

Internet Engineering Task Force (IETF)
Request for Comments: 9301
Obsoletes: 6830, 6833
Category: Standards Track
ISSN: 2070-1721

D. Farinacci
lispers.net
F. Maino
Cisco Systems
V. Fuller
vaf.net Internet Consulting
A. Cabellos, Ed.
Universitat Politecnica de Catalunya
October 2022

Locator/ID Separation Protocol (LISP) Control Plane

Плоскость управления протокола разделения идентификаторов и локаторов (LISP)

Аннотация

Этот документ описывает плоскость управления и службу сопоставления (Mapping Service) для протокола разделения идентификаторов и локаторов (Locator/ID Separation Protocol или LISP), реализованные двумя типами использующих LISP устройств - распознавателями LISP Map-Resolver и серверами LISP Map-Server, - которые обеспечивают упрощённый интерфейс (front end) для одного или нескольких идентификаторов конечных точек (Endpoint ID или EID) в базу сопоставления с локаторами маршрутизации (Routing Locator или RLOC).

Используя этот интерфейс службы плоскости управления и взаимодействуя с распознавателями Map-Resolver и серверами Map-Server, входные (LISP Ingress Tunnel Router или ITR) и выходные (Egress Tunnel Router или ETR) маршрутизаторы туннелей независимы от деталей базы данных системы сопоставления, что способствует модульности с разными вариантами баз данных. Поскольку эти устройства реализуются на «периметре» (edge) инфраструктуры плоскости управления LISP, соединяя узлы с адресами EID на сайте LISP, снижается сложность и стоимость реализации и эксплуатации развёртывания LISP.

Этот документ отменяет RFC 6830 и RFC 6833.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF¹ и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG². Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке <https://www.rfc-editor.org/info/rfc9301>.

Авторские права

Copyright (c) 2022. Авторские права принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

Оглавление

1. Введение.....	2
1.1. Сфера применимости.....	2
2. Уровни требований.....	3
3. Определения терминов.....	3
4. Базовый обзор.....	3
5. Форматы пакетов плоскости управления LISP IPv4 и IPv6.....	4
5.1. Типы пакетов управления LISP.....	4
5.2. Формат сообщения Map-Request.....	5
5.3. Сообщение EID-RLOC UDP Map-Request.....	6
5.4. Формат сообщения Map-Reply.....	7
5.5. Сообщение EID-RLOC UDP Map-Reply.....	8
5.6. Формат сообщения Map-Register.....	9
5.7. Формат сообщений Map-Notify и Map-Notify-Ack.....	11
5.8. Формат инкапсулированного управляющего сообщения.....	11
6. Изменение содержимого отображений EID-RLOC.....	12
6.1. Solicit-Map-Request (SMR).....	12
7. Доступность локаторов маршрутизации.....	13

¹Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

²Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

7.1. Алгоритм зондирования RLOC.....	13
8. Взаимодействие с другими компонентами LISP.....	13
8.1. Распознавание отображения ITR EID-RLOC.....	13
8.2. Настройка EID-Prefix и регистрация ETR.....	14
8.3. Обработка в Map-Server.....	14
8.4. Обработка в Map-Resolver.....	15
8.4.1. Операции Anycast.....	15
9. Вопросы безопасности.....	15
10. Вопросы приватности.....	16
11. Отличия от RFC 6830 и RFC 6833.....	16
12. Взаимодействие с IANA.....	16
12.1. Номера портов LISP UDP.....	17
12.2. Коды типа пакетов LISP.....	17
12.3. Коды LISP Map-Reply EID-Record Action.....	17
12.4. Коды LISP Address Type.....	17
12.5. Номера LISP Algorithm ID.....	17
12.6. Битовые флаги LISP.....	17
13. Литература.....	18
13.1. Нормативные документы.....	18
13.2. Дополнительная литература.....	19
Благодарности.....	20
Адреса авторов.....	20

1. Введение

Протокол разделения локаторов и идентификаторов (Locator/ID Separation Protocol или LISP) [RFC9300] (см. также [RFC9299]) задаёт архитектуру и механизм для динамического туннелирования путём разделения адресов IP на два пространства имён - идентификаторы конечных точек (Endpoint ID или EID), используемые внутри сайтов, и локаторы маршрутизации (Routing Locator или RLOC), используемые в транзитных сетях, образующих инфраструктуру Internet. Для такого разделения LISP задаёт протокольные механизмы сопоставления EID с RLOC. Кроме того, в LISP предполагается наличие базы данных, хранящей и распространяющей такие отображения между узлами системы отображения (Mapping System). Предложено несколько таких баз, включая наложенную службу распространения содержимого (Content distribution Overlay Network Service) для LISP-NERD (стареет, чем EID-to-RLOC Database) [RFC6837], дополнительную логическую топологию LISP (LISP Alternative Logical Topology или LISP-ALT) [RFC6836] и дерево делегированной базы данных LISP (LISP Delegated Database Tree или LISP-DDT) [RFC8111].

LISP Mapping Service определяет два типа понимающих LISP узлов - Map-Resolver, который воспринимает Map-Request от входных маршрутизаторов туннелей (Ingress Tunnel Router или ITR) и преобразует сопоставления EID-RLOC с помощью базы данных, и Map-Server, который узнаёт полномочные отображения EID-RLOC у выходных маршрутизаторов туннелей (Egress Tunnel Router или ETR) и публикует их в базе данных.

Плоскость управления LISP и службу сопоставления можно применять с множеством плоскостей данных на основе инкапсуляции или трансляции, включая заданные в LISP [RFC9300], расширении базового протокола LISP (LISP Generic Protocol Extension или LISP-GPE) [RFC9305], виртуальных расширяемых ЛВС (Virtual eXtensible Local Area Network или VXLAN) [RFC7348], VXLAN-GPE [NVO3-VXLAN-GPE], GRE¹ [RFC2890], протоколе туннелирования GPRS (GPRS Tunneling Protocol или GTP) [GTP-3GPP], адресации ILA (Identifier-Locator Addressing) [INTAREA-ILA] и маршрутизации по сегментам (Segment Routing или SRv6) [RFC8402].

Концептуально серверы отображения LISP Map-Server имеют некоторые базовые свойства настройки и поддержки серверов системы доменных имён (Domain Name System или DNS) [RFC1035], а распознаватели Map-Resolver похожи на кэширующие распознаватели DNS. С учётом этого в данной спецификации применяются термины (распознаватель и сервер) из спецификаций DNS.

Отметим, что этот документ не предполагает какую-либо инфраструктуру баз отображения для иллюстрации некоторых аспектов операций Map-Server и Map-Resolver. Интерфейс службы отображения может и, скорее всего, будет) применяться ITR и ETR для доступа к другим системам баз данных по мере развития инфраструктуры LISP.

Протоколы LISP не предназначены для решения задач связности и расширяемости от имени произвольных взаимодействующих сторон. Соответствующие ситуации описаны в параграфе 1.1 [RFC9300].

Этот документ отменяет [RFC6830] и [RFC6833].

1.1. Сфера применимости

Изначально протокол LISP создавался для решения проблемы расширения маршрутизации в сети Internet [RFC4984]. Хотя имеется ряд подходов к решению этой задачи, по мере разработки и совершенствования LISP было найдено и реализовано много других применений LISP. В результате устройство и разработка LISP изменились с нацеленностью на эти варианты применения. Общим свойством таких вариантов является большой набор кооперирующихся объектов, стремящихся взаимодействовать через Internet или иную крупную инфраструктуру IP, сохраняя адресацию и топологию сотрудничающих элементов отдельно от топологии, маршрутизации и адресации базовой сети и Internet.

При взаимодействии через общедоступную сеть Internet **должны** учитываться приведённые ниже руководства.

1. **Должна** быть реализована защита LISP (LISP Security или LISP-SEC) [RFC9303]. Это значит, что бит S **должен** быть установлен в сообщениях Map-Reply (параграф 5.4), Map-Register (параграф 5.6), Encapsulated Control (ECM) (параграф 5.8).
2. Разработчикам **следует** использовать HMAC-SHA256-128+HKDF-SHA256 как Algorithm ID (параграф 12.5) в сообщениях Map-Register (параграф 5.6) и **недопустимо** использовать None или HMAC-SHA-1-96-None как Algorithm ID (параграф 12.5) в сообщениях Map-Register (параграф 5.6).

¹Generic Routing Encapsulation - базовая инкапсуляция маршрутных данных.

2. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

3. Определения терминов

Map-Server - сервер отображений (сопоставлений)

Элемент инфраструктуры сети, изучающий записи отображений EID-Prefix от ETR через описанный ниже механизм регистрации или от какого-либо иного полномочного источника, если он имеется. Map-Server публикует эти EID-Prefix в базе данных отображений.

Map-Request - запрос отображения

Сообщение плоскости управления, запрашивающее у системы отображения распознавание EID. LISP Map-Request может передаваться также по адресу RLOC для проверки доступности или обмена ключами защиты между инкапсулятором и декапсулятором. Этот тип Map-Request называют также RLOC-Probe Request.

Map-Reply - отклик с отображением

Сообщение плоскости управления, возвращаемое в ответ на сообщение Map-Request, переданное в Mapping System при распознавании EID. LISP Map-Reply может также возвращаться декапсулятором в ответ на Map-Request от инкапсулятора для проверки доступности. Этот тип Map-Reply называют также RLOC-Probe Reply.

Encapsulated Map-Request - инкапсулированный запрос отображения

Запрос LISP Map-Request, передаваемый с инкапсуляцией LISP (ECM). Этот Map-Request имеет в начале дополнительный заголовок LISP и передаётся в порт UDP 4342. Внешним адресом является маршрутизируемый адрес, называемый также RLOC. Применяется ITR при отправке Map-Resolver и сервером Map-Server при пересылке Map-Request в ETR.

Map-Resolver - распознаватель отображений

Элемент инфраструктуры сети, воспринимающий инкапсулированные в LISP (ECM) сообщения Map-Request (обычно от ITR) и определяющий, является ли IP-адрес получателя частью пространства EID. Если это не так, возвращается Negative Map-Reply, в ином случае Map-Resolver находит подходящее отображение EID-RLOC, запрашивая базу данных отображений.

Negative Map-Reply - негативный отклик для отображения

LISP Map-Reply с пустым набором Locator-Set, возвращаемый в ответ на Map-Request, если EID получателя не зарегистрирован в Mapping System, запрещён правилами или не прошла аутентификация.

Map-Register message - сообщение Map-Register

Сообщение LISP, передаваемое ETR серверу Map-Server для регистрации связанных с маршрутизатором EID-Prefix. В дополнение к отправке EID-Prefix для регистрации сообщение включает 1 или несколько RLOC, обеспечивающих доступ к ETR. Map-Server использует эти RLOC при пересылке Map-Request (переформатированных как Encapsulated Map-Request). ETR **может** запросить, чтобы Map-Server отвечал на Map-Request от своего имени, установив в сообщении флаг проху Map-Reply (P).

Map-Notify message - сообщение Map-Notify

Сообщение LISP, передаваемое Map-Server маршрутизатору ETR для подтверждения приёма и обработки Map-Register. ETR запрашивает возврат Map-Notify установкой флага want-map-notify (M-bit) в сообщении Map-Register. В отличие от Map-Reply, сообщения Map-Notify используют порт UDP 4342 для источника и получателя. Сообщения Map-Notify передаются также маршрутизаторам ITR от Map-Server при изменении RLOC-Set.

