

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

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 MSA. 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.)

Для выполнения аутентификации домашний агент и внешний агент используют организуют защищённую связь MSA, указываемую SPI (в расширении Foreign-Home Authentication) и полем IP Source Address в Registration Request. Если расширение используется в сообщении Registration Reply, в качестве адреса получателя в заголовке IP **должен** использоваться адрес внешнего агента.

При использовании данного расширения в сообщениях Registration Request защищённая связь MSA для проверки корректности аутентификационных данных выбирается домашним агентом на основе значения поля Source IP Address в сообщении Registration Request и SPI в аутентификационном расширении. Значение Source IP Address будет совпадать с Care-of Address в сообщении Registration Request (см. параграф 3.7.2.2).

При использовании этого расширения в сообщениях Registration Reply защищённая связь MSA для проверки корректности аутентификационных данных выбирается внешним агентом по адресу домашнего агента в сообщении Registration Reply.

Если адреса Care-of Address из сообщения Registration Request не было в сообщении Agent Advertisement, внешнему агенту **недопустимо** добавлять расширение Foreign-Home Authentication при трансляции сообщения домашнему агенту. Более того, для сообщение об отмене регистрации (Lifetime = 0) внешнему агенту **недопустимо** добавлять расширение Foreign-Home Authentication при трансляции сообщения этому домашнему агенту. Следовательно, при получении домашним агентом (HA) запроса на отмену регистрации без расширения Foreign-Home Authentication **недопустимо** отбрасывать запрос на основании лишь отсутствия такого расширения.

3.6. Мобильные узлы

На мобильном узле **должна** быть (статически или динамически) задана маска сети и MSA 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) [2] 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 C 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 такое 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 [18].

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 (совмещенный). 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 совмещенный 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 рассмотрен ниже.

- Если мобильный узел регистрируется на внешнем агенте, значение поля Lifetime **не следует** устанавливать больше значения Registration Lifetime в полученном от данного агента сообщении Agent Advertisement. Когда метод определения адреса обслуживания не включает Lifetime, **может** использоваться принятое по умолчанию значение ICMP Router Advertisement Lifetime (1800 сек.).

- Мобильный узел **может** запросить у домашнего агента удаление конкретной мобильной привязки, передав сообщение Registration Request с адресом обслуживания этой привязки и Lifetime = 0 (параграф 3.8.2).

- Отмена регистрации всех адресов обслуживания с Lifetime = 0 указывает на возврат мобильного узла домой.

В поле Home Address **должен** быть указан домашний адрес мобильного узла, если он известен. В противном случае **должен** указываться адрес 0.0.0.0.

В поле Home Agent **должен** указываться адрес домашнего агента мобильного узла, если он известен мобильному узлу. В противном случае мобильный узел **может** использовать динамическое преобразование адресов для определения адреса своего домашнего агента. Для этого мобильный узел **должен** указать в поле Home Agent широковещательный адрес своей домашней подсети. Каждый домашний агент, получивший сообщение Registration Request с таким широковещательным адресом в поле Destination Address **должен** отвергнуть регистрацию мобильного узла и ему **следует** также передать сообщение Registration Reply, указывающее его индивидуальный адрес IP для использования мобильным узлом при следующей попытке регистрации.

Поле Care-of Address **должно** содержать конкретный адрес обслуживания, который мобильный узел хочет зарегистрировать (или отменить его регистрацию). Если мобильный узел хочет отменить регистрацию всех своих адресов обслуживания, он **должен** указать в этом поле свой домашний адрес.

Мобильный узел выбирает значение поля Identification в соответствии с используемой защитой от повторов. Это является частью защищённой связи MSA между мобильным узлом и домашним агентом. Описание методов расчёта значений поля Identification приведено в параграфе 5.7.

3.6.1.3. Расширения

В этом параграфе описан порядок следования обязательных и необязательных расширений, которые мобильный узел добавляет в конце сообщений Registration Request. **Требуется** соблюдать указанный здесь порядок.

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) все разрешающие аутентификацию расширения (см. параграф 1.6), после которых

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 MSA.

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 MSA, 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, gratuitous 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 совмещенный 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 запросе используется расширение NAI (например, при нулевом значении Home Address), внешний агент **должен** следовать процедурам, описанным в RFC 2794 [2]. 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. [2]).

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 MSA с другими узлами. При трансляции сообщений Registration Request от мобильного узла его домашнему агенту, если у внешнего агента имеется MSA 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 MSA 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 194 (недопустимый 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 MSA, 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:

- **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;
- если внешний агент имеет защищённую связь MSA с домашним агентом и значение Lifetime в запросе отлично от 0, внешний агент **должен** добавить в конце расширение Foreign-Home Authentication.

Приведённые ниже поля заголовков IP и UDP транслируемого сообщения Registration Request **должны** быть изменены.

IP Source Address
Адрес обслуживания, предложенный внешним агентом для мобильного узла, передавшего Registration Request.

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 MSA, 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 отклик содержит 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 конец расширение Mobile-Foreign Authentication, если имеется защищённая связь MSA 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 MSA 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 [2]. 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 MSA с разными внешними агентами. При получении сообщения Registration Request от внешнего агента, с которым имеется защищённая связь MSA, домашний агент **должен** проверить значение Authenticator в обязательном расширении Foreign-Home Authentication данного сообщения, основываясь на своей MSA, если значение поля Lifetime отлично от 0. При обработке регистрационного запроса с Lifetime = 0, домашний **может** пропустить проверку наличия и корректности расширения Foreign-Home Authentication. Аналогично, при передаче сообщения Registration Reply внешнему агенту, с которым домашний агент имеет защищённую связь MSA, домашний агент **должен** включить в сообщение расширение Foreign-Home Authentication на основе MSA.

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 хотя бы одного разрешающего аутентификацию расширения и убедиться, что все указанные аутентификационные действия выполнены. В сообщении Registration Request **должно** присутствовать по крайней мере одно разрешающее аутентификацию расширение и домашний агент **должен** проверить значение Authenticator в этом расширении или убедиться в том, что это значение проверено другим агентом, с которым имеется защищённая связь.

   Если домашний агент получает сообщение Registration Request от мобильного узла, с которым у него нет защищённой связи, домашний агент **должен** отбросить регистрационный запрос без уведомления.

   Если домашний агент получает сообщение Registration Request без разрешающего аутентификацию расширения, он **должен** отбросить такой запрос без уведомления.

   Если значение Authenticator не приемлемо, домашний агент **должен** отвергнуть регистрацию мобильного узла. Дальнейшие действия зависят от наличия в запросе приемлемого расширения Foreign-Home (см. ниже):

   - При наличии подходящего расширения Foreign-Home домашний агент **должен** отправить сообщение Registration Reply с кодом 131.

   - В остальных случаях, если нет защищённой связи между домашним и внешним агентом (Foreign-Home Security Association), домашний агент **может** передать сообщение Registration Reply с кодом 131. Если домашний агент передаёт Registration Reply, это сообщение **должно** включать расширение Mobile-Home Authentication. При создании отклика домашнему агенту **следует** выбрать защищённую связь, которая может быть организована с мобильным узлом. Например, это может быть старая защищённая связь или связь, время жизни которой превышает время жизни той связи, которой пытался воспользоваться при запросе мобильный узел. Следует соблюдать осторожность при обновлении защищённых связей, чтобы обеспечить постоянное наличие по крайней мере одной действующей связи между мобильным узлом и домашним агентом. В случае отказа при проверке значения Authenticator, домашний агент **должен** отбросить запрос без дополнительной обработки, **следует** также сделать в системном журнале запись о нарушении безопасности.

b. Домашний агент **должен** проверять корректность поля Identification с использованием контекста, выбранного SPI в разрешающем аутентификацию расширении, которое домашний агент применяет для аутентификации сообщения Registration Request от мобильного узла. 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 MSA с внешним агентом и в сообщении Registration Request поле Lifetime отлично от 0, 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.

d. Если между домашним и внешним агентом нет защищённой связи MSA, а регистрационное сообщение включает расширение Foreign-Home Authentication, домашний агент **должен** отбросить запрет, 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 путем 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 применимого 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 записи с таким же адресом сохраняются неизменными.

- 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 MSA 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 MSA с внешним агентом. Если отклик не передаётся, срок действия записи в списке посетителей внешнего агента завершается естественным путем по истечении времени Lifetime.

Когда внешний агент транслирует запрос дерегистрации, содержащий адрес обслуживания, не принадлежащий данному агенту, **недопустимо** добавлять расширение Foreign-Home Authentication в этот запрос (см. параграф 3.5.4).

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 [16] 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 gratuitous 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 специфические правила, по которым домашний агент устанавливает значения полей в заголовках IP и UDP сообщений 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 путем 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 Registration Reply выбирается в соответствии с правилами предыдущих параграфов. При ответе на воспринятую регистрацию домашнему агенту **следует** отвечать с Code = 1, если он не поддерживает одновременных регистраций.

Поле Lifetime **должно** копироваться из соответствующего поля в Registration Request, если запрошенное значение не превышает максимальное время, в течение которого домашний агент согласен предоставлять обслуживание. В последнем случае для поля Lifetime **должно** устанавливаться значение времени, в течение которого домашний агент действительно будет осуществлять обслуживание. В качестве такого уменьшенного значения Lifetime **следует** использовать максимальное значение Lifetime, дозволенное домашним агентом (для данного мобильного узла и адреса обслуживания).