Определения других терминов, в частности Ingress Tunnel Router (ITR), Egress Tunnel Router (ETR), Re-encapsulating Tunnel Router (RTR), приведены в спецификации плоскости данных LISP [RFC9300].

4. Базовый обзор

Map-Server - это устройство, публикующее EID-Prefix в базе отображений LISP от имени набора ETR. При получении Map-Request (обычно от ITR) сервер обращается к базе данных для поиска ETR и может получить в ответ набор RLOC для EID-Prefix. Для публикации EID-Prefix маршрутизатор ETR периодически отправляет сообщения Map-Register серверу Map-Server. Сообщение Map-Register содержит список EID-Prefix и набор RLOC, которые можно использовать для доступа к ETR.

При использовании LISP-ALT [RFC6836] в качестве базы данных отображений Map-Server соединяется с сетью ALT и действует как последний маршрутизатор (last-hop) ALT-Router. Промежуточные ALT-Router пересылают Map-Request серверу Map-Server, который анонсирует конкретный EID-Prefix, а тот пересылает их владельцу ETR, который отвечает сообщениями Map-Reply.

При использовании базы отображения LISP-DDT [RFC8111] Map-Server передаёт финальные сообщения Map-Referral от дерева делегированной базы данных (Delegated Database Tree или DDT).

Map-Resolver получает инкапсулированные Map-Request от своих ITR-клиентов и использует базу отображений в поиске подходящего ETR для ответа на эти запросы. В сети LISP-ALT Map-Resolver выступает как первый маршрутизатор (first-hop) ALT-Router. Он имеет туннели GRE к другим ALT-Router и использует BGP для изучения путей к ETR с разными префиксами в базе данных LISP-ALT. Map-Resolver использует сведения о путях для пересылки Map-Request через ALT корректным ETR. В сети LISP-DDT [RFC8111] Map-Resolver поддерживает кэш ссылок и выступает первым (first-hop) узлом DDT. Map-Resolver использует ссылочные данные для пересылки Map-Request.

Хотя Map-Resolver может кэшировать отклики для повышения производительности, нужно решать проблемы, связанные с управлением кэшем, чтобы это было надёжно и практично. В этой спецификации Map-Resolver работают без кэширования, декапсулируя и пересылая инкапсулированные Map-Request, полученные от ITR. Спецификация функций кэширования выходит за рамки этого документа.

Отметим, что одно устройство может совмещать функции Map-Server и Map-Resolver и это будет применяться во многих случаях. При использовании LISP-ALT и LISP-DDT могут быть узлы, поддерживающие только ALT или только DDT, соответственно, соединяющие Map-Resolver и Map-Server для создания системы отображения Mapping System.

5. Форматы пакетов плоскости управления LISP IPv4 и IPv6

Ниже представлены форматы пакетов UDP, используемых плоскостью управления LISP.

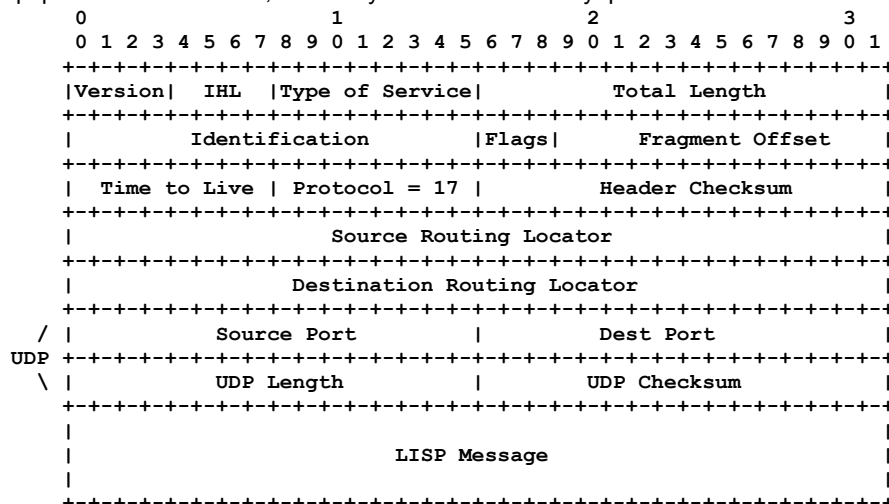


Рисунок 1. Управляющее сообщение IPv4 UDP LISP.

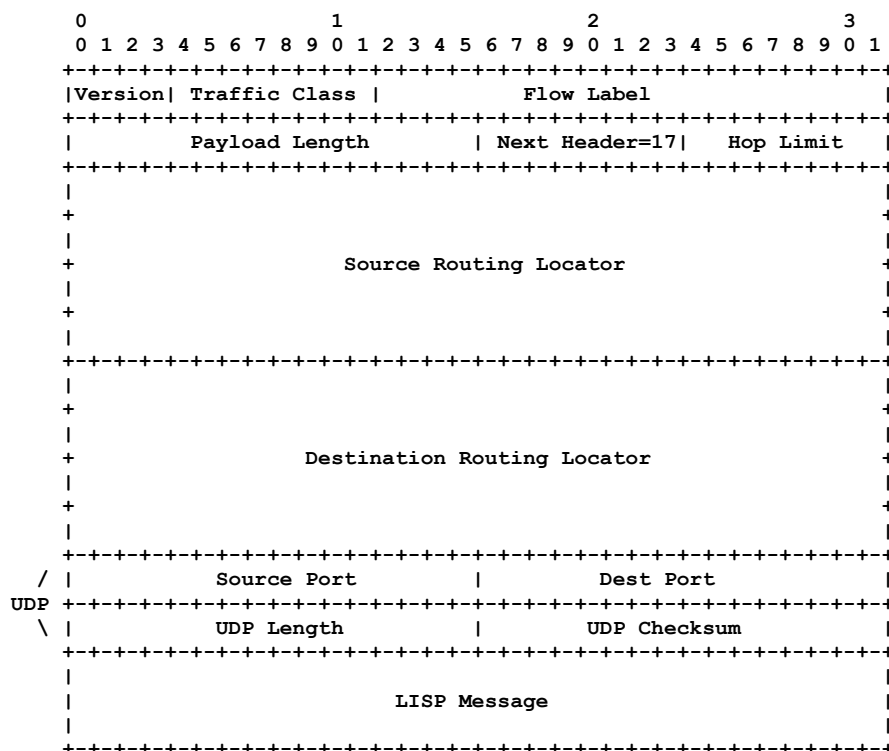


Рисунок 2. Управляющее сообщение IPv6 UDP LISP.

При отправке UDP Map-Request, Map-Register, Map-Notify (в качестве уведомления) порт источника UDP выбирается отправителем, а для порта получателя устанавливается значение 4342. При передаче UDP Map-Reply, Map-Notify (как подтверждения Map-Register), Map-Notify-Ack устанавливается порт отправителя UDP 4342, а номер порта получателя копируется из поля порта отправителя в Map-Request или вызвавшем сообщении пакете данных. реализации **должны** быть готовы воспринимать пакеты, в которых указан порт отправителя или получателя UDP 4342 в результате смены номера порта системой NAT.

Поле UDP Length отражает размер заголовка UDP и содержимого сообщения LISP. Предполагается, что LISP будет применяться сотрудничающими организациями, взаимодействующими через базовые сети. При внедрении предполагается установка MTU в соответствии с конкретными рекомендациями по развёртыванию для предотвращения фрагментации внутренних пакетов или внешних инкапсулированных пакетов. Для внедрений, где ограничения базовых сетей в части MTU на пути неизвестны, размер сообщения **должен** ограничиваться 576 байтами для IPv4 и 1280 - для IPv6 с учётом всего пакета IP, как описано в [RFC8085].

Контрольная сумма UDP рассчитывается и устанавливается (не 0) для всех сообщений, передаваемых в порт 4342 или из него. Это **должно** проверяться при получении и управляющие сообщения с ошибкой контрольной суммы **должны** отбрасываться [RFC1071].

Формат управляющих сообщения включает заголовок UDP, поэтому поля контрольной суммы и размера можно использовать для защиты и обозначения границ сообщений.

5.1. Типы пакетов управления LISP

В этом параграфе описаны форматы управляющих сообщений LISP и дана сводка назначенных документом кодов LISP Type для IANA. Для полноты в сводку включено сообщение LISP Shared Extension, заданное в [RFC9304]. Определения типов сообщений перечислены в таблице 1.

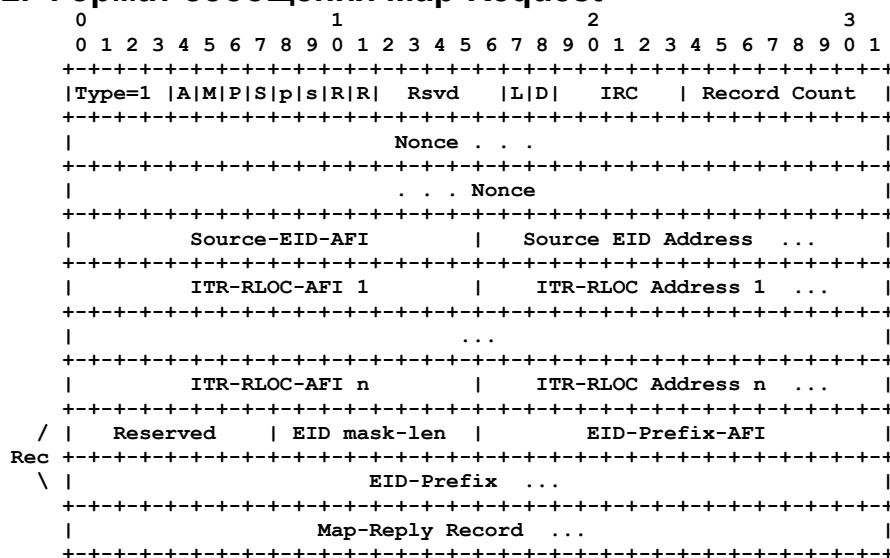
Сообщение	Код	Двоичный код
Резерв	0	b'0000'
LISP Map-Request	1	b'0001'
LISP Map-Reply	2	b'0010'
LISP Map-Register	3	b'0011'
LISP Map-Notify	4	b'0100'
LISP Map-Notify-Ack	5	b'0101'
LISP DDT Map-Referral	6	b'0110'
Unassigned	7	b'0111'
LISP Encapsulated Control	8	b'1000'
Не выделены	9-14	b'1001'- b'1110'
LISP Shared Extension	15	b'1111'

Разработчикам протоколов, экспериментирующим с новыми форматами сообщений, рекомендуется применять тип LISP Shared Extension, описанный в [RFC9304].

Сообщения плоскости управления LISP используют идентификаторы семейств адресов (Address Family Identifier или AFI) [AFN] или канонический формат адресов LISP (LISP Canonical Address Format или LCAF) [RFC8060] для представления адресов с фиксированным или переменным размером. Это включает явные поля в каждом управляющем сообщении или части EID-Record или RLOC-Record в сообщениях с базовым форматом. Сообщения плоскости управления LISP с нераспознанным AFI **должны** отбрасываться и в системных журналах **должна** вноситься запись об этом.

Плоскость управления LISP описывает, как другие плоскости данных могут кодировать сообщения для поддержки запросов Map-Request, а также процедур RLOC-Probing.