Если поле Home Address в регистрационном запросе (Registration Request) отлично от 0, это поле **должно** копироваться в поле Home Address сообщения Registration Reply. Если домашний агент не может поддерживать указанный ненулевой индивидуальный (unicast) адрес, указанный в поле Home Address сообщения Registration Request, он должен отвергнуть запрос регистрации с возвратом Code = 129.

Если же поле Home Address в сообщении Registration Request имеет значение 0, как указано в параграфе 3.6, домашнему агенту **следует** выбрать домашний адрес для мобильного узла и поместить этот адрес в поле Home Address сообщения Registration Reply. В документе [2] приведены дополнительные подробности для случая, когда мобильный узел представляет себя с помощью NAI вместо своего домашнего адреса IP.

Если поле Home Agent в сообщении Registration Request содержит индивидуальный адрес этого домашнего агента, значение поля **должно** копироваться в поле Home Agent сообщения Registration Reply. В остальных случаях домашний агент **должен** указать в поле Home Agent сообщения Registration Reply свой индивидуальный адрес. При этом домашний агент **должен** отвергнуть регистрацию с использованием подходящего кода (например, Code = 136) для предотвращения одновременной регистрации мобильного узла на нескольких домашних агентах.

3.8.3.3. Расширения

В этом параграфе описан порядок всех обязательных и опциональных расширений Mobile IP, которые домашний агент добавляет в конце сообщений Registration Reply. **Должен** соблюдаться приведённый далее порядок.

a. Заголовок IP, за ним заголовок UDP, а затем фиксированная по размеру часть Registration Reply.

b. Все имеющиеся (если они есть) расширения, не относящиеся к проверке подлинности, которые использует мобильный узел (они могут использоваться и внешним агентом).

c. Расширение Mobile-Home Authentication.

d. Все имеющиеся (если они есть) расширения, не относящиеся к проверке подлинности, которые использует только внешний агент.

e. Расширение Foreign-Home Authentication при его наличии.

Отметим, что элементы (a) и (c) **должны** присутствовать в каждом сообщении Registration Reply, передаваемом домашним агентом. Элементы (b), (d) и (e) являются не обязательными. Однако элемент (e) **должен** включаться в тех случаях, когда внешний и домашний агенты связаны через общую MSA.

4. Вопросы маршрутизации

В этом разделе описано взаимодействие мобильных узлов, домашних агентов и (возможно) внешних агентов при маршрутизации дейтаграмм мобильного узла, подключённого к чужой сети. Мобильный узел информирует домашнего агента о своём текущем местоположении, используя процедуру регистрации, описанную в разделе 3. В обзоре протокола (параграф 1.7) описаны местоположения домашних адресов мобильных узлов относительно домашних агентов и самих мобильных узлов относительно внешних агентов, но которых мобильные узлы пытаются зарегистрироваться.

4.1. Типы инкапсуляции

Домашние и внешние агенты **должны** поддерживать туннелирование дейтаграмм с использованием инкапсуляции IP в IP [14]. Любой мобильный узел, использующий совмещенный адрес обслуживания (co-located care-of address), **должен** поддерживать приём дейтаграмм, туннелированных с использованием инкапсуляции IP в IP. Минимальная инкапсуляция [15] и инкапсуляция GRE [13] являются дополнительными методами и **могут** опционально поддерживаться мобильными узлами. Использование дополнительных форм инкапсуляции происходит по запросам мобильных узлов на усмотрение домашнего агента.

4.2. Маршрутизация индивидуальных дейтаграмм

4.2.1. Мобильный узел

При подключении к своей домашней сети мобильный узел работает без поддержки услуг мобильности. Т. е. он работает так же, как любой другой (стационарный) хост или маршрутизатор. Метод выбора мобильным узлом

используемого по умолчанию маршрутизатора при подключении к своей домашней сети или выходе из неё с использованием совмещённого адреса обслуживания выходит за рамки данного документа. Одним из таких методов является ICMP Router Advertisement [5].

При регистрации в чужой сети мобильный узел выбирает используемый по умолчанию маршрутизатор в соответствии с приведёнными ниже правилами.

- Если мобильный узел зарегистрирован с использованием адреса внешнего агента (foreign agent care-of address), он **может** указать этот агент в качестве первого интервала маршрутизации (first-hop router). MAC-адрес внешнего агента может быть определён из сообщения Agent Advertisement от этого агента. В остальных случаях мобильный узел **должен** выбрать маршрут по умолчанию из числа адресов, анонсируемых в части ICMP Router Advertisement portion сообщения Agent Advertisement message.

- Если мобильный узел регистрируется напрямую со своим домашним агентом, используя совмещенный адрес обслуживания (co-located care-of address), ему **следует** выбрать маршрут по умолчанию из числа анонсируемых в любых принятых сообщениях ICMP Router Advertisement, для которых полученный извне адрес обслуживания и адрес маршрутизатора совпадают по префиксу. Если полученный мобильным узлом извне адрес обслуживания соответствует по префиксу IP-адресу отправителя Agent Advertisement, мобильный узел **может** рассмотреть этот адрес в качестве возможного маршрута по умолчанию. Сетевой префикс **может** быть получен из Prefix-Lengths Extension в Router Advertisement (при наличии). Префикс **можно** также определить с помощью других механизмов, не рассмотренных в этом документе.

Когда мобильный узел находится за пределами своей домашней сети, ему **недопустимо** передавать в широковещательному режиме пакеты ARP для определения MAC-адреса другого узла Internet. Таким образом, список (возможно, пустой) адресов маршрутизаторов из компоненты ICMP Router Advertisement сообщения не поможет при выборе используемого по умолчанию маршрутизатора, пока у мобильного узла нет какого-либо способа определения MAC-адресов маршрутизаторов из этого списка без использования широковещательных пакетов ARP, не заданного в этом документе. Аналогично, при отсутствии не заданных в спецификации механизмов получения MAC-адресов в чужой сети мобильный узел **должен** игнорировать перенаправление на другие маршрутизаторы чужой сети.

4.2.2. Внешний агент

При получении инкапсулированной дейтаграммы, переданной по анонсированному адресу обслуживания, внешний агент **должен** сравнить внутренний адрес получателя со своими записями списка посетителей. Если этот адрес не соответствует ни одному из присутствующих в списке мобильных узлов, внешнему агенту **недопустимо** пересылать дейтаграмму без изменения исходного заголовка IP, поскольку в противном случае с высокой вероятностью возникнет петля в маршрутизации. Дейтаграмму **следует** отбросить без уведомления. Сообщения ICMP Destination Unreachable **недопустимо** передавать, если внешний агент не способен переслать входящую туннелированную дейтаграмму. В остальных случаях внешний агент пересылает инкапсулированную дейтаграмму мобильному узлу.

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

Внешний агент **должен** маршрутизировать дейтаграммы, принятые от зарегистрированных мобильных узлов. Это означает, по меньшей мере, что внешний агент должен проверять контрольную сумму заголовка IP, декрементировать IP TTL, пересчитывать контрольную сумму заголовка IP и пересылать дейтаграмму заданному по умолчанию маршрутизатору.

Внешнему агенту **недопустимо** использовать широковещание ARP для MAC-адреса мобильного узла в чужой сети. Он может определить MAC-адрес путем копирования данных из сообщения Agent Solicitation или Registration Request, переданного мобильным узлом. Записи в кэше ARP внешнего агента для IP-адреса мобильного узла **недопустимо** устаревать да окончания срока действия записи мобильного узла в списке посетителей, если у внешнего агента нет отличного от широковещания ARP способа обновления MAC-адреса, связанного с адресом IP мобильного узла.

Каждому внешнему агенту **следует** поддерживать обязательные функции обратного туннелирования [12].

4.2.3. Домашний агент

Домашний агент **должен** быть способен перехватывать любые дейтаграммы в домашней сети, адресованные мобильному узлу, когда этот узел зарегистрирован в чужой сети. **Можно** применять Proxy ARP и Gratuitous ARP для обеспечения такого перехвата, как описано в параграфе 4.6.

Домашний агент должен проверять IP-адрес получателя во всех принимаемых дейтаграммах на предмет совпадения с домашним адресом какого-либо из мобильных узлов, подключённых к чужим сетям. При обнаружении такой дейтаграммы домашний агент туннелирует её мобильному узлу, зарегистрированному по адресу (адресам) обслуживания. Если домашний агент поддерживает необязательную функцию множества одновременных мобильных привязок, он туннелирует копию дейтаграммы по каждому адресу обслуживания в списке привязок мобильного узла. Если мобильный узел не имеет действующих привязок, домашнему агенту **недопустимо** пытаться перехватывать адресованные этому узлу дейтаграммы, поэтому в общем случае агент просто 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 находится в домашней сети и просто пересылать дейтаграммы напрямую в эту сеть.

Для многодомных домашних агентов адресом отправителя во внешнем заголовке IP **должен** быть адрес, переданный мобильному узлу в поле Home Agent сообщения Registration Reply. Т. е. домашний агент не может использовать в качестве адреса отправителя адрес того или иного сетевого интерфейса.

Методы инкапсуляции, которые могут применяться для туннелирования, описаны в параграфе 4.1. Узлам, реализующим туннелирование, **следует** также поддерживать механизм tunnel soft state [14], который позволяет возвращать сообщения ICMP об ошибках из туннеля для корректного указания исходных отправителей туннелированных дейтаграмм.

Домашние агенты **должны** декапсулировать адресованные им пакеты, отправленные мобильным узлом для поддержки приватности местоположения, как описано в параграфе 5.5. Это требуется также для поддержки реверсного туннелирования [12].

Если Lifetime для данной мобильной привязки завершается до того, как домашний агент получит другой действительный запрос Registration Request от мобильного узла, эта привязка удаляется из списка мобильных привязок. Домашнему агенту **недопустимо** отправлять какие-либо сообщения Registration Reply, поскольку срок действия мобильной привязки истёк. Запись в списке посетителей текущего внешнего агента этого мобильного узла будет устаревать естественным образом, вероятно в то же время, что и привязка у домашнего агента. Когда срок действия мобильной привязки завершается, домашний агент **должен** удалить эту привязку, но он **должен** сохранить все другие (не устаревшие) мобильные привязки, которые он имеет для данного мобильного узла.

Когда домашний агент получает дейтаграмму, перехваченную для одного из своих мобильных узлов, находящихся вне домашней сети, он **должен** проверить не является ли дейтаграмма уже инкапсулированной. При положительном ответе для пересылки такой дейтаграммы мобильному узлу используются перечисленные ниже правила.

- Если внутренний (инкапсулированный) адрес получателя совпадает в внешним Destination Address (мобильный узел), домашний агент **должен** также проверить внешний адрес отправителя инкапсулированной дейтаграммы (адрес источника для туннеля). Если этот адрес совпадает с текущим адресом обслуживания (care-of) мобильного узла, домашний агент **должен** отбросить дейтаграмму без уведомление для того, чтобы предотвратить возникновение маршрутной петли. Если же внешний адрес отправителя не совпадает с адресом care-of мобильного узла, домашнему агенту **следует** переслать дейтаграмму мобильному узлу. Для пересылки дейтаграммы с этом случае домашний агент **может** просто изменить адрес получателя на адрес обслуживания мобильного узла, не инкапсулируя дейтаграмму снова.
- В остальных случаях (внутренний адрес получателя **не** совпадает с внешним) домашнему агенту **следует** инкапсулировать дейтаграмму ещё раз (вложенная инкапсуляция) с установкой в поле Destination Address адреса обслуживания (care-of) мобильного узла. Затем домашний агент пересылает всю дейтаграмму мобильному узлу как это делается для всех прочих дейтаграмм (уже инкапсулированных или нет).

4.3. Широковещательные дейтаграммы

При получении домашним агентом широковещательной дейтаграммы **недопустимо** пересылать её каким-либо мобильным узлам из списка мобильных привязок, кроме тех узлов, которые запросили пересылку широковещательных дейтаграмм. Мобильный узел **может** запросить такую пересылку, установив флаг B в своём сообщении Registration Request (параграф 3.3). Для каждого такого узла домашнему агенту **следует** пересылать принятые широковещательные дейтаграммы, хотя это может решаться настройкой домашнего агента, в результате которой мобильным узлам будут пересылаться лишь заданные категории широковещательных дейтаграмм.

Если установлен бит D в сообщении Registration Request, указывающий использованием мобильным узлом совмещённого адреса обслуживания (co-located care-of), домашний агент просто туннелирует широковещательные дейтаграммы IP по адресу обслуживания мобильного узла. В остальных случаях (флаг D **не** установлен), домашний агент сначала инкапсулирует широковещательную дейтаграмму в индивидуальную на домашний адрес мобильного узла, а затем туннелирует инкапсулированную дейтаграмму внешнему агенту. Дополнительная инкапсуляция нужна для того, чтобы внешний агент мог определить, какому из мобильных узлов следует переслать дейтаграмму после её декапсуляции. При получении внешним агентом индивидуальной инкапсулированной дейтаграммы он извлекает её из туннеля и доставляет мобильному узлу так же, как остальные дейтаграммы. В любом случае мобильный узел должен декапсулировать полученную дейтаграмму для восстановления исходной широковещательной дейтаграммы.

4.4. Маршрутизация групповых дейтаграмм

Как было отмечено выше, мобильный узел в своей домашней сети работает так же, как любые другие (стационарные) хосты или маршрутизаторы. Т. е. дома мобильный узел функционирует аналогично другим отправителям и получателя группового (multicast) трафика. Поэтому в данном параграфе описывается поведение мобильного узла в чужой сети.

Для получения группового трафика мобильный узел **должен** присоединиться к multicast-группе одним из двух способов. Мобильный узел **может** подключиться к группе через (локальный) групповой маршрутизатор подсети, в которой он находится. Этот вариант предполагает наличие такого маршрутизатора в чужой сети. Если мобильный узел использует совмещенный адрес обслуживания, ему **следует** указывать этот адрес в качестве IP-адреса отправителя в своих сообщениях IGMP [6]. В остальных случаях мобильный узел **может** использовать свой домашний адрес.

Кроме того, желающий получать групповой трафик мобильный узел **может** присоединиться к группе через двухсторонний туннель к домашнему агенту, если этот агент является также групповым маршрутизатором. Мобильный узел туннелирует сообщения IGMP своему домашнему агенту, а тот пересылает групповые дейтаграммы по туннелю мобильному узлу. Для пакетов, туннелируемых домашнему агенту в качестве адреса отправителя в заголовке IP **следует** указывать домашний адрес мобильного узла.

Правила доставки групповых дейтаграмм мобильному узлу в этом случае идентичны правилам доставки широковещательных дейтаграмм (параграф 4.3). Если мобильный узел использует совмещенный адрес обслуживания (co-located care-of), т. е. был установлен бит 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 для домашнего адреса мобильного узла, а затем **должен** туннелировать полученную в результате дейтаграмму (вложенное туннелирование) по адресу обслуживания мобильного узла. Поэтому мобильный узел **должен** быть способен декапсулировать пакеты, переданные по его домашнему адресу, чтобы получать групповые дейтаграммы с использованием этого метода.

Мобильный узел, желающий отправлять дейтаграммы в multicast-группу, также имеет два варианта - (1) передавать напрямую в сеть, куда он в данный момент подключён, или (2) передавать домашнему агенту через туннель. Поскольку групповая маршрутизация в общем случае зависит от IP-адреса отправителя, в первом варианте мобильный узел **должен** использовать совмещенный адрес обслуживания (co-located care-of) в качестве IP-адреса отправителя. При туннелировании групповых дейтаграмм домашнему агенту мобильный узел **должен** использовать свой домашний адрес в качестве IP-адреса отправителя как для внутренней групповой дейтаграммы, так и для инкапсулирующей

(внешней) дейтаграммы. Во втором варианте предполагается, что домашний агент является multicast-маршрутизатором.

4.5. Мобильные маршрутизаторы

Мобильный узел может быть маршрутизатором, отвечающим за мобильность одной или множества сетей, перемещающихся вместе (например, на самолёте, корабле, поезде, автомобиле). Соединённые в сеть узлы, обслуживаемые маршрутизатором, могут быть стационарными или мобильными узлами и маршрутизаторами. В данном документе такие сети называются мобильными.

Мобильный маршрутизатор **может** служить внешним агентом и предоставлять адреса обслуживания для мобильных узлов, подключённых к мобильной сети. Ниже приведён пример типовой маршрутизации через мобильный маршрутизатор.

a. Переносной компьютер отключается от домашней сети, а затем подключается к сетевому порту в кресле самолёта. Компьютер использует Mobile IP для регистрации в чужой сети с использованием адреса обслуживания от внешнего агента, найденного через сообщения Agent Advertisement от внешнего агента на борту самолёта.

b. Бортовая сеть самолёта. сама является мобильной. Предположим, что узел, являющийся внешним агентом, к которому подключена бортовая сеть, служит также принятым по умолчанию маршрутизатором, соединяющим сеть самолёта. с Internet. Когда самолёт находится «дома», этом маршрутизатор подключается к некой стационарной сети авиакомпании, которая является домашней сетью этого маршрутизатора. Во время полёта бортовой маршрутизатор время от времени регистрируется по радиоканалу на внешних агентах, расположенных на земле вдоль трассы полёта. Домашним агентом этого маршрутизатора является узел стационарной сети в офисе авиакомпании.

c. Некий узел передаёт дейтаграмму переносному компьютеру, направляя её по домашнему адресу этого компьютера. Дейтаграмма сначала маршрутизируется в домашнюю сеть переносного компьютера.

d. Домашний агент переносного компьютера перехватывает дейтаграмму в домашней сети и туннелирует её по адресу обслуживания переносного компьютера, который а данном случае является адресом узла, служащего маршрутизатором и внешним агентом на борту самолёта. Обычная маршрутизация IP будет доставлять эту дейтаграмму в стационарную сеть авиакомпании.

e. Домашний агент маршрутизатора и бортового внешнего агента перехватывает дейтаграмму и туннелирует её по текущему адресу обслуживания, которым в нашем примере является некий (наземный) внешний агент на трассе полёта. Исходная дейтаграмма в результате будет инкапсулирована дважды - домашним агентом переносного компьютера и домашним агентом самолёта.

f. Внешний агент на земле декапсулирует дейтаграмму, извлекая из неё дейтаграмму, инкапсулированную домашним агентом переносного компьютера с полем Destination Address, указывающим адрес обслуживания переносного компьютера. Полученную в результате дейтаграмму этот внешний агент передаст по радиоканалу на борт самолёта.

g. Бортовой внешний агент декапсулирует дейтаграмму, извлекая исходную дейтаграмму с Destination Address, указывающим домашний адрес переносного компьютера. Затем этот агент доставит эту дейтаграмму через бортовую сеть, используя канальный адрес переносного компьютера.