5.2. Формат сообщения Map-Request



Тип

1 (Map-Request)

A

Бит полномочий (authoritative) устанавливаемый (1), когда ITR хочет, чтобы Map-Reply возвращал сайт получателя, а не база данных. В ином случае бит сбрасывается (0).

M

Бит map-data-present, установка (1) которого показывает, что в Map-Request включён сегмент Map-Reply Record.

P

Бит зондирования (probe-bit), указывающий, что сообщение Map-Request **должно** считаться зондом доступности локатора. Получатель **должен** отвечать сообщением Map-Reply с установленным (1) битом probe-bit, указывающим, что Map-Reply является откликом на зонд доступности локатора, и копией nonce из Map-Request (см. параграф 7.1. Алгоритм зондирования RLOC). Такое сообщение RLOC-Probe Map-Request **недопустимо** передавать в Mapping System. Если Map-Resolver или Map-Server получает Map-Request с установленным битом probe-bit, он **должен** отбросить сообщение.

S

Флаг сообщения Solicit-Map-Request (SMR), см. параграф 6.1. Solicit-Map-Request (SMR).

P

Бит Proxy Ingress Tunnel Router (PITR), устанавливаемый (1) при передаче маршрутизатором PITR сообщения Map-Request. Использование этого бита зависит от развёртывания.

s

Бит вызова SMR, устанавливаемый (1) xTR при передаче Map-Request в ответ на Map-Request на основе SMR.

R

Резервный бит, который **должен** сбрасываться (0) при передаче, а получатель **должен** игнорировать его.

Rsvd

Это поле **должно** устанавливаться в 0 при передаче, а получатель **должен** игнорировать его.

L

Бит local-xtr, используемый xTR на сайте LISP для указания другим xTR того же сайта, что он является частью RLOC-Set для сайта LISP. Бит L устанавливается (1), когда RLOC является IP-адресом отправителя.

D

Бит dont-map-reply, используемый в процедуре SMR, описанной в параграфе 6.1. Когда xTR передаёт сообщение SMR, ему не требуется возврат Map-Reply. При установленном (1) бите получатель Map-Request не передаёт Map-Reply.

IRC

Это 5-битовое поле служит счётчиком ITR-RLOC Count, который указывает число дополнительных полей (ITR-RLOC-AFI, ITR-RLOC Address) в данном сообщении. **Должна** кодироваться хотя бы 1 пара (ITR-RLOC-AFI, ITR-RLOC Address). Применяется несколько полей ITR-RLOC Address, поэтому передающая Map-Reply сторона может выбрать адрес получателя для указания в Map-Reply. Значение IRC может быть от 0 до 31, 0 указывает наличие одного адреса ITR-RLOC, 1 - 2 ITR-RLOC и т. д. до 31 для указания 32 адресов ITR-RLOC.

Record Count

Число записей в сообщении Map-Request. Запись состоит из части пакета, помеченной на рисунке выше как Rec, которая повторяется Record Count раз. В этой версии протокола получатель **должен** воспринимать и обрабатывать сообщения Map-Request с одной или несколькими записями, но отправитель **должен** передавать Map-Request лишь с одной записью.

Nonce

8-октетное случайное значение, создаваемое отправителем Map-Request, которое будет возвращаться в Map-Reply. Значение nonce служит для идентификации соответствующего Map-Request при получении Map-Reply. Значение **должно** генерироваться генератором псевдослучайных чисел с подобающей затравкой (seed), например, [RFC4086].

Source-EID-AFI

Семейство адресов для поля Source EID Address.

Source EID Address

EID хоста-источника, создавшего пакет, который вызвал Map-Request. При использовании Map-Request для обновления записи Map-Cache или зондирования RLOC-Probing применяется AFI = 0 и это поле имеет размер 0.

ITR-RLOC-AFI

Семейство адресов для поля ITR-RLOC Address, которое следует за этим полем.

ITR-RLOC Address

Служит для предоставления ETR возможности выбора адреса получателя сообщения Map-Reply из любого семейства. Этот адрес **должен** быть маршрутизируемым адресом RLOC отправителя сообщения Map-Request.

EID mask-len

Размер маски для EID-Prefix.

EID-Prefix-AFI

Семейство адресов EID-Prefix в соответствии с [AFN] и [RFC8060].

EID-Prefix

Префикс адреса размером 4 октета для IPv4 и 16 октетов для IPv6 при EID-Prefix-AFI со значением 1 или 2, соответственно. Для других AFI [AFN] размер адреса меняется и для LCAF AFI формат задан в [RFC8060]. Если Map-Request передаётся ITR в результате приёма пакета данных для адресата, с которым не связана запись отображения, в качестве EID-Prefix устанавливается IP-адрес получателя пакета данных, а в поле EID mask-len — значение 32 для IPv4 или 128 для IPv6. Когда xTR хочет запросить у сайта статус отображения, которое уже кэшировано, EID-Prefix в Map-Request имеет такой же размер маски, что и префикс EID-Prefix, возвращённый сайтом при отправке сообщения Map-Reply.

Map-Reply Record

При установленном (1) бите M это поле содержит размер одной записи (Record) в формате Map-Reply. Эта запись Map-Reply содержит отображение EID на RLOC, связанное с EID источника. Это позволяет ETR, получившему этот Map-Request, кэшировать данные по своему усмотрению. Важно отметить, что это отображение Mapping System не проверяет.

5.3. Сообщение EID-RLOC UDP Map-Request

ITR передаёт Map-Request, когда ему нужно отображение для EID, проверка доступности RLOC или обновление отображения до завершения срока действия (Time to Live или TTL). В первом случае IP-адресом получателя Map-Request является адрес получателя пакета (EID получателя), который не удалось найти в кэше отображений. В двух других случаях IP-адресом получателя Map-Request является один из адресов RLOC из Locator-Set записи Map-Cache. Адресом отправителя является адрес IPv4 или IPv6 RLOC в зависимости использования в Map-Request заголовка IPv4 или IPv6. Во всех случаях номер порта UDP у источника для сообщения Map-Request является 16-битовым значением, выбранным ITR/PITR, а для порта отправителя UDP устанавливается общеизвестный номер 4342. Получение Map-Reply с nonce, соответствующим nonce в остающемся Map-Request, будет обновлять кэшированный набор RLOC, связанных с EID-Prefix.

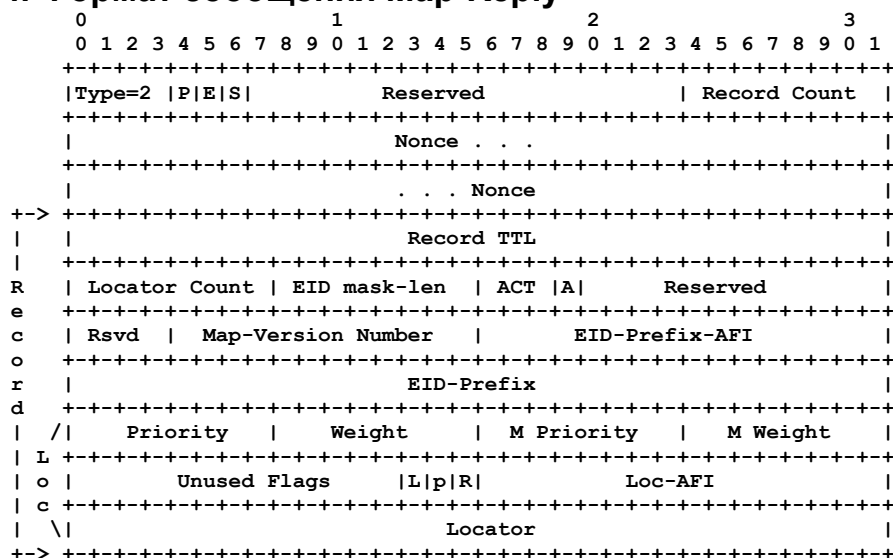
ITR **должен** указать в Map-Request одно или несколько полей (ITR-RLOC-AFI, ITR-RLOC Address). Число полей за вычетом 1 **должно** указываться в поле IRC. ITR **может** включить в этот список все локально настроенные локаторы или указать 1 Routing Locator Address для каждого поддерживаемого семейства адресов. Если ITR по ошибке не указал адресов ITR-RLOC, передающая Map-Reply сторона **должна** отбросить Map-Request.

Сообщения Map-Request можно инкапсулировать в LISP с использованием порта получателя UDP 4342 и LISP Type Encapsulated Control Message при передаче от ITR к Map-Resolver. Точно так же сообщения Map-Request инкапсулируются в LISP при передаче от Map-Server в ETR. Подробности представлены в параграфе 5.8.

Частота передачи Map-Request **должна** ограничиваться 1 сообщением в секунду на EID-Prefix. После 10 повторов без получения Map-Reply, отправитель **должен** установить паузу в 30 секунд.

ITR, настроенный со сведениями из базы отображений (т. е., являющийся также ETR), **может** включать эти отображения в Map-Request. Когда ETR, настроенный на восприятие и проверку таких (piggybacked) данных отображения, получает такой Map-Request и не имеет этого отображения в Map-Cache, он **должен** инициировать проверочное сообщение Map-Request через базу данных отображений.

5.4. Формат сообщения Map-Reply



Type

2 (Map-Reply)

P

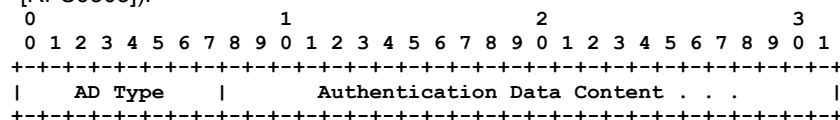
Бит зондирования (probe-bit), указывающий, что сообщение Map-Reply является откликом на Map-Request зондирования доступности локатора **должно** считаться зондом доступности локатора. Поле Nonce должно отвечать сообщением Map-Reply с установленным (1) битом probe-bit, указывающим, что Map-Reply является содержать копию nonce из исходного Map-Request (см. параграф 7.1. Алгоритм зондирования RLOC). При установленном (1) флаге probe-bit в сообщении Map-Reply бит A в каждой записи EID-Record, включённой в сообщение, **должен** иметь значение 1, в противном случае сообщение **должно** просто отбрасываться.

E

Указывает, что ETR, передающий это сообщение Map-Reply, анонсирует поддержку на сайте алгоритма проверки доступности локаторов Echo-Nonce (см. параграф 10.1 в [RFC9300]).

S

Бит защиты (Security), при установке (1) которого добавляются показанные ниже сведения в конце Map-Reply (см. [RFC9303]).



Reserved

Это поле **должно** устанавливаться в 0 при передаче, а получатель **должен** игнорировать его.

Record Count

Число записей в отклике. Запись состоит из части пакета, помеченной на рисунке выше как Record, которая повторяется Record Count раз. Отметим, что число записей в отклике может превышать число записей в запросе, например, при наличии более конкретных префиксов.

Nonce

64-битовое значение из Map-Request, копируемое в Map-Reply.

Record TTL

Число минут, в течение которых получатель Map-Reply может сохранять отображение. Значение 0xffffffff позволяет получателю самому определять срок хранения.

Locator Count

Число записей элементов Locator в данной записи Record. Элемент для локатора представляет собой часть, помеченную на рисунке выше как Loc. Счётчик может иметь значение 0, указывающее отсутствие локаторов для EID-Prefix.

EID mask-len

Размер маски для EID-Prefix.