Этот пример иллюстрирует случай подключения мобильного узла к мобильной сети. Т. е. мобильный узел является мобильным в сети, которая сама по себе также мобильна (в примере, относительно земли). Если же узел является стационарным в мобильной сети (т. е. мобильная сеть является домашней для мобильного узла), может применяться любой из двух методов доставки дейтаграмм такому узлу.

Для стационарного узла домашний агент **можно** настроить для постоянной регистрации, которая указывает адрес мобильного маршрутизатора в качестве адреса обслуживания хоста. Для этого обычно используется домашний агент мобильного маршрутизатора. В этом случае домашний агент отвечает за анонсирование связности со стационарным узлом с помощью обычных протоколов маршрутизации. Все дейтаграммы для стационарного узла будут использовать вложенное туннелирование, как описано выше.

Кроме того, мобильный маршрутизатор **может** анонсировать связность для всей мобильной сети, используя обычные протоколы маршрутизации IP через двухсторонний туннель со своим домашним агентом. Этот метод позволяет отказаться от вложенного туннелирования дейтаграмм.

4.6. ARP, Proxy ARP, Gratuitous ARP

Использование ARP [16] требует специальных правил для случаев, когда вовлечён беспроводный или мобильный узел. Заданные в этом параграфе требования применимы ко всем домашним сетям, где применяется протокол ARP для преобразования адресов.

В дополнение к обычному использованию ARP для сопоставления адреса канального уровня с IP-адресом узла этот документ выделяет два специальных случая применения протокола ARP, описанных ниже.

- Proxy ARP [49] представляет собой отклик ARP Reply, передаваемый одним узлом от имени другого узла, который не может или не хочет сам отвечать на запросы ARP Request. Отправитель Proxy ARP резервирует поля протокольных адресов Sender и Target, как описано в [16], по подставляет некий заданный в конфигурации (обычно свой) адрес канального уровня в поле Sender Hardware Address. Узел, получивший сообщение Reply, будет связывать адрес канального уровня с IP-адресом исходного целевого узла, что приведёт к передаче дейтаграмм для этого узла по указанному адресу канального уровня.

- Механизм Gratuitous ARP [45] использует пакеты ARP, отправляемые узлом, для того, чтобы другие узлы обновили записи в своём кэше ARP. Беспричинный ARP **может** использовать пакеты ARP Request или ARP Reply. В любом случае поля ARP Sender Protocol Address и ARP Target Protocol Address содержат адрес IP, для которого нужно обновить кэш-запись, в для ARP Sender Hardware Address указывается адрес канального

уровня, который должен появиться в обновлённой записи. При использовании пакетов ARP Reply в поле Target Hardware Address также указывается адрес канального уровня, который должен появиться в обновлённой записи (в ARP Request это поле не используется).

В любом случае для беспричинного ARP пакеты ARP **должны** передаваться как локальные широковещательные пакеты на локальном канале. Как указано в [16], любой узел, получивший пакет ARP (Request или Reply), **должен** обновить свой локальный кэш ARP с использованием адресов Sender Protocol и Hardware из пакета ARP, если принявший пакет узел уже имеет запись для этого адреса IP в своём кэше ARP. Это требование протокола ARP применимо даже к пакетам ARP Request и пакетам ARP Reply, которые не соответствуют запросам ARP, переданным узлом, который получил пакет [16].

Когда мобильный узел зарегистрирован в чужой сети, его домашний агент использует proxy ARP [49] для отклика на пакеты ARP Request, запрашивающие адрес канального уровня мобильного узла. При получении пакета ARP Request домашний агент **должен** проверить целевой адрес в запросе и при соответствии этого адреса домашнему адресу мобильного узла, для которого зарегистрирована мобильная привязка, домашний агент **должен** передать пакет ARP Reply от имени мобильного узла. После перестановки адресов получателя и отправителя в пакете [49] домашний агент **должен** установить в качестве адреса канального уровня в пакете адрес своего интерфейса, с которого будет передан пакет Reply.

Когда мобильный узел покидает домашнюю сеть и регистрирует привязку к чужой сети, его домашний агент использует Gratuitous ARP для обновления кэша ARP на узлах домашней сети. В результате узлы домашней сети связывают канальный адрес домашнего агента с домашним IP-адресом мобильного узла. При регистрации привязки мобильного узла, для которого у домашнего агента раньше не было привязок (мобильный узел не покидал домашней сети) домашний агент **должен** передать Gratuitous ARP от имени мобильного узла. Этот пакет ARP **должен** передаваться как широковещательный для канала, с которым связан домашний адрес мобильного узла. Поскольку широковещание на локальном соединении (например, Ethernet) обычно не обеспечивает гарантии доставки, пакет Gratuitous ARP **следует** повторить несколько раз для повышения надёжности.

При возвращении мобильного узла в домашнюю сеть этот узел и его домашний агент используют Gratuitous ARP, чтобы побудить все узлы домашней сети к обновлению своего кэше ARP в соответствии с адресом канального уровня и домашним IP-адресом мобильного узла. Перед отправкой сообщения (de)Registration Request своему домашнему агенту мобильный узел **должен** передать Gratuitous ARP в свою домашнюю сеть в широковещательном пакете для локального соединения. Пакет Gratuitous ARP **следует** повторить несколько раз для надёжности., однако повторы **следует** передавать параллельно передаче и обработке (de)Registration Request.

Когда домашний агент мобильного узла получает и воспринимает это сообщение (de)Registration Request, он **должен** также предаёт пакет Gratuitous ARP в домашнюю сеть мобильного узла. Этот пакет служит для связывания домашнего адреса мобильного узла с его адресом канального уровня. Пакеты Gratuitous ARP передаются мобильным узлом и домашним агентом, поскольку в случае беспроводных интерфейсов область передачи мобильного узла может отличаться от области передачи домашнего агента. Пакеты ARP от домашнего агента **должны** передаваться как широковещательные для домашнего канала мобильного узла и **следует** повторять передачу пакета несколько раз для повышения надёжности. Повторы **следует** выполнять параллельно с передачей и обработкой сообщения (de)Registration Reply для мобильного узла.

Пока мобильный узел находится в домашней сети, ему **недопустимо** передавать какие-либо широковещательные сообщения ARP Request или ARP Reply. Наконец, хотя мобильный узел находится дома, ему **недопустимо** отвечать на сообщения ARP Request, в которых целевым указан его домашний адрес IP, если только ARP Request не является индивидуальным от внешнего агента, на котором мобильный узел пытался зарегистрироваться или от внешнего агента, на котором на закончилась регистрация мобильного узла. В последнем случае мобильный узел **должен** использовать индивидуальную адресацию ARP Reply для ответа внешнему агенту. Отметим, что если мобильный узел использует совмещенный адрес обслуживания и получает ARP Request, в котором в качестве целевого адреса IP указан его адрес обслуживания, мобильному узлу **следует** отвечать на это сообщение ARP Request. Отметим также, что при передаче Registration Request в чужой сети мобильный узел может определить канальный адрес внешнего агента сохраняя адрес, который был получен из сообщения Agent Advertisement от этого агента, но не из широковещательного сообщения ARP Request.

Конкретный порядок, в котором применяется каждое из приведённых выше требований для ARP, proxy ARP и gratuitous ARP, относительно передачи и обработки сообщений мобильного узла Registration Request и Registration Reply при выходе из домашней сети или возвращении в неё важен для корректной работы протокола.

При выходе мобильного узла из домашней сети д**олжны** выполняться перечисленные ниже действия в указанном порядке.

- Мобильный узел решает зарегистрироваться вне дома, возможно в результате получения анонса Agent Advertisement от внешнего агента и продолжительного отсутствия таких анонсов от домашнего агента.
- Перед отправкой сообщения Registration Request мобильный узел отключает на будущее обработку любых сообщений ARP Request с запросом адреса канального уровня для его домашнего адреса, которые он может получить, за исключением нужных для взаимодействия с внешними агентами в чужих сетях.
- Мобильный узел передаёт Registration Request.
- Когда домашний агент мобильного узла получает и воспринимает сообщение Registration Request, он отправляет Gratuitous ARP от имени мобильного узла и начинает использовать proxy ARP для откликов на получаемые сообщения ARP Request с запросом канального адреса мобильного узла. В Gratuitous ARP поле ARP Sender Hardware Address содержит адрес канального уровня домашнего агента. Если вместо этого домашний агент станет отвергать сообщения Registration Request, обработка ARP (gratuitous и proxy) не будет выполняться домашним агентом.

При возвращении мобильного узла в домашнюю сеть **должны** быть выполнены приведённые ниже операции с сохранением их порядка.

- Мобильный узел принимает решение о регистрации в домашней сети (возможно в результате получения Agent Advertisement от своего домашнего агента).
- Перед отправкой сообщения Registration Request мобильный узел восстанавливает будущую обработку любых сообщений ARP Requests с запросом его адреса канального уровня.
- Мобильный узел выполняет для себя Gratuitous ARP, указывая в поле ARP Sender Hardware Address свой адрес канального уровня.
- Мобильный узел повторяет передачу сообщения Registration Request.
- Когда домашний агент мобильного узла получает и воспринимает сообщение Registration Request, он прекращает использование proxy ARP для откликов на сообщения ARP Request, запрашивающие канальный адрес мобильного узла, и выполняет процедуру Gratuitous ARP от имени мобильного узла, указывая в поле ARP Sender Hardware Address канальный адрес мобильного узла. Если вместо этого домашний агент отвергает сообщения Registration Request, ему **недопустимо** менять способ обработки ARP (ни gratuitous, ни proxy) для мобильного узла. В этом случае домашнему агенту следует вести себя так, будто мобильный узел не вернулся домой и продолжать выполнение proxy ARP от имени мобильного узла.