ACT

3-битовое поле, описывающее действия Negative Map-Reply. В сообщениях иного типа устанавливается 0, а при получении поле игнорируется. Эти биты используются, когда поле Locator Count имеет значение 0. Биты действий указываются в сообщениях Map-Reply и говорят ITR или Pitr причину возврата пустого Locator-Set системой отображения и влияние отклика на Map-Cache (см. 12.3. Коды LISP Map-Reply EID-Record Action).

- (0) No-Action - Map-Cache сохраняется, инкапсуляции пакета не происходит.
- (1) Natively-Forward - пакет не инкапсулируется и не отбрасывается, а пересылается обычным способом.
- (2) Send-Map-Request - создаётся запись Map-Cache и помечается так, чтобы любой пакет, который соответствует ей, вызывал отправку Map-Request.
- (3) Drop/No-Reason - пакет, соответствующий этой записи Map-Cache, отбрасывается, при этом **следует** передавать сообщение ICMP Destination Unreachable.
- (4) Drop/Policy-Denied - пакет, соответствующий этой записи Map-Cache, отбрасывается. Причина заключается в том, что Map-Request для целевого EID отвергнут правилами xTR или Mapping System.
- (5) Drop/Auth-Failure - пакет, соответствующий этой записи Map-Cache, отбрасывается. Причина заключается в том, что запрос Map-Request для целевого EID не прошёл проверку подлинности в xTR или Mapping System.

A

Бит полномочий (authoritative), который **может** устанавливать (1) только ETR. Серверу Map-Server, создающему сообщения Map-Reply как посреднику, **недопустимо** устанавливать A = 1. Этот бит указывает запрашивающим ITR, исходит ли Map-Reply от узла LISP на сайте, владеющем EID-Prefix.

Map-Version-Number

12-битовое поле номера версии отображения в EID-Record сообщения Map-Reply (см. [RFC9302]).

EID-Prefix-AFI

Семейство адресов EID-Prefix в соответствии с [AFN] и [RFC8060].

EID-Prefix

4-октетный префикс для семейства адресов IPv4 или 16-октетный для IPv6.

Priority

Для каждого RLOC устанавливается значение Priority, меньшее значение указывает более высокий приоритет. Когда у нескольких RLOC значения Priority совпадают, их можно применять для распределения нагрузки. Значение 255 указывает, что RLOC **недопустимо** использовать для пересылки индивидуальных пакетов.

Weight

При совпадении приоритета у нескольких RLOC значение Weight задаёт долю индивидуального трафика между ними. Вес кодируется как относительная доля unicast-пакетов, соответствующих записи отображения. Например, при наличии в Locator-Set 4 локаторов с Weight 30, 20, 20 и 10 первый локатор получит 37,5% трафика, второй и третий - по 25%, а четвёртый - 12,5%. Если все значения Weight для Locator-Set совпадают, получатель Map-Reply сам принимает решение о распределении трафика. В разделе 12 [RFC9300] предложен алгоритм хэширования для распределения трафика между локаторами с одинаковыми значениями Priority и Weight.

M Priority

Для каждого RLOC назначается групповой приоритет, используемый ETR на принимающем multicast-трафике сайте для выбора ITR на групповом сайте-источнике при построении деревьев распространения группового трафика. Значение 255 указывает, что RLOC **недопустимо** использовать для присоединения к multicast-дереву (см. [RFC6831]).

M Weight

При совпадении приоритета у нескольких RLOC значение Weight задаёт распределение трафика при построении multicast-деревя с несколькими ITR. Вес указывает относительную долю (как unicast Weight) от общего числа деревьев, строящихся к сайту-источнику, заданному EID-Prefix. Если все веса в Locator-Set совпадают, получатель Map-Reply будет сам распределять групповой трафик между ITR (см. [RFC6831]).

Unused Flags

Это поле устанавливается в 0 при передаче и игнорируется получателем.

L

Установка этого бита помечает локатор как локальный для ETR, передающего Map-Reply. Когда Map-Server служит посредником для Map-Reply сайта LISP, бит L сбрасывается (0) для всех локаторов этого Locator-Set.

P

Когда этот бит установлен, ETR информирует маршрутизатор ITR, передающий RLOC-Probe, о том, что адрес локатора маршрутизации, для которого этот бит установлен, является одним из проверяемых с помощью RLOC-Probe и может отличаться от адреса отправителя Map-Reply. ITR, использующий RLOC-Probe для конкретного локатора, **должен** использовать этот Locator для извлечения структуры данных, служащей для хранения факта достижимости этого локатора. Бит p устанавливается для одного локатора в одном Locator-Set. Если реализация по ошибке установит несколько флагов p, получатель Map-Reply **должен** выбирать первый локатор с установленным битом p. Флаг p **недопустимо** устанавливать для записей Locator-Set, передаваемых в сообщениях Map-Request и Map-Register.

R

Устанавливается, когда отправитель Map-Reply имеет маршрут к локатору в записи данных Locator. Этому получателю может быть полезно знать, активен (up) ли локатор, с точки зрения получателя (не обязательно достижим).

Locator

Адрес IPv4 или IPv6 (в соответствии с полем Loc-AFI), назначенный ETR и используемый ITR в качестве RLOC получателя во внешнем заголовке пакета с инкапсуляцией LISP. Отметим, что RLOC получателя в пакете с инкапсуляцией LISP **может** быть anycast-адресом, равно как RLOC отправителя пакета с инкапсуляцией LISP. В качестве RLOC отправителя или получателя **недопустимо** применять широковещательный адрес (255.255.255.255 или иной широковещательный адрес подсети, известный маршрутизатору) и ему **недопустимо** быть групповым адресом link-local. В качестве RLOC отправителя **недопустим** групповой адрес. Для RLOC получателя **следует** указывать групповой адрес, если он сопоставлен с групповым EID получателем.

Частота передачи сообщений Map-Reply **должна** ограничиваться и **рекомендуется** передавать Map-Reply с одним RLOC получателя не чаще 1 раза за три секунды.

Формат Record, указанный здесь, включая определения всех полей, применяется в сообщениях Map-Reply и Map-Register.

5.5. Сообщение EID-RLOC UDP Map-Reply

Map-Reply возвращает EID-Prefix с размером маски не более запрошенного EID из поля адреса получателя в заголовке IP пакета Data-Probe или EID записи Map-Request. RLOC в Map-Reply являются маршрутизируемыми адресами IP всех ETR для сайта LISP. Каждый RLOC сообщает статус своей доступности, но не сообщает статус доступности пути с точки зрения запрашивающего, поэтому для пути нужна отдельная проверка (см. 7.1. Алгоритм зондирования RLOC).

Отметим, что в Map-Reply **может** использоваться детализация EID-Prefix (префикс и размер маски), отличающаяся от указанной в вызвавшем отклик сообщении Map-Request. Это может быть обусловлено отправкой Map-Request для префикса, возвращённого в предшествующем Map-Reply. В таком случае запрашивающий обновляет свой кэш новыми сведениями для префикса. Например, запрашивающий с двумя эшированными EID-Prefix, охватываемыми Map-Reply с менее конкретным префиксом, заменяет свою запись этим менее конкретным EID-Prefix. Отметим, что возможна и обратная ситуация с включением нескольких более конкретных префиксов без удаления менее конкретного, поскольку при поиске возвращается более конкретный префикс.

При переносе EID за пределы сайта LISP [EID-MOBILITY], в базе данных Mapping System могут возникать перекрывающиеся EID-Prefix. Аналогичная ситуация может возникать при настройке на сайте LISP нескольких наборов ETR, поддерживающих различные размеры масок EID-Prefix. При перекрытии EID-Prefix сообщение Map-Request для EID **должно** возвращать EID-Prefix с максимальным соответствием в сообщении Map-Reply. Например, если ETR имеет записи отображений для EID-Prefix

```
2001:db8::/32
2001:db8:1::/48
2001:db8:1:1::/64
2001:db8:1:2::/64
```

Map-Request для EID 2001:db8:1:1::1 будет приводить к получению Map-Reply с одной записью EID-Prefix 2001:db8:1:1::/64. Map-Request для EID 2001:db8:1:5::5 будет возвращать Map-Reply с 3 записями для EID-Prefix 2001:db8:1::/48, 2001:db8:1:1::/64, 2001:db8:1:2::/64, заполняя /48 более конкретными префиксами из Mapping System.

Отметим, что возвращать требуется не все перекрывающиеся EID-Prefix, а лишь более конкретные (во втором примере выше префикс 2001:db8::/32 не был возвращён для запроса EID 2001:db8:1:5::5) для EID-Prefix из запроса EID. При возврате более одного EID-Prefix для всех **следует** использовать одно значение TTL, чтобы срок их действия завершался одновременно. При получении позднее более конкретного EID-Prefix его значение TTL в записи Map-Reply может быть сохранено даже при наличии менее конкретных записей. При получении позднее менее конкретного EID-Prefix время завершения Map-Cache **следует** установить в соответствии с минимальным временем завершения более конкретного EID-Prefix в Map-Cache. Это делается для сохранения целостности набора EID-Prefix, чтобы из Map-Cache не удалялись более конкретные записи при сохранении менее конкретных.

Предполагается, что с точки зрения расширяемости агрегирование адресов EID в префиксы EID-Prefixes позволит одному сообщению Map-Reply соответствовать отображению адресов EID в диапазоне префиксов, снижая число сообщений Map-Request.

Записи Map-Reply могут включать пустой набор Locator-Set. Сообщение Negative Map-Reply - это Map-Reply с пустым Locator-Set. Такие сообщения Map-Reply передают специальные действия отправителя Map-Reply маршрутизаторам ITR и Pitr, которые запросили Map-Reply. Имеется два основных применения Negative Map-Reply. Во-первых, Map-Resolver указывает ITR или Pitr, когда адресат является сайтом LISP (в отличие от прочих), а во-вторых, для подавления источников Map-Request, передающих невыделенные EID.

Для каждой записи Map-Reply список локаторов в Locator-Set **должен** сортироваться в порядке роста адресов IP, при этом адреса IPv4 считаются численно меньшими по сравнению с адресами IPv6.

При передаче сообщения Map-Reply адрес получателя копируется из одного из полей ITR-RLOC в Map-Request. ETR может выбрать адрес локатора маршрутизации одного из семейств адресов, которые он поддерживает. Для Data-Probe адрес получателя Map-Reply копируется из поля отправителя сообщения Data-Probe, вызвавшего отклик. Адресом отправителя Map-Reply является один из локальных адресов IP, это позволяет применять индивидуальную проверку пересылки по обратному пути (Unicast Reverse Path Forwarding или uRPF) для восходящего поставщика услуг. Порт получателя Map-Reply копируется из поля порта отправителя сообщения Map-Request или Data-Probe, а для порта отправителя Map-Reply устанавливается стандартное значение UDP 4342.

5.6. Формат сообщения Map-Register

Ф этот параграфе задан формат кодирования сообщений Map-Register. Сообщения передаются в порт UDP 4342 из выбранного случайно порта UDP.

Показанные ниже поля применяются в нескольких типах сообщений и определены для Map-Register, Map-Notify, Map-Notify-Ack.

```

0      1      2      3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|Type=3|P|S|I|I|      Reserved      |E|T|a|R|M|Record Count|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                           Nonce . . . |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                           . . . Nonce |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|Key ID |Algorithm ID |Authentication Data Length|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
~                                           Authentication Data ~
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
+> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
R |Locator Count|EID mask-len|ACT|A|Reserved|
e +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
c |Rsvd |Map-Version Number|EID-Prefix-AFI|
o +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
r |EID-Prefix|
d +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|/|Priority|Weight|M Priority|M Weight|
|L +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|o|Unused Flags|L|p|R|Loc-AFI|
|c +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| \ |Locator|
+> +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type

3 (Map-Register)

P

Флаг посредника для Map-Reply. Установка (1) флага показывает, что ETR, передавший Map-Register, запросил у Map-Server посредничество для Map-Reply. Map-Server передаёт неполномочные Map-Reply от имени ETR.

S

Бит поддержки защиты, установка (1) которого включает поддержку процедур [RFC9303].

I

Бит присутствия идентификатор, установка (1) которого показывает наличие 128-битового поля xTR-ID и 64-битового Site-ID в конце сообщения Map-Register. Если xTR настроен с xTR-ID и Site-ID, он **должен** устанавливать I=1 и включать свои xTR-ID и Site-ID в создаваемые сообщения Map-Register. Комбинация Site-ID и xTR-ID однозначно указывает xTR в домене LISP и служит для отслеживания его последнего nonce.

Reserved

Это поле **должно** устанавливаться в 0 при передаче, а получатель **должен** игнорировать его.

E

Бит уведомления EID Map-Register, используемый первым (First-Hop) маршрутизатором, обнаружившим динамический адрес EID. Это сообщение Map-Register на основе EID-notify передаётся первым маршрутизатором xTR того же сайта, распространяющему Map-Register в Mapping System. Сайт xTR сохраняет состояние последнего Map-Notify первого маршрутизатора после удаления EID (см. подробности применения в [EID-MOBILITY]).

T

Флаг использования TTL для тайм-аута. Установка (1) флага указывает, что xTR хочет, чтобы Map-Server прерывал регистрацию на основе значения поля Record TTL в этом сообщении. В ином случае применяется заданный по умолчанию тайм-аут (8.2. Настройка EID-Prefix и регистрация ETR).

a

Бит слияния, установка (1) которого показывает, что xTR запрашивает слияние записей RLOC-Record от разных xTR, регистрирующих одну и ту же запись EID-Record (см. пример использования в [RFC8378]).

R

Резервный бит, который **должен** сбрасываться (0) при передаче, а получатель **должен** игнорировать его.

M

Бит want-map-notify, установка (1) которого показывает, что ETR запрашивает возврат сообщения Map-Notify в ответ на Map-Register. Сообщение Map-Notify от Map-Server служит подтверждением приёма Map-Register.

Record Count

Число записей в Map-Register. Запись состоит из части пакета, помеченной на рисунке выше как Record, которая повторяется Record Count раз.

Nonce

Это 8-октетное поле Nonce инкрементируется при каждой отправке сообщения Map-Register. При запросе подтверждения Map-Register значение nonce серверы Map-Server возвращают в сообщениях Map-Notify. Поскольку проверяется подлинность всего сообщения Map-Register, поле Nonce служит для защиты от атак с повторным использованием Map-Register (replay). ETR при регистрации в Mapping System **следует** сохранять последнее значение nonce в постоянном хранилище, чтобы при перезапуске можно было продолжать использование инкрементируемых nonce. Если ETR не может сохранить nonce, то при перезапуске он **должен** использовать новый ключ аутентификации для регистрации в Mapping System. Map-Server **должен** отслеживать и записывать в постоянное хранилище последнее значение nonce, принятое для каждой пары ETR xTR-ID и ключа. При получении Map-Register со значением nonce, которое не превышает сохранённое значение сервер **должен** отбрасывать сообщение Map-Register и **следует** записывать это в системный журнал, как возможную replay-атаку.

Key ID

Значение key-id, указывающее заранее распространённый секрет для ETR и Map-Server. Ключи для каждого сообщения выводятся из этого секрета для аутентификации источника и защиты целостности Map-Register. Key ID позволяет менять заранее распространённые секреты без нарушения работы. Секрет **должен** быть уникальным для каждого LISP Site-ID.

Algorithm ID

Указывает алгоритмы функции вывода ключа (Key Derivation Function и KDF) и кода аутентификации сообщений (Message Authentication Code или MAC), применяемые для создания ключа и расчёта данных аутентификации (Authentication Data) для Map-Register. Это 8-битовое поле указывает пару KDF и алгоритма MAC, возможные значения указаны в параграфе 12.5. Номера LISP Algorithm ID.

Authentication Data Length

Число октетов следующего поля Authentication Data. Размер Authentication Data зависит от применяемого алгоритма MAC. Это поле позволяет корректно анализировать пакет устройству, не знающему алгоритм MAC.

Authentication Data

Вывод алгоритма MAC, помещаемый после расчёта, описанного ниже.

1. Алгоритм KDF указывается полем Algorithm ID в соответствии с таблицей 5. Реализации этой спецификации **должны** поддерживать HMAC-SHA-256-128 [RFC4868] и следует поддерживать HMAC-SHA-256-128+HKDF-SHA256 [RFC5869].
2. Алгоритм MAC указывается полем Algorithm ID в соответствии с таблицей 5.
3. Выводится ключ для сообщения из заранее распространённого секрета, указанного PSK[Key ID].
4. Ключ для сообщения выводится как $\text{per-msg-key} = \text{KDF}(\text{nonce} + \text{PSK}[\text{Key ID}], s)$, где nonce - значение поля Nonce из Map-Register, + означает конкатенацию, а s (salt) указывает строку, соответствующую типу аутентифицируемого сообщения. Для Map-Register это Map-Register Authentication, для Map-Notify и Map-Notify-Ack - Map-Notify Authentication и Map-Notify-Ack Authentication, соответственно. Для Algorithm ID, из таблицы 5, задающих для KDF значение nonce, ключ сообщения создается как $\text{per-msg-key} = \text{PSK}[\text{Key ID}]$. Это означает использование одного ключа для разных сообщений протокола.
5. Вывод MAC рассчитывается с применением алгоритма MAC и ключа для сообщения ко всему содержимому (payload) сообщения Map-Register (начиная с поля типа сообщения LISP до конца последней записи RLOC-Record). Для поля данных аутентификации при расчёте принимается значение 0.

Определения оставшихся полей Map-Register приведены в описании EID-Record (5.4. Формат сообщения Map-Reply). При установленном (1) бите I в конец сообщения Map-Register добавляются указанные ниже поля.

xTR-ID

128-битовое поле в конце сообщения Map-Register вслед за последним полем Record. xTR-ID служит для однозначного указания xTR и **недопустимо** применять 1 значение для разных xTR в области действия Site-ID.

Site-ID

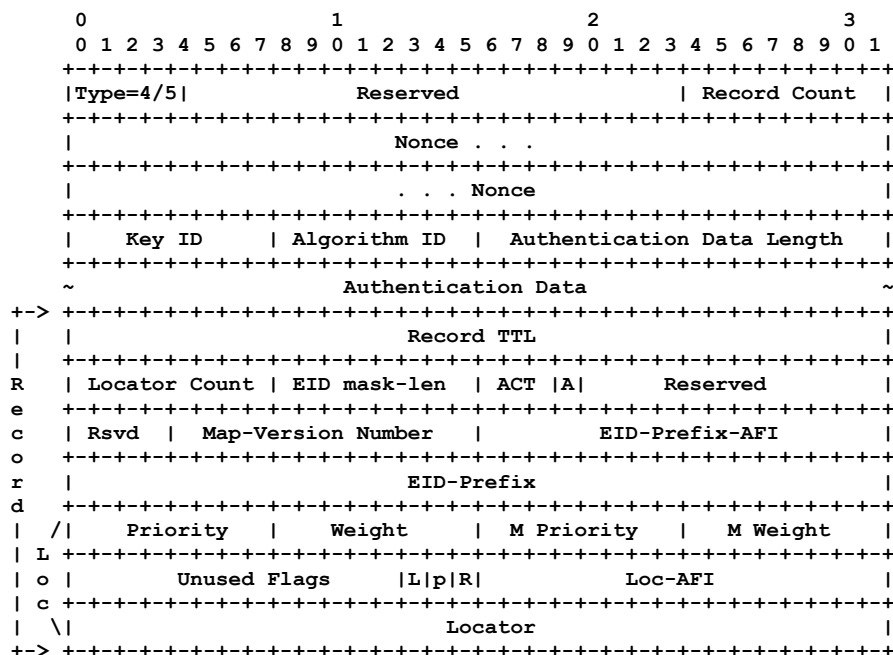
64-битовое поле в конце сообщения Map-Register вслед за xTR-ID. Site-ID служит для однозначного указания сайта, к которому относится xTR, передающий сообщение. Этот документ не задаёт смысл поля Site-ID строго.

Неформально оно указывает группу xTRs, как-то связанных между собой административно, топологически или иначе.

5.7. Формат сообщений Map-Notify и Map-Notify-Ack

This section specifies the encoding format for the Map-Notify and Map-Notify-Ack messages. The messages are sent inside a UDP packet with source and destination UDP ports equal to 4342.

The Map-Notify and Map-Notify-Ack message formats are:



Type

4/5 (Map-Notify/Map-Notify-Ack)

Сообщения Map-Notify по составу содержимого совпадают с Map-Register. Описания полей приведены в параграфе 5.6. Формат сообщения Map-Register, а описания EID-Record и RLOC-Record - в 5.4. Формат сообщения Map-Reply.

Поля Map-Notify копируются из соответствующего сообщения Map-Register для подтверждения корректной обработки. В Map-Notify поле Authentication Data рассчитывается заново с использованием соответствующего ключа сообщения по процедуре, описанной в предыдущем параграфе. Сообщения Map-Notify могут передаваться без запроса, но это выходит за рамки документа (см. [LISP-PUBSUB]).

Если после отправки Map-Register сообщение Map-Notify не было получено в течение 1 секунды, передающая сторона **должна** повторять передачу исходного Map-Register с экспоненциально растущим интервалом повтора (с базой 2, т. е. удвоением интервала перед каждым повтором) вплоть до 1 минуты. Сообщения Map-Notify передаются лишь при получении Map-Register с установленным флагом M и не повторяются. Единственным исключением являются незапрошенные сообщения Map-Notify (см. ниже).

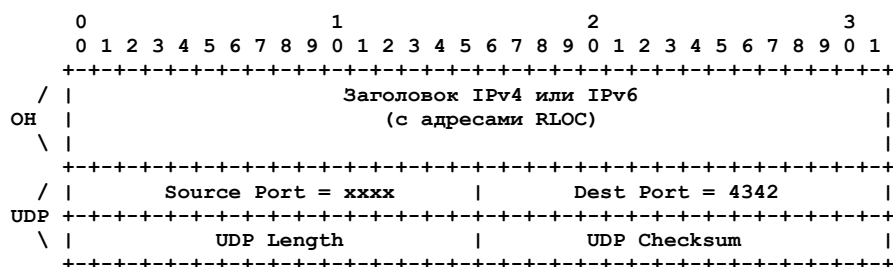
Map-Server передаёт незапрошенное сообщение Map-Notify (т. е. не являющееся подтверждением Map-Register) лишь в соответствии с параграфами 3.1 и 3.3 в [RFC8085]. Передача Map-Notify повторяется, пока Map-Server не получит Map-Notify-Ack с тем же nonce, что и в сообщении Map-Notify. Реализациям **следует** повторять передачу до 3 раз с интервалом 3 секунды, после чего интервал повтора следует экспоненциально увеличивать (вдвое при каждом следующем повторе) до 3 раз. Сообщения Map-Notify-Ack передаются лишь при получении незапрошенного Map-Notify и не повторяются.

Содержимое Map-Notify-Ack совпадает с содержимым Map-Notify. Сообщение служит подтверждением приёма незапрошенного Map-Notify и, поскольку Authentication Data проверяются, позволяет отправителю остановить повтор Map-Notify с теми же nonce и (проверенными) Authentication Data. Поля Map-Notify-Ack копируются из соответствующего Map-Notify для подтверждения корректной обработки. Поле Authentication Data рассчитывается заново с использованием соответствующего ключа сообщения по процедуре, описанной в предыдущем параграфе.

При получении Map-Register, Map-Notify или Map-Notify-Ack получатель проверяет Authentication Data и при отказе отбрасывает сообщение без дальнейшей обработки.

5.8. Формат инкапсулированного управляющего сообщения

Инкапсулированные управляющие сообщения (Encapsulated Control Message или ECM) применяются для инкапсуляции пакетов управления, передаваемых между xTR и системой отображения.