5. Вопросы безопасности

Мобильные компьютерные среды существенно отличаются от традиционных вычислительных сред. Во многих случаях мобильные компьютеры подключаются к сети по беспроводным каналам. Такие каналы могут быть уязвимыми для пассивного перехвата данных, активных атак с повторным использованием пакетов (replay) и других активных атак.

5.1. Коды проверки подлинности сообщений

Домашние агенты и мобильные узлы **должны** быть способны выполнять проверку подлинности. По умолчанию используется алгоритм HMAC-MD5 [10] с размером ключей 128 битов. Внешние агенты также **должны** поддерживать аутентификацию с использованием алгоритма HMAC-MD5 и ключей размером не менее 128 битов с ручным распространением ключей. **Должны** поддерживаться ключи с произвольными двоичными значениями.

Механизм prefix+suffix использует MD5 для защиты данных и общий секрет считается криптографическим сообществом уязвимым для атак. Если нужна совместимость со старыми реализациями Mobile IP, использующими этот режим, новым реализациям **следует** включать MD5 с ключами [19] в качестве одного из дополнительных алгоритмов аутентификации для использования при создании и проверке аутентификационных данных, которые представляются в регистрационных сообщениях Mobile IP, например, в расширениях, заданных в параграфах 3.5.2, 3.5.3 и 3.5.4.

Могут также поддерживаться дополнительные алгоритмы проверки подлинности, режимы алгоритмов, методы распространения и размеры ключей для всех аутентификационных расширений.

5.2. Проблемы безопасности, связанные с протоколом

Протокол регистрации, описанный в этом документе, будет приводить к туннелированию трафика мобильного узла на его адрес обслуживания. Это туннелирование может иметь серьёзные уязвимости, если регистрация проводится без проверки подлинности. Дистанционное перенаправление, выполняемое протоколом мобильной регистрации, считается одной из проблем безопасности Internet, если оно не использует аутентификации [30]. Кроме того, протокол ARP не использует проверки подлинности и может использоваться для кражи чужого трафика. Применение Gratuitous ARP (параграф 4.6) влечёт за собой все риски, связанные с ARP.

5.3. Управление ключами

Данная спецификация требует использования механизма строгой аутентификации (MD5 с ключами), что позволяет предотвратить множество потенциальных атак, основанных на протоколе регистрации Mobile IP. Однако в силу затруднительности распространения ключей без сетевого протокола управления ключами для взаимодействия с внешним агентом проверка подлинности сообщений не требуется. В коммерческих средах аутентификация сообщений между внешним и домашним агентом может быть важна для выставления счетов за обслуживание, поскольку сервис-провайдеры не обслуживают пользователей, которые не являются их легитимными заказчиками.

5.4. Выбор хороших случайных чисел

Надёжность любого механизма аутентификации зависит от нескольких факторов, включая стойкость алгоритма, секретность и стойкость используемого ключа, а также качества конкретной реализации. Данная спецификация требует реализации MD5 с ключом для проверки подлинности, но не исключает использования других алгоритмов и режимов аутентификации. Для эффективной аутентификации keyed MD5 128-битовый ключ должен быть секретным (известным лишь уполномоченным лицам) и псевдослучайным.

Если используются nonce для защиты от повторов, одноразовые значения тоже нужно выбирать осторожно. В RFC 4086 [8], написанном Eastlake с соавторами, приведены рекомендации по созданию псевдослучайных значений.

5.5. Приватность

Пользователям, имеющим конфиденциальные данные, которые они не хотят раскрывать, следует использовать выходящие за рамки этого документа механизмы (например, шифрование) для обеспечения подходящей защиты. Пользователям, озабоченным анализом трафика, следует применять подходящее шифрование каналов. Если требуется скрыть местоположение, мобильный узел может организовать туннель со своим домашним агентом. Тогда дейтаграммы будут представляться узлам-корреспондентам приходящими из домашней сети и это осложнит определение места размещения мобильного узла. Такие механизмы выходят за рамки этого документа.

5.6. Фильтрация на входе

На многих маршрутизаторах используются правила безопасности типа входной фильтрации [35], которые не позволяют пересылать пакеты, в которых Source Address представляется топологически некорректным. В средах, где это

вызывает проблемы, мобильные узлы могут применять реверсное туннелирование [12] с представленным внешним агентом адресом обслуживания в поле Source Address. Пакеты в реверсных туннелях смогут нормально проходить через такие маршрутизаторы, а входная фильтрация сможет определять корректно топологический источник как и для пакетов от стационарных узлов.

5.7. Защита от повторного использования для запросов регистрации

Поле Identification позволяет домашнему агенту проверить свежесть регистрационного сообщения, созданного мобильным узлом, и избавиться от используемых атакующими пакетов от предшествующих регистраций. В этом разделе описаны два метода защиты — временные метки (обязательный) и nonce (опция). Все мобильные узлы и домашние агенты **должны** поддерживать защиту от повторов на основе временных меток. Они **могут** также поддерживать защиту на базе одноразовых значений nonce.

Способ защиты от повторов между мобильным агентом и домашним узлом является частью MSA. Мобильный узел и его домашний агент **должны** согласовать используемый метод защиты. Интерпретация поля Identification зависит от выбранного метода, как описано в последующих параграфах.

Независимо от выбранного метода 32 младших бита поля Identification **должны** без изменений копироваться из регистрационного запроса в отклик. Внешний агент использует эти биты (и домашний адрес мобильного узла) для сопоставления регистрационных запросов и откликов. Мобильный узел **должен** проверить идентичность 32 младших битов в Registration Reply и соответствующих битов Registration Request.

В поле Identification нового сообщение Registration Request **недопустимо** указывать значение, которое использовалось в непосредственно предшествующем запросе и **не следует** повторять значение в течение всего срока действия контекста защиты между мобильным узлом и домашним агентом. Разрешена повторная передача в соответствии с параграфом 3.6.3.

5.7.1. Защита с использованием временных меток

Основа защиты от повторного использования с помощью временных меток заключается в том, что узел, генерирующий сообщение, вставляет в него временную метку, достаточно близкую к текущему времени на узле, а приёмный узел проверяет близость этой метки к своему текущему времени. Если в защитной связи между узлами не задано иное, **может** допускаться отклонение значений до 7 секунд. Допустимое отклонение **следует** делать больше 3 секунд. Обычно взаимодействующие узлы должны синхронизировать свои часы. Как и все другие, синхронизационные сообщения могут использовать механизм аутентификации, определённый в контексте защиты между парой узлов.

При использовании временных меток мобильный узел **должен** помещать в поле Identification 64-битовое значение в формате протокола NTP[1] [11]. 32 младших бита в формате NTP представляют доли секунды и при недоступности этих битов от источника временных меток взамен **следует** применять случайное значение из хорошего источника. Однако следует отметить, что при использовании временных меток 64-битовое поле Identification в сообщениях Registration Request от мобильного узла **должно** быть больше любого использованного в предыдущих сообщениях Registration Request значения, поскольку для домашнего агента это значение служит порядковым номером. Без такого номера становится возможным восприятие домашним агентом просроченных дубликатов предшествующих сообщений Registration Request (в соответствии с требуемой домашним агентом синхронизацией часов) и соответствующее нарушения порядка, ошибочно меняющее текущий зарегистрированный адрес обслуживания мобильного узла.

При получении сообщения Registration Request с разрешающим проверку полномочий расширением домашний агент **должен** проверить пригодность поля Identification. В действительном поле временная метка **должна** быть достаточно близка к текущему времени домашнего агента и **должна** быть больше значений предшествующих временных меток от этого мобильного узла. Допустимые отклонения и детали синхронизации определяются конкретной защищённой связью (Mobility Security Association).

Если временная метка действительна, домашний агент копирует поле Identification целиком в своё сообщение Registration Reply для мобильного узла. Если метка не действительна, домашний агент копирует в Registration Reply лишь 32 младших бита, а в старших указывает 32 бита своего текущего времени. В этом случае домашний агент **должен** отвергнуть регистрацию и возвратить код 133 (несоответствие Identification) в отклике Registration Reply.

Как описано в параграфе 3.6.2.1, мобильный узел **должен** проверить идентичность 32 младших битов поля Identification в сообщении Registration Reply битам в отвергнутой попытке регистрации до применения старших 32 битов для синхронизации часов.

5.7.2. Защита с использованием Nonce

Базовым принципом защиты от повторного использования с помощью одноразовых значений (nonce) является то, что узел А включает новое случайное значение в каждое сообщение для узла В и проверяет возврат узлом В того же значения в следующем сообщении для узла А. Оба сообщения используют код аутентификации для защиты от подмены атакующим. В то же время узел В может передавать свои значения nonce узлу А (которые А будет возвращать),так что «свежесть» принимаемых сообщений легко проверить.