www.protokols.ru

передавать данных на сайт. Нет смысла обновлять ITR, пока им не нужно ничего передавать, а перед передачей можно отправить Map-Request для получения записи.

7. Доступность локаторов маршрутизации

Этот документ задаёт несколько механизмов плоскости управления для проверки доступности RLOC. В [RFC9300] определены механизмы проверки доступности в плоскости данных.

1. ITR может получать сообщения ICMP Network Unreachable или Host Unreachable для используемых RLOC, указывающие недоступность адреса. Отметим, что сообщениям ICMP не всегда можно доверять, но игнорировать их полностью не следует. Реализациям рекомендуется следовать основанной на опыте трактовке таких сообщений, описанной в [OPSEC-ICMP-FILTER].
2. При участии ITR в протоколе маршрутизации базовой сети, он может определить недоступность RLOC по отсутствию в базе маршрутных сведений (Routing Information Base или RIB) записи для IP-адреса RLOC.
3. ITR может получить от целевого хоста сообщение ICMP Port Unreachable. Это может происходить при использовании ITR взаимодействия [RFC6832] с передачей пакетов LISP сайту, не поддерживающему LISP.
4. ITR может получить отклик Map-Reply от ETR в ответ на переданное сообщение Map-Request. RLOC источника Map-Reply вероятно будет активен (up), поскольку ETR удалось передать Map-Reply маршрутизатору ITR. Следует отметить, что в некоторых случаях значение RLOC из внешнего заголовка может быть подменено.
5. Пара ITR - ETR может использовать описанный ниже механизм зондирования RLOC-Probing.

Когда ITR получают сообщения ICMP Network Unreachable или Host Unreachable как метод определения недоступности, они будут воздерживаться от использования локаторов из списков сообщений Map-Reply. Однако такой подход ненадёжен, поскольку многие сетевые операторы отключают генерацию сообщений ICMP Destination Unreachable.

Если ITR получает сообщение ICMP Network Unreachable или Host Unreachable, он **может** создать своё сообщение ICMP Destination Unreachable для хоста, создавшего пакет данных, инкапсулированный ITR.

Это допущение создаёт зависимость - недоступность локатора обнаруживается получением сообщений ICMP Host Unreachable. Когда Locator считается недоступным, он не используется для активного трафика, как будто был указан в Map-Reply с Priority = 255.

ITR может проверить доступность локатора, периодически отправляя Map-Request. Частота отправки сообщений Map-Request и Map-Reply должна ограничиваться (см. 5.3. Сообщение EID-RLOC UDP Map-Request и 5.4. Формат сообщения Map-Reply). Тестирование доступности локаторов никогда не выполняется с пакетами данных, поскольку это повышает риск потерь для сквозных сессий.

7.1. Алгоритм зондирования RLOC

RLOC-Probing - это метод, который ITR и PITR могут применять для определения статуса доступности одного или нескольких локаторов в записи Map-Cache. Для этого служит флаг probe-bit в сообщениях Map-Request и Map-Reply.

RLOC-Probing выполняется в плоскости управления по таймеру, а ITR или PITR передаёт Map-Request для адреса локатора с одного из своих адресов RLOC. Map-Request в качестве RLOC-Probe **не** инкапсулируется и **не** передаются Map-Server или базе данных отображений как при запросе отображения. EID-Record в Map-Request является EID-Prefix из записи Map-Cache на ITR или PITR. ITR **может** включить запись данных отображения из своих сведений о сопоставлениях, содержащую локальные EID-Prefix и RLOC для сайта. RLOC-Probe передаются периодически с внесением вариаций в интервал отправки.

Когда ETR получает Map-Request с установленным флагом probe-bit, он возвращает Map-Reply с таким же флагом. В качестве адреса отправителя Map-Reply указывается IP-адрес исходящего интерфейса, на который маршрутизируется адрес получателя Map-Reply. В Map-Reply **следует** включать данные отображения для EID-Prefix из Map-Request. Это позволяет ITR и PITR передавать RLOC-Probe для получения обновлений отображений, если они возникли с записей базы сопоставлений ETR.

Метод RLOC-Probing имеет преимуществ и недостатки. Основным преимуществом является возможность работы при разных отказах, что позволяет ITR определить, когда путь к конкретному локатору доступен или стал недоступным, обеспечивая надёжный способ переключения на другой локатор. RLOC-Probing может также давать приблизительную оценку времени кругового обхода (Round-Trip Time или RTT) между парой локаторов, что может быть полезно для функций управления сетью, а также для выбора пути с меньшей задержкой. Основным недостатком RLOC-Probing является большое число управляющих сообщений и расход пропускной способности для получения упомянутых преимуществ, особенно при жёстких требованиях в времени обнаружения отказов.

8. Взаимодействие с другими компонентами LISP

8.1. Распознавание отображения ITR EID-RLOC

На ITR настраивается 1 или несколько адресов Map-Resolver, которые служат локаторами (RLOC) и должны быть маршрутизируемыми в базовой сети ядра. Для этих адресов недопустимо требовать распознавания через отображения LISP EID-RLOC, поскольку это будет создавать циклические зависимости. При использовании Map-Resolver маршрутизатору ITR не требуется соединение с другими базами данных Mapping System.

ITR передаёт инкапсулированный Map-Request настроенному Map-Resolver, когда ему нужно отображение EID-RLOC, отсутствующее в его локальном Map-Cache. Использование Map-Resolver сильно сокращает сложности реализации ITR и поддержки, связанные с его работой.

В ответ на инкапсулированное сообщение Map-Request маршрутизатор ITR может получить один из указанных ниже вариантов.

- Незамедлительный отклик Negative Map-Reply (с кодом действия Natively-Forward и 15-минутным TTL) от Map-Resolver, если тот может определить, что запрошенного EID не существует. ITR сохраняет EID-Prefix, возвращённый в Map-Reply в своём кэше, помечает его как не поддерживающий LISP и знает, что не нужно пытаться инкапсулировать в LISP пакеты для этого префикса.
- Negative Map-Reply (с кодом действия Natively-Forward) от Map-Server, полномочного (внутри развёртывания LISP, см. параграф 1.1. Сфера применимости) для EID-Prefix, соответствующего запрошенному EID, но не имеющего активно зарегистрированного более конкретного EID-Prefix. В этом случае говорят, что запрошенный EID соответствует «дыре» (hole) в полномочном префиксе. Если запрошенный EID соответствует более конкретному EID-Prefix, чем был делегирован серверу Map-Server, для которого не зарегистрировано ETR, возвращается 1-минутное значение TTL. Если запрошенный EID соответствует неделегированной части полномочного EID-Prefix, это не LISP EID и возвращается 15-минутное значение TTL. Подробное обсуждение делегирования EID-Prefix и детали сопоставления префиксов в Map-Server рассмотрены в параграфе 8.2. Настройка EID-Prefix и регистрация ETR.
- LISP Map-Reply от ETR, владеющего отображением EID-RLOC, или от Map-Server, отвечающего от имени ETR. Более подробно обработка сообщений в Map-Resolver описана в параграфе 8.4. Обработка в Map-Resolver.

Отметим, что ITR можно настроить как на использование Map-Resolver, так и на участие в логической сети LISP-ALT. В такой ситуации ITR **следует** передавать Map-Request через сеть ALT для любого EID-Prefix, полученного от ALT BGP. Такая конфигурация предполагается очень редкой, так как от применения Map-Resolver мало пользы, если ITR уже применяет LISP-ALT. Например, такому ITR не требуется передавать Map-Request для возможно несуществующего EID (и полагаться на Negative Map-Reply), если он может обратиться к базе данных ALT для проверки наличия EID-Prefix до отправки Map-Request.

8.2. Настройка EID-Prefix и регистрация ETR

ETR публикует свои EID-Prefix на Map-Server, передавая сообщения LISP Map-Register. Сообщения Map-Register включает данные аутентификации (AD), поэтому перед их отправкой ETR и Map-Server **должны** получить общий секрет, используемый для вывода ключей аутентификации Map-Register. В конфигурацию Map-Server **следует** также включать список EID-Prefix, для которых ETR имеет полномочия. После получения Map-Register от ETR сервер будет воспринимать лишь настроенные для этого ETR префиксы EID-Prefix. Отказ от реализации такой проверки сделает систему отображения уязвимой для тривиальных атак с захватом EID-Prefix.

В дополнение к набору EID-Prefix для каждого ETR, который может быть зарегистрирован, на Map-Server обычно настраивается один или несколько агрегированных префиксов, указывающих части выделенного ему пространства EID. При использовании базы данных LISP-ALT агрегированные префиксы реализуются как маршруты отбрасывания и анонсируются в ALT BGP. Наличие агрегированных EID-Prefix в базе данных Map-Server означает, что сервер может получать Map-Request для EID-Prefix, которые соответствуют агрегату, но не соответствуют зарегистрированному префиксу. Обработка таких ситуаций описана в параграфе 8.3. Обработка в Map-Server.

Сообщения Map-Register передаются периодически от ETR на Map-Server с рекомендуемым интервалом в 1 минуту. Серверу **следует** удалять регистрацию ETR по тайм-ауту, если он не получил от него действительного сообщения Map-Register в течение 3 минут. При первом контакте с Map-Server после перезапуска или смене отображений в своей базе данных EID-RLOC маршрутизатор ETR **может** сначала передавать сообщения Map-Register более часто, вплоть до 1 каждые 20 секунд. Продолжительность интервала «ускоренной регистрации» ограничена 5 минутами.

ETR **может** запросить у Map-Server явное подтверждение приёма и обработки сообщения Map-Register, установив (1) флаг want-map-notify (M). Map-Server, получивший Map-Register с установленным флагом, будет отвечать сообщением Map-Notify. Обычно ETR будет устанавливать этот флаг в сообщениях Map-Register, передаваемых при начальной ускоренной регистрации на Map-Server, а затем применять его лишь время от времени при наличии установившейся ассоциации с этим Map-Server. Отметим, что сообщение Map-Notify передаётся в порт UDP 4342, а не в порт, из которого передано исходное сообщение Map-Register.

Отметим, что 1-минутный минимальный интервал регистрации при наличии поддерживаемой ассоциации ETR-Map-Server задаёт нижнюю границу скорости и частоты возможных обновления базы отображений. Это может влиять на типы напрямую поддерживаемой системой отображений мобильности - в некоторых случаях могут потребоваться более короткие интервалы или иные механизмы регистрации. Обсуждение способов реализации ускорения мобильности для индивидуальных устройств можно найти в [LISP-MN].

ETR **может**, устанавливая флаг проху Map-Reply (P) в сообщении Map-Register, запросить у Map-Server отклики на Map-Request вместо их пересылки ETR. В параграфе 7.1. Алгоритм зондирования RLOC описана установка сервером Map-Server некоторых флагов (таких, как указание полномочности сообщения и как **следует** трактовать возвращённые локаторы) при передаче Map-Reply от имени ETR. Когда ETR запрашивает услуги посредника для откликов, ему **следует** включать все RLOC для всех ETR регистрируемого EID-Prefix вместе с установкой флага маршрутизируемости (R) для каждого RLOC. Map-Server включает все эти сведения в сообщения Map-Reply, передаваемые от имени ETR. Это отличается от регистрации без посредника, поскольку та требует лишь предоставить 1 или несколько RLOC для Map-Server, применяемых при пересылке Map-Request, регистрационные сведения не используются в Map-Reply, поэтому неполнота информации не ведёт к ошибке.

ETR, использующему Map-Server для публикации своих отображений EID-RLOC, не требуется дальнейшее участие в протоколах баз данных отображений. При использовании базы отображений LISP-ALT это означает, например, что ETR не нужно реализовать GRE или BGP, что значительно упрощает настройку и эксплуатационные издержки.

Отметим, что использование Map-Server не препятствует подключению ETR к базе данных отображений (т. е. он может подключаться и к сети LISP-ALT), но это не представляется особо полезным, поскольку целью использования Map-Server является избавление от сложностей протоколов баз данных отображения.

8.3. Обработка в Map-Server

Когда Map-Server имеет EID-Prefix, зарегистрированные его клиентами ETR, он может воспринимать и обрабатывать сообщения Map-Request от них. При получении Map-Request сервер Map-Server сначала проверяет соответствие EID

получателя настроенному EID-Prefix. Если совпадений не найдено, Map-Server возвращает Negative Map-Reply с кодом действия Natively-Forward и 15-минутным TTL. Это может происходить при получении а Map-Request для настроенного агрегированного EID-Prefix, не имеющего более конкретного EID-Prefix, и указывает наличие «дыры», не поддерживающей LISP в агрегате EID-Prefix. Затем Map-Server проверяет наличие зарегистрированных ETR для соответствующего EID-Prefix. Если ничего не найдено, Map-Server возвращает Negative Map-Reply с кодом действия Natively-Forward и 1-минутным TTL.

Независимо от регистрации EID-Prefix в Mapping System при наличии на Map-Server правила отбрасывания запрашивающим пакетов для соответствующего EID-Prefix возвращается код действия Drop/Policy-Denied. Если возникает отказ при аутентификации (независимо от регистрации EID-Prefix), возвращается код действия Drop/Auth-Failure. Если любое из этих действий создаёт временное состояние политики или аутентификации, **может** возвращаться код действия Send-Map-Request с 1-минутным TTL, чтобы запрашивающий мог повторить Map-Request.

Если любой из ETR, зарегистрированных для EID-Prefix, запросил посредничество при ответе, Map-Server отвечает на запрос вместо его пересылки. Он возвращает Map-Reply с EID-Prefix, адресами RLOC и другими сведениями, полученными в процессе регистрации.

Если ни один из ETR не запрашивал посреднических услуг, Map-Server заново инкапсулирует и пересылает инкапсулированное сообщение Map-Request одному из зарегистрированных ETR. В остальном Map-Request не меняется, поэтому сообщение Map-Reply, переданное ETR, возвращается по RLOC из Map-Request, а не на Map-Server. Если сервер действует и как Map-Resolver, ему не следует получать сообщения Map-Reply и любое такое сообщение **следует** просто отбрасывать, возможно указывая это в системном журнале, если частота получения Map-Reply указывает вредоносный трафик.

8.4. Обработка в Map-Resolver

При получении инкапсулированного Map-Request распознаватель Map-Resolver деинкапсулирует вложенное сообщение и ищет запрошенный EID в локальной базе отображений (статической или полученной от связанных ETR, если Map-Resolver служит также посредничающим Map-Server). При наличии записи распознаватель возвращает LISP Map-Reply с найденным отображением.

Если у Map-Resolver нет записи отображения и распознаватель может определить, что EID нет в базе данных отображений (например, при использовании LISP-ALT у Map-Resolver может быть таблица пересылки ALT, охватывающая все пространство EID), он сразу же возвращает Negative Map-Reply с кодом действия Natively-Forward и 15-минутным TTL. Для минимизации числа кэшированных негативных записей, необходимых для ITR, распознавателю **следует** возвращать наименее конкретный префикс, соответствующий исходному запросу, но не соответствующий ни одному из EID-Prefix, наличие которых известно поддерживающей LISP инфраструктуре.

Если Map-Resolver не может узнать, существует ли EID, ему нужно переслать Map-Request другому устройству, у которого может быть больше сведений о запрошенном EID. Для этого он пересылает неинкапсулированное сообщение Map-Request с RLOC отправителя исходного ITR в систему баз данных отображений. Используя LISP-ALT, Map-Resolver подключается к сети ALT и передаёт Map-Request следующему узлу (hop) ALT, найденному среди соседей ALT BGP. Map-Resolver не передаёт ITR никакого отклика, поэтому в RLOC источника указывается этот ITR, ETR или Map-Server, получающий Map-Request через ALT и отвечающий напрямую маршрутизатору ITR.

8.4.1. Операции Anycast

Для Map-Resolver можно настроить использование anycast, когда один адрес назначается нескольким Map-Resolver и распространяется через маршрутизацию IGP для упрощения работы каждого ITR с более близким Map-Resolver.

ETR **могут** иметь anycast-адреса RLOC, зарегистрированные как часть их RLOC-Set в Mapping System. Однако регистрация **должна** использовать их уникальные адреса RLOC, разные ключи аутентификации или xTR-ID, чтобы различать защищённые связи с Map-Server.

9. Вопросы безопасности

Анализ угроз для LISP приведён в [RFC7835]. Здесь рассматриваются вопросы безопасности, связанные с применением LISP в средах, подобных описанным в параграфе 1.1, где соблюдаются указанные ниже допущения.

1. Mapping System защищена и является доверенной в плане безопасности, поэтому считается доверенным элементом.
2. На ETR заранее настроены отношения доверия с Mapping System, включая общие секреты в том или ином виде. Mapping System знает, какие EID может анонсировать ETR. Организация этих ключей и сопоставлений выходит за рамки документа.
3. **Должно** быть реализовано расширение LISP-SEC [RFC9303]. Сетевым операторам следует внимательно оценить применимость модели угроз LISP-SEC к их варианту применения и развёртыванию. Если оператор решить игнорировать те или иные рекомендации, ему следует убедиться в осознании связанных с этим рисков.

Обмен сообщениями Map-Request/Map-Reply злоумышленник может использовать для организации атак с усилением (amplification) или DoS-атак. Злоумышленники могут передавать Map-Request с высокой скоростью, чтобы перегрузить узлы LISP и увеличить число поддерживаемых узлов состояний или повысить нагрузку на CPU. Такие угрозы можно смягчить применением фильтров и ограничителей скорости.

Обмен сообщениями Map-Request/Map-Reply для внедрения фиктивных отображений непосредственно в ITR EID-RLOC Map-Cache, что может привести к перенаправлению трафика злоумышленнику (см. [RFC7835]). Кроме того, действительные ETR в системе могут выполнять атаки с перезаявлением (overclaiming). В этом случае злоумышленник может заявить свой EID-Prefix, который больше префикса, принадлежащего ETR. Эту проблему можно решить с помощью протокола LISP-SEC [RFC9303], определяющего механизм аутентификации источников, защиты целостности, а также предотвращение MITM¹-атак и перезаявления префиксов при обмене Map-Request/Map-Reply. Кроме того, зотя

¹Man-in-the-middle - перехват и изменение пакетов с участием человека.

это и выходит за рамки защиты отдельного Map-Server или Map-Resolver, следует отметить, что LISP-SEC можно дополнить механизмами защиты инфраструктуры Mapping System. Например, LISP-ALT [RFC6836] на основе BGP может применять стандартные средства BGP, а LISP-DDT [RFC8111] задаёт свои механизмы защиты.

Для публикации полномочного отображения EID-RLOC на Map-Server с помощью сообщения Map-Register маршрутизатор ETR включает данные аутентификации AD, которые представляют собой код MAC для всего сообщения с использованием ключа, выведенного из заранее распространённого секрета. Реализациям **следует** поддерживать алгоритм HMAC-SHA256-128+HKDF-SHA256 [RFC5869]. Сообщение Map-Register защищено от replay-атак с участием человека (MITM). Однако сохраняется возможность атак, в который скомпрометированный ETR может перезаявить префикс, которым он владеет, и зарегистрировать его на соответствующем Map-Server. Для смягчения таких атак, как отмечено в параграфе 8.2. Настройка EID-Prefix и регистрация ETR, Map-Server **должен** убедиться, что все EID-Prefix, регистрируемые ETR, соответствуют конфигурации, сохранённой на Map-Server.

Развёртывания, связанные с манипулированием сообщениями Map-Request и Map-Reply, а также перезаявлением EID-Prefix вредоносными ETR, **должны** отбрасывать сообщения плоскости управления LISP, не включающие материала LISP-SEC (бит S, EID-AD, OTK-AD, PKT-AD, см. раздел 3 в [RFC9303]).

Следует развёртывать механизмы шифрования, защиты приватности и предотвращения перехвата и фальсификации сообщений между маршрутизаторами xTRs, xTRs и Mapping System, а также между узлами, образующими Mapping System. Примерами таких механизмов могут служить DTLS [RFC9147] и lisp-crypto [RFC8061].

10. Вопросы приватности

Как отмечено в [RFC6973], вопросы приватности достаточно сложны и зависят от конкретного варианта применения протокола и развёртывания. В параграфе 1.1 [RFC9300] сказано, что LISP фокусируется на взаимодействии элементов через общедоступную сеть Internet при сохранении независимой адресации и топологии. Здесь рассматриваются угрозы приватности, создаваемые плоскостью управления LISP, на основе рекомендаций приведённых в [RFC6973].

LISP может применять долгоживущие идентификаторы (EID), которые связаны с перемещаемыми узлами. Такие идентификаторы привязываются к RLOC узлов. Адреса RLOC представляют топологическое размещение относительно конкретных развёртываний LISP. Кроме того, сопоставления EID с RLOC обычно считаются общедоступными сведениями внутри развёртывания LISP, где сообщения плоскости управления не шифруются и могут быть перехвачены при отправке сообщений Map-Request соответствующим Map-Resolver или Map-Register соответствующим Map-Server.