Предполагается, что у домашнего агента есть ресурсы для расчёта псевдослучайных чисел, полезных для nonce [8]. Новое значение nonce помещается в старшие 32 бита поля Identification каждого сообщения Registration Reply. Домашний агент копирует 32 младших бита поля Identification из сообщения Registration Request в 32 младших бита поля Identification в сообщении Registration Reply. Когда мобильный узел получает аутентифицированный отклик Registration Reply от домашнего агента, он сохраняет 32 старших бита поля Identification для использования в качестве 32 старших битов следующего сообщения Registration Request.

Мобильный узел отвечает за генерацию младших 32 битов поля Identification в каждом сообщении Registration Request. В идеальном случае узлу следует самостоятельно генерировать случайные значения nonce. Однако узел может использовать любой подходящий метод, включая дублирование случайного значения, переданного домашним агентом. Выбранный метод интересует лишь сам мобильный узел, поскольку он сам проверяет пригодность значений в Registration Reply. Значения старших и младших 32 поля Identification **следует** выбирать так, чтобы они отличались от

[1]Network Time Protocol - протокол сетевого времени.

предшествующих. Домашний агент использует в каждом сообщении новое значение для старших битов, а мобильный узел - для младших. Внешние агенты используют значение младших битов (и домашний адрес мобильного узла) для сопоставления регистрационных откликов с ожидающими запросами (параграф 3.7.1).

Если регистрационное сообщение отвергается по причине непригодности nonce, сообщение Reply всегда указывает мобильному узлу новое значение nonce для следующей регистрации. Это обеспечивает самосинхронизацию протокола nonce.

6. Взаимодействие с IANA

Mobile IP задаёт несколько пространств номеров для значений, используемых в различных полях сообщений. Эти пространства включают перечисленные ниже.

- Типы сообщений Mobile IP, отправляемых в порт UDP 434, как описано в параграфе 1.8.
- Типы расширений Registration Request и Registration Reply (см. параграфы 3.3 и 3.4, а также [12], [43], [2], [3] и [7]).
- Значения кодов в сообщениях Registration Reply (см. параграф 3.4, а также [12], [43], [2], [3], [7]).
- Mobile IP определяет сообщения Agent Solicitation и Agent Advertisement, которые фактически являются сообщениями Router Discovery [5], дополненными связанными с Mobile-IP расширениями. Таким образом, для этих сообщений не определяется новое пространство имён, но определяются дополнительные расширения Router Discovery, как описано ниже в параграфе 6.2. См. также параграф 2.1 и работы [3] и [7].

В документе [3] заданы дополнительные пространства номеров Mobile IP.

Информацию о выделении номеров Mobile IP в других спецификациях можно найти на сайте IANA по ссылке http://www.iana.org/protocols (см. раздел Mobile Internet Protocol (IP) Numbers).

В этой пересмотренной спецификации потребовалось новое значение кода для поля сообщений Registration Reply в рамках диапазона, обычно используемого для сообщений внешних агентов. Этот код ошибки требуется для отклика о некорректном адресе домашнего агента (Invalid Home Agent Address), как описано в параграфе 3.7.2.

6.1. Типы сообщений Mobile IP

Для сообщений Mobile IP определена передача в порт получателя с номером 434 (UDP или TCP). Пространство номеров для сообщений Mobile IP задано в параграфе 1.8. Выделение номеров для расширений происходит по процедуре Expert Review, как указано в [22]. Стандартизованные к настоящему моменту номера сообщений перечислены в таблице и описаны в указанных в таблице параграфах.

Тип	*Имя*	*Параграф*
1	Registration Request	3.3
3	Registration Reply	3.4

6.2. Расширения для анонсов маршрутизаторов RFC 1256

RFC 1256 определяет два типа сообщений ICMP - Router Advertisement и Router Solicitation. Mobile IP определяет пространство номеров для Router Advertisement, которые могут применяться не только протоколом Mobile IP. Номера, стандартизованные для использования с Mobile IP, перечислены в таблице.

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

Выделение номеров для расширений происходит по процедуре Expert Review, как указано в [22].

6.3. Расширения для регистрационных сообщений Mobile IP

Сообщения Mobile IP, заданные в этом документе и перечисленные в параграфах 1.8 и 6.1, могут использовать расширения. Расширения сообщений Mobile IP используют общее пространство номеров, даже если они относятся к разным сообщениям Mobile IP. Пространство номеров расширений Mobile IP задано в этом документе. Выделение номеров для расширений происходит по процедуре Expert Review, как указано в [22].

Тип	*Имя*	*Параграф*
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 сообщений Mobile IP Registration Reply

Сообщение Mobile IP Registration Reply, описанное в параграфе 3.4, имеет поле Code. Пространство значений кодов также указано в параграфе 3.4. Это пространство структурировано в соответствии с результатами регистрации, как показано в таблице ниже.

Таблица 1. Рекомендации по выделению значений кодов.

Коды	*Рекомендации*
0-8	Коды успешного выполнения
9-63	Данный документ не даёт рекомендаций для этого диапазона кодов
64-127	Коды ошибок от внешнего агента
128-192	Коды ошибок от домашнего агента
193-200	Коды ошибок от внешнего агента-шлюза [29]
201-255	Данный документ не даёт рекомендаций для этого диапазона кодов

Выделение новых кодов происходит в соответствии с процедурой Expert Review [22].

7. Благодарности

Особая благодарность Steve Deering (Xerox PARC), а также Dan Duchamp и John Ioannidis (JI) (Columbia University) за формирование рабочей группы, руководство ею и значительный вклад в ранний этап разработки. Раннюю работу по Columbia Mobile IP можно найти в [37], [38], [39].

Спасибо также Kannan Alaggapan, Greg Minshall, Tony Li, Jim Solomon, Erik Nordmark, Basavaraj Patil и Phil Roberts за их вклад в работу группы при выполнении обязанностей руководителя, а также множество полезных замечаний.

Спасибо активным участникам рабочей группы IP Working, особенно тем, кто принял участие в написании текста (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 редакторам Charlie Kunzinger и Bill Simpson, которые создали первый черновой вариант документа, отражающий обсуждения в рабочей группе. Значительная часть текста в последних версиях перед выпуском RFC 2002 подготовлена 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 проведении совещаний рабочей группы.

Параграфы 1.10 и 1.11, которые описывают новые форматы расширений для использования с агрегируемыми типами расширений, были заимствованы из спецификации Mobile IP Extensions Rationalization (MIER), которую написали:

Mohamed Khalil (Nortel Networks);

Raja Narayanan (nVisible Networks);

Haseeb Akhtar (Nortel Networks);

Emad Qaddoura (Nortel Networks).

Спасибо этим авторам также за дополнительную работу в MIER, выполненную Basavaraj Patil, Pat Calhoun, Neil Justusson, N. Asokan и Jouni Malinen.

Спасибо Vijay Devarapalli, потратившему много часов на преобразование текста исходного документа в формат XML.

8. Литература

8.1. Нормативные документы

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

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

[3] Perkins, C., Calhoun, P., and J. Bharatia, "Mobile IPv4 Challenge/Response Extensions (Revised)", RFC 4721, January 2007.

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

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

[6] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.

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

[8] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[9] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

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

[11] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

[12] Montenegro, G., Ed., "Reverse Tunneling for Mobile IP, revised", RFC 3024, January 2001.

[13] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

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

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

[16] 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.

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

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

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

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

[21] Perkins, C., Ed., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[22] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

8.2. Дополнительная литература

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

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

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

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

[27] Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices", RFC 3519, April 2003.

[28] Glass, S. and M. Chandra, "Registration Revocation in Mobile IPv4", RFC 3543, August 2003.

[29] Fogelstroem, E., Jonsson, A., and C. Perkins, "Mobile IPv4 Regional Registration", RFC 4857, June 2007.

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

[31] Border, J., Kojo, M., Griner, J., Montenegro, G., and Z. Shelby, "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations", RFC 3135, June 2001.

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

[33] 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.

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

[35] 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.

[36] Jacobson, V., "Compressing TCP/IP Headers for Low-Speed Serial Links", RFC 1144, February 1990.

[37] Ioannidis, J., Duchamp, D., and G. Maguire, "IP-Based Protocols for Mobile Internetworking", In Proceedings of the SIGCOMM '01 Conference: Communications Architectures and Protocols, pages 235-245, September 1991.

[38] Ioannidis, J. and G. Maguire, "The Design and Implementation of a Mobile Internetworking Architecture", In Proceedings of the Winter USENIX Technical Conference, pages 489-500, January 1993.

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

[40] Jacobson, V., "Congestion Avoidance and Control", In Proceedings of the SIGCOMM '88 Workshop, ACM SIGCOMM, ACM Press, pages 314-329, August 1998.

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

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

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

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

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

[46] Perkins, C. and P. Calhoun, "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4", RFC 3957, March 2005.

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

[48] IANA, "Mobile IPv4 Numbers", http://www.iana.org.

[49] Postel, J., "Multi-LAN address resolution", RFC 925, October 1984.

[50] Perkins, C., Ed., "IP Mobility Support for IPv4", RFC 3220, January 2002.

Приложение A. Канальный уровень

Мобильный узел **может** использовать механизмы канального уровня для обнаружения смены точки подключения. Такая индикация включает состояния интерфейса Down/Testing/Up [41] и изменения в ячейке или администрировании. Механизмы будут зависеть от применяемой технологии канального уровня и выходят за рамки этого документа.

Протоколы PPP[1] [47] и IPCP[2] [42] согласуют использование адресов IP.