В этом контексте злоумышленник может сопоставить EID с RLOC и отслеживать топологическое размещение и перемещения соответствующего пользователя. Это может быть реализовано злоумышленниками вне пути (off-path), если они аутентифицированы, через запросы к Mapping System. Развёртывания, для которых такая угроза значима, могут использовать списки контроля доступа или более строгие механизмы аутентификации [ECDSA-AUTH] в Mapping System, чтобы доступ к сведениям получали лишь уполномоченные пользователи (минимизация данных). Применение эфемерных EID [EID-ANONYMITY] для обеспечения анонимности является другим механизмом предотвращения отслеживания.

11. Отличия от RFC 6830 и RFC 6833

Из соображений реализации в [RFC6830] и [RFC6833] были внесены перечисленные ниже изменения.

- 16-битовое поле Key ID в сообщениях Map-Register и Map-Notify, определённое в [RFC6830], было разделено на два 8-битовых поля - Key ID и Algorithm ID. Это изменение относится и к сообщению Map-Notify-Ack, заданному в этом документе (5.6. Формат сообщения Map-Register, 5.7. Формат сообщений Map-Notify и Map-Notify-Ack).
- В этом документе определено сообщение Map-Notify-Ack для обеспечения надёжности доставки Map-Notify. Получатель Map-Notify должен передавать в ответ сообщение Map-Notify-Ack. Серверы Map-Server, являющиеся отправителями Map-Notify, должны держать содержимое Map-Notify в очереди, пока не будет получено сообщение Map-Notify-Ack со значением nonce из этого Map-Notify. Отметим, что реализации Map-Notify-Ack уже имелись до выхода этого документа.
- В этом документе применяется код для сообщений Map-Referral из спецификации LISP-DDT [RFC8111], указывающий, что Map-Server должен передавать финальное сообщение Map-Referral, когда он участвует в процедурах LISP-DDT Mapping System.
- Добавлены флаги L и D для сообщений Map-Request (5.3. Сообщение EID-RLOC UDP Map-Request).
- Добавлены флаги S, I, E, T, a, R, M для сообщений Map-Register (5.6. Формат сообщения Map-Register).
- Поля nonce и Authentication Data в сообщении Map-Register ведут себя по-разному (5.6. Формат сообщения Map-Register).
- Этот документ добавляет два кода действий в EID-Record сообщений Map-Reply, Map-Register, Map-Notify и Map-Notify-Ack - Drop/Policy-Denied и Drop/Auth-Failure (5.4. Формат сообщения Map-Reply).

12. Взаимодействие с IANA

В этом разделе приведены рекомендации для IANA по части регистрации значений, связанных с этой спецификацией плоскости управления LISP, в соответствии с BCP 26 [RFC8126].

- Значения из реестра LISP IANA не следует выделять для целей, не связанных с маршрутизацией и транспортными протоколами LISP.
- Далее используются заданные в BCP 26 [RFC8126] процедуры Specification Required, IETF Review, Experimental Use, First Come First Served.

В LISP имеется 3 пространства регистрируемых имён (см. ниже) in LISP (см. [RFC9299]).

12.1. Номера портов LISP UDP

Агентство IANA выделило номер порта UDP 4342 для плоскости управления LISP и обновило описание этого порта, как показано в таблице 2

Таблица 2.

Имя службы	Номер порта	Транспортный протокол	Описание	Документ
lisp-control	4342	udp	Пакеты управления LISP	RFC 9301

12.2. Коды типа пакетов LISP

Агентство IANA теперь полномочно определять типы пакетов LISP, поэтому в реестре ссылки на [RFC6830] заменены указанием этого документа.

На основе опыта развёртывания, связанного с [RFC6830], в этом документе определено сообщение Map-Notify-Ack (тип 5), включённое в реестр, как показано в таблице 3.

Таблица 3.

Сообщение	Код	Документ
LISP Map-Notify-Ack	5	RFC 9301

12.3. Коды LISP Map-Reply EID-Record Action

Новые значения АСТ могут выделяться по процедуре IETF Review или IESG Approval. Четыре значения уже были выделены в [RFC6830]. Агентство IANA заменило ссылки на [RFC6830] указанием этого документа. Данная спецификация изменила имя для действия с кодом 3 с Drop на Drop/No-Reason. Новые действия и значения АСТ указаны в таблице 4.

Таблица 4. Значения LISP Map-Reply Action.

Значение	Действие	Описание	Документ
4	Drop/Policy-Denied	Пакет, соответствующий этой записи Map-Cache отброшен, поскольку целевой EID запрещён правилами xTR или Mapping System.	RFC 9301
5	Drop/Auth-Failure	Пакет, соответствующий этой записи Map-Cache отброшен, поскольку сообщение Map-Request для целевого EID не прошло проверку подлинности в xTR или Mapping System.	RFC 9301

В LISP имеется множество флагов и резервных полей, таких как поля и флаги заголовка LISP [RFC9300]. Новые флаги для этих полей могут быть реализованы по процедуре IETF Review или IESG Approval, но не обязательно будут управляться IANA.

12.4. Коды LISP Address Type

Канонический формат адресов LISP (LISP Canonical Address Format или LCAF) [RFC8060] имеет 8-битовое поле Type, указывающее кодирование LISP для семейства адресов AFI = 16387. Кодирование LCAF применяется в особых случаях, когда нужны разные типы адресов в EID-Record и RLOC-Record.

Для типов LCAF используется реестр LISP Canonical Address Format (LCAF) Types, для которого применяется процедура Specification Required [RFC8126]. Исходные значения и дополнительные сведения даны в [RFC8060].

Реестр LISP Address Type Codes, запрошенный [RFC6830], больше не требуется и этот документ закрывает его.

12.5. Номера LISP Algorithm ID

В [RFC6830] был представлен запрос на реестр LISP Key ID Numbers. В соответствии с этим документом агентство IANA переименовало этот реестр в LISP Algorithm ID Numbers и указало этот документ как ссылку на реестр.

Определённые этой спецификацией значения Algorithm ID, применяемые во всех типах пакетов с полем Algorithm ID, указаны в таблице 5.

Таблица 5.

Имя	Номер	MAC	KDF
Нет	0	Нет	none
HMAC-SHA-1-96-None	1	[RFC2404]	none
HMAC-SHA-256-128-None	2	[RFC4868]	none
HMAC-SHA256-128+HKDF-SHA256	3	[RFC4868]	[RFC4868]

Номера выделяются из диапазона от 0 до 255 в порядке поступления запросов (First Come First Served).

12.6. Битовые флаги LISP

Этот документ запрашивает у IANA создание реестра для выделения битов в нескольких заголовках сообщений плоскости управления LISP, а именно, Map-Request, Map-Reply, Map-Register, Encapsulated Control, а также записей EID-Record и RLOC-Record. Реестр следует назвать LISP Control Plane Header Bits и создать в нем субреестры для каждого сообщения и записи EID-Record. Имена этих субреестров указаны ниже вместе с форматом и выделенными этим документом битами. Для выделения дополнительных битов требуется спецификация в соответствии с правилами [RFC8126].

Субреестр Map-Request Header Bits (5.2. Формат сообщения Map-Request).

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
+-+-+-----+-+-+-----+-+-+-----+-+-+-----+-+-+-----+			
Type=1 A M P S P s R R	Rsvd	L D	IRC
+-+-+-----+-+-+-----+-+-+-----+-+-+-----+-+-+-----+			
Record Count			

Имя	Имя IANA	Номер бита	Описание
A	Map-Request-A	4	Флаг полномочности
M	Map-Request-M	5	Флаг наличия данных отображения
P	Map-Request-P	6	Флаг запроса RLOC-Probe
S	Map-Request-S	7	Флаг запрошенного Map-Request (SMR)
p	Map-Request-p	8	Флаг Proxy-ITR
s	Map-Request-s	9	Флаг вызванного запрошенного Map-Request
L	Map-Request-L	17	Флаг локального xTR
D	Map-Request-D	18	Флаг отказа от Map-Reply

	0									1									2									3								
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1				
	+-----+-----+-----+-----+-----+-----+-----+-----+																																			
	Type=2 P E S								Reserved																Record Count											
	+-----+-----+-----+-----+-----+-----+-----+-----+																																			

Имя	Имя IANA	Номер бита	Описание
P	Map-Reply-P	4	Флаг RLOC-Probe
E	Map-Reply-E	5	Флаг Echo-Nonce Capable
S	Map-Reply-S	6	Флаг Security

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+																																							
Type=3 P S I										Reserved										E T a R M										Record Count									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+																																							

Имя	Имя IANA	Номер бита	Описание
P	Map-Register-P	4	флаг Proxy Map-Reply
S	Map-Register-S	5	флаг поддержки LISP-SEC
I	Map-Register-I	6	флаг наличия xTR-ID

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Type=8 S D E M										Reserved																													

Имя	Имя IANA	Номер бита	Описание
S	ECM-S	4	Флаг Security
D	ECM-D	5	Флаг LISP-DDT
E	ECM-E	6	Флаг пересылки ETR
M	ECM-M	7	Флаг назначения Map-Server

0										1										2										3											
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9		
+-----+-----+-----+-----+										+-----+-----+-----+-----+										+-----+-----+-----+-----+										+-----+-----+-----+-----+											
Locator Count										EID mask-len										ACT		A		Reserved																	
+-----+-----+-----+-----+										+-----+-----+-----+-----+										+-----+-----+		+-----+-----+		+-----+-----+-----+-----+																+-----+-----+	

Имя	Имя IANA	Номер бита	Описание
A	EID-Record-A	19	Флаг полномочности

[illegible]

Имя	Имя IANA	Номер бита	Описание
L	RLOC-Record-L	13	Флаг локального RLOC
p	RLOC-Record-p	14	Флаг RLOC-Probe Reply
R	RLOC-Record-R	15	Флаг RLOC Reachable

www.protokols.ru

- [RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, DOI 10.17487/RFC4868, May 2007, <<https://www.rfc-editor.org/info/rfc4868>>.
- [RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010, <<https://www.rfc-editor.org/info/rfc5869>>.
- [RFC6833] Fuller, V. and D. Farinacci, "Locator/ID Separation Protocol (LISP) Map-Server Interface", [RFC 6833](#), DOI 10.17487/RFC6833, January 2013, <<https://www.rfc-editor.org/info/rfc6833>>.
- [RFC8085] Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage Guidelines", BCP 145, [RFC 8085](#), DOI 10.17487/RFC8085, March 2017, <<https://www.rfc-editor.org/info/rfc8085>>.
- [RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, [RFC 8126](#), DOI 10.17487/RFC8126, June 2017, <<https://www.rfc-editor.org/info/rfc8126>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC9300] Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos, Ed., "The Locator/ID Separation Protocol (LISP)", [RFC 9300](#), DOI 10.17487/RFC9300, October 2022, <<https://www.rfc-editor.org/info/rfc9300>>.
- [RFC9302] Iannone, L., Saucez, D., and O. Bonaventure, "Locator/ID Separation Protocol (LISP) Map-Versioning", [RFC 9302](#), DOI 10.17487/RFC9302, October 2022, <<https://www.rfc-editor.org/info/rfc9302>>.
- [RFC9303] Maino, F., Ermagan, V., Cabellos, A., and D. Saucez, "Locator/ID Separation Protocol Security (LISP-SEC)", [RFC 9303](#), DOI 10.17487/RFC9303, October 2022, <<https://www.rfc-editor.org/info/rfc9303>>.
- [RFC9304] Boucadair, M. and C. Jacquenet, "Locator/ID Separation Protocol (LISP): Shared Extension Message and IANA Registry for Packet Type Allocations", [RFC 9304](#), DOI 10.17487/RFC9304, October 2022, <<https://www.rfc-editor.org/info/rfc9304>>.

13.2. Дополнительная