Мобильному узлу **следует** сначала попытаться задать свой домашний адрес, поскольку при подключении к домашней сети немаршрутизируемый канал будет работать корректно. Если партнёр не воспринимает домашний адрес, но мобильному узлу динамически выделяется временный адрес IP и узел способен поддерживать совмещенный адрес обслуживания (co-located care-of), этот узел **может** зарегистрировать полученный адрес в качестве адреса обслуживания. Когда партнёр задаёт свой адрес, **недопустимо** предполагать, что это адрес внешнего агента (care-of) или IP-адрес домашнего агента. Расширения PPP для Mobile IP заданы в RFC 2290 [23]. В этом документе приведена дополнительная информация по получению адресов обслуживания от PPP наиболее эффективным путем.

Приложение B. Проблемы TCP

B.1. Таймеры TCP

При работе по каналам с высокой задержкой (например, спутниковым) или малой пропускной способностью (например, по радиоканалу) некоторые стеки TCP могут иметь недостаточно адаптивные (нестандартные) тайм-ауты повтора передачи. Это может приводить к ложным тайм-аутам даже при корректной работе сети просто по причине значительной задержки в используемой среде. В результате организация или поддержка соединений TCP может стать невозможной или будут возникать необоснованные повторы передачи, которые будут приводить к дополнительному расходу дефицитной пропускной способности. Производителям рекомендуется следовать алгоритмам RFC 2988 [26] при реализации таймеров повтора TCP. Производителям систем для работы на низкоскоростных каналах со значительной задержкой следует обратиться к RFC 2757 и RFC 2488 [24], [25]. Разработчикам приложений для мобильных узлов следует принимать во внимание сложности, связанные с таймерами.

B.2. Контроль насыщения TCP

Мобильные узлы часто используют среды, в которых вероятность ошибок достаточно высока и пакеты могут отбрасываться. Это порождает конфликты с механизмами контроля перегрузок, используемыми в современных версиях TCP [40]. При отбрасывании пакет реализация TCP на стороне партнёра вероятно отреагирует на это как на перегрузку сети и инициирует механизм замедленного старта (slow-start) [40], разработанный для контроля перегрузок. Однако этот механизм не подходит для сетей с избыточными ошибками на каналах и в реальности лишь усиливает негативное влияние потери пакетов. Эта проблема была проанализирована в работе Caceres с соавторами [32]. Подходы TCP к обработке ошибок, которые могут конфликтовать с контролем перегрузок, рассмотрены в документах рабочей группы PILC [31] [33]. Хотя эти подходы выходят за рамки данного документа, они показывают, что обеспечение производительности для мобильных узлов включает механизмы, выходящие за пределы сетевого уровня. Проблемы, вызываемые большим числом ошибок в среде, также показывают необходимость избегать использования решений, которые систематически отбрасывают пакеты. В других ситуациях такие решения могут быть эффективными с учётом инженерных компромиссов.

Приложение C. Примеры

В этом приложении приведены примера сообщений Registration Request для типичных сценариев.

C.1. Регистрация с Foreign Agent Care-of Address

Мобильный узел получает сообщение Agent Advertisement от внешнего агента и хочет зарегистрироваться у него с использованием адреса обслуживания от этого агента. Мобильный узел желает применять лишь инкапсуляцию IP-in-IP, не хочет получать широковещательных пакетов и не желает одновременных мобильных привязок.

Поля IP

Source Address = домашний адрес мобильного узла;

Destination Address = копируется из IP-адреса отправителя в Agent Advertisement;

Time to Live = 1.

Поля UDP

Source Port = <любой>;

Destination Port = 434.

Поля сообщения Registration Request

Type = 1;

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

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

[1] Point-to-Point-Protocol - протокол для соединений «точка-точка».
[2] Internet Protocol Control Protocol - протокол управления IP.

Home Address = домашний адрес мобильного узла;

Home Agent = IP-адрес домашнего агента;

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

Identification = временная метка NTP или Nonce.

Расширения

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

C.2. Регистрация с Co-Located Care-of Address

Мобильный узел подключается к чужой сети, в которой нет внешнего агента. Узел получает адрес от сервера DHCP [34] для использования в качестве совмещённого адреса обслуживания (co-located care-of). Мобильный узел поддерживает все формы инкапсуляции (IP-in-IP, минимальная инкапсуляция, GRE), желает получать широковещательные дейтаграммы из домашней сети и не желает одновременных мобильных привязок.

Поля IP

Source Address = адрес обслуживания (care-of), полученный от сервера DHCP;

Destination Address = IP-адрес домашнего агента;

Time to Live = 64.

Поля UDP

Source Port = <любой>

Destination Port = 434.

Поля сообщения 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;

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

Identification = временная метка NTP или Nonce.

Расширения

Mobile-Home Authentication.

C.3. Дерегистрация

Мобильный узел возвращается домой и отменяет регистрацию всех адресов обслуживания на своём домашнем агенте.

Поля IP

Source Address = домашний адрес мобильного узла;

Destination Address = IP-адрес домашнего агента;

Time to Live = 1.

Поля UDP

Source Port = <любой>;

Destination Port = 434.

Поля сообщения 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;

Care-of Address = домашний адрес мобильного узла;

Identification = временная метка NTP или Nonce.

Расширения

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

Приложение D. Применимость расширения Prefix-Lengths

Следует отметить использование расширения Prefix-Lengths на беспроводных каналах, поскольку беспроводные приемопередатчики не обеспечивают равномерного покрытия. В результате могут возникать ситуации, когда два внешних агента, анонсирующих одинаковый префикс, могут различную связность с потенциальными мобильными узлами. Расширение Prefix-Lengths **не следует** включать в анонсы, передаваемые агентами в такой конфигурации.

Внешние агенты, использующие разные беспроводные интерфейсы, должны будут взаимодействовать по специальному протоколу для обеспечения идентичного пространственного покрытия и таким образом заявлять о наличии беспроводных интерфейсов из одной подсети. В случае проводных интерфейсов мобильный узел отключающийся от сети и затем подключающийся к другой точке привязки, может отправить новое сообщение Registration Request независимо от того, относится ли новый анонс к той же среде, из которой был получен предыдущий анонс. И, наконец, в областях с высокой плотностью внешних агентов было бы неразумно требовать распространения через протоколы маршрутизации префиксов подсетей, связанных с каждым отдельным беспроводным внешним агентом. Такая стратегия может привести к быстрому истощению доступного для таблиц маршрутизации пространства, необоснованному росту времени, требуемого для обработки таблиц маршрутизации и замедлению принятия решений по выбору маршрутов, если маршруты (которые почти никогда не нужны) будут сохраняться для беспроводных «подсетей».

Приложение E. Вопросы взаимодействия

Этот документ задаёт пересмотр RFC 2002 в целях повышения уровня взаимодействия за счет устранения содержавшихся в документе неоднозначностей. Реализации, выполняющие проверку подлинности св соответствии с новым, заданным более точно алгоритмом, смогут взаимодействовать с прежними реализациями, которые выполняют то, что первоначально ожидалось для обеспечения аутентификационных данных. Это было основным источником проблем совместимости.

Однако данная спецификация не включает новых функций, использование которых могло бы вызвать проблемы при взаимодействии с ранними реализациями. Все функции, заданные в RFC 2002, будут работать с новыми реализациями, за исключением компрессии V-J [36]. В приведённом ниже списке перечислены возможные проблемы совместимости, с которыми могут столкнуться узлы, соответствующие данной спецификации, при взаимодействии с узлами RFC 2002.

- Клиент, ожидающий новых обязательных функций (типа реверсных туннелей) от внешнего агента (FA), сохранит возможность взаимодействия, если он принимает во внимание бит T.
- Мобильные узлы (MN), использующие расширение NAI для идентификации себя, не смогут работать со старыми агентами мобильности.
- Мобильные узлы, использующие нулевой домашний адрес и предполагающие получить домашний адрес в сообщении Registration Reply, не смогут работать со старыми агентами мобильности.
- Мобильные узлы, пытающиеся подтвердить свою подлинность без использования расширения Mobile-Home authentication, не смогут зарегистрироваться у своего домашнего агента.

Во всех таких случаях отказоустойчивый и корректно настроенный мобильный узел скорей всего сможет нормально работать, если предпримет разумные действия при получении регистрационного отклика с кодом ошибки, указывающим причину отказа. Например, если мобильный узел передаёт сообщение Registration Request, которое отвергается по причине указания неприемлемого аутентификационного расширения, этот узел может повторить попытку регистрации с расширением Mobile-home authentication, поскольку внешний и/или домашний агент в этом случае не будет запрашивать дополнительных данных для проверки подлинности.

Приложение F. Отличия от RFC 3344

Ниже перечислены изменения, внесённые в спецификацию с момента публикации RFC 3344. Список отличий от RFC 2002, внесённых при создании RFC 3344 [21], можно найти в RFC 3344.Для изменений, указанных с номерами выпусков, можно найти дополнительную информацию в архивах списка рассылок MIP4.

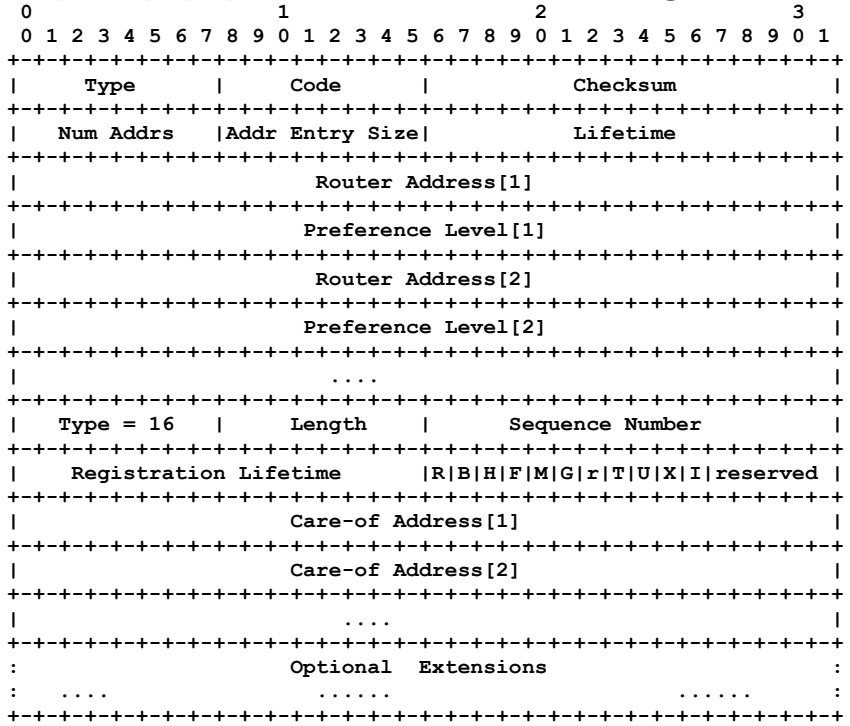
- Показано больше определений битов в структуре сообщения Agent Advertisement (параграф 2.1.1). В других спецификациях были определены новые биты анонсов, которые не были представлены в этой спецификации, что приводило к путанице. Включены также выдержки из соответствующих спецификаций.
- (Выпуск 6) Было изменено поведение домашнего агента чтобы избежать обязательной отправки откликов об ошибках на регистрационные запросы, в которых отказ был вызван тем, что внешний агент не прошёл проверку подлинности. Цель заключается в том, чтобы сделать домашний агент более устойчивым к атакам, нацеленным на отказ в обслуживании (DoS[1]), когда враждебное устройство не предоставляет действительных сообщений Registration Request, а лишь загружает трафиком домашнюю сеть (см. параграф 3.8.2.1).
- По причине использования неуникальных адресов IPv4 во многих домена у разных мобильных узлов могут оказаться одинаковые домашние адреса. Если эти узлы используют NAI, внешний агент сможет различить их. В параграфы 3.7.1 и 3.7.3.1 был добавлен текст о том, что внешний агент **должен** использовать NAI, чтобы различать мобильные узлы с совпадающими домашними адресами.
- (Выпуск 45) Отмечено, что внешнему агенту **недопустимо** применять расширение Foreign-Home Authentication для запросов дерегистрации мобильных узлов. Также для внешнего агента **недопустимо** использовать расширение Foreign-Home Authentication, если Care-of Address в Registration Request не соответствует адресу, анонсируемому этим агентом.
- Указано, что MSA будет применяться внешним и домашним агентом в зависимости от значений, содержащихся в данных сообщения, а не от заголовка IP.

[1]Denial of Service.

- (Выпуски 9, 18) Определён новый код ошибки для использования внешним агентом для случая, когда внешний агент не обслуживает мобильный узел как домашний агент. Раньше в таких случаях внешний агент мог использовать код 136.
- (Выпуск 17) Указано, что в случаях, когда домашний агент не может поддерживать запрошенный ненулевой индивидуальный адрес в поле Home Address сообщения Registration Request, он **должен** отвергнуть регистрацию с кодом 129 (см. параграф 3.8.3.2).
- (Выпуск 19) Указана возможность присутствия множества разрешающих проверку полномочий расширений в сообщении Registration Request, но домашний агент должен (каким-либо образом) обеспечить выполнение всех таких проверок (см. параграф 3.8.3.1).
- (Выпуск 20) Указано, что внешнему агенту **не следует** менять какие-либо поля сообщения Registration Reply, охватываемые расширением Mobile-Home Authentication, когда он транслирует пакет мобильному узлу.
- (Выпуск 21) Уточнено, что внешний агент удаляет расширения, которые не предшествуют каким-либо аутентификационным расширениям, а не только Mobile-Home Authentication (параграф 3.7.3.2).
- (Выпуск 44) Указано, что адрес, анонсируемый внешним агентом в сообщениях Agent Advertisement, является адресом care-of, предлагаемом на сетевом интерфейсе, а не обязательно адресом сетевого интерфейса (параграф 3.7.2.2).
- (Выпуск 45) В параграфе 3.7.2.1 уточнено, что код 77 применяется только для сообщений Registration Request с отличным от 0 значением Lifetime.
- Добавлен код ошибки для использования внешним агентом в тех случаях, когда он может обнаружить некорректность поля с адресом домашнего агента.
- Запрещено использование расширения Foreign-Home Authorization в сообщениях дерегистрации.
- Исключены некоторые формулировки, связанные с расширениями, разрешающими проверку полномочий.
- Для согласованности изменён текст о копировании портов UDP.
- Добавлена формулировка, которая явно не запрещает динамически настраиваемые маски сети и данные защиты на мобильных узлах.
- Переписан данный раздел.
- Обновлены цитаты из других документов.

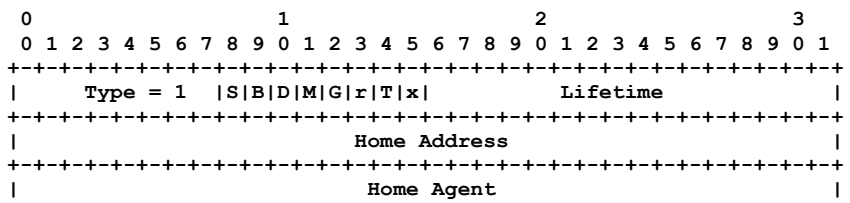
Приложение G. Примеры сообщений

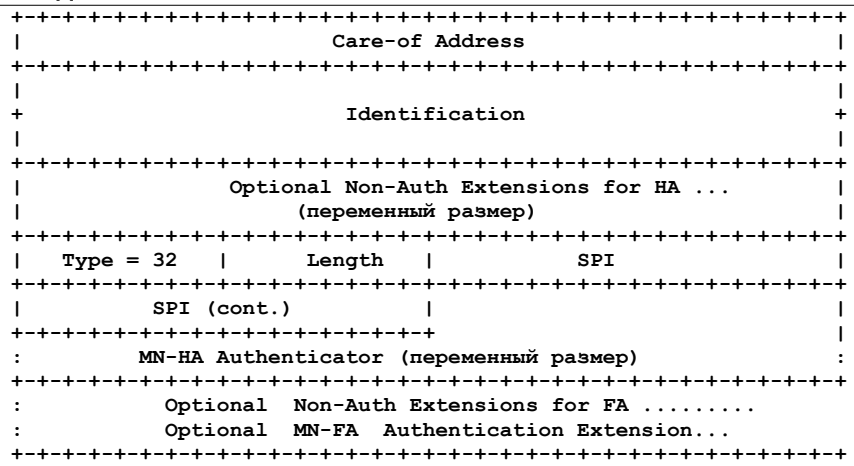
G.1. Пример формата сообщения ICMP Agent Advertisement



G.2. Пример формата сообщения Registration Request

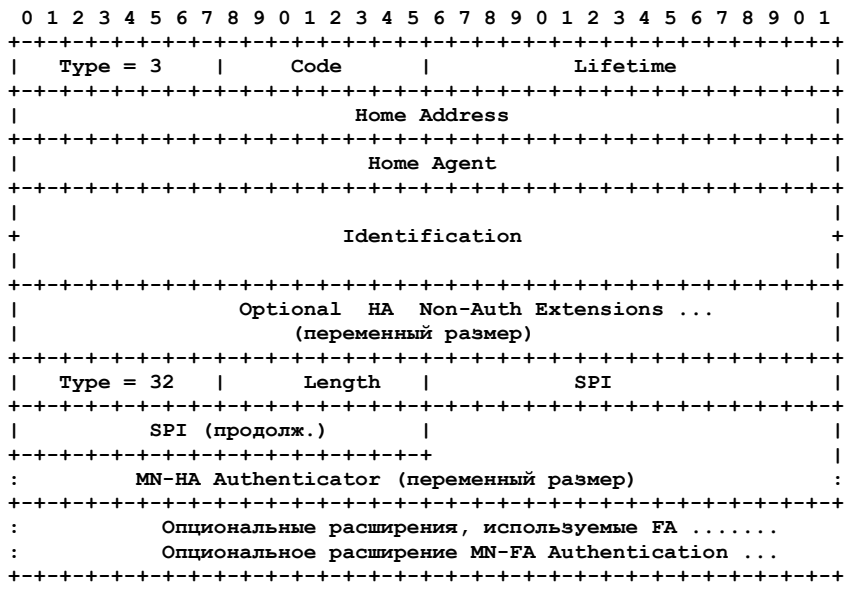
Ниже показан пример заголовка UDP, за которым следуют поля Mobile IP.





G.3. Пример формата сообщения Registration Reply

Ниже показан заголовок UDP и следующие за ним поля Mobile IP.



Адрес автора

Charles E. Perkins (редактор)

WiChorus Inc.

3590 N. 1st Street, Suite 300

San Jose, CA 95134

USA

EMail: charliep@computer.org

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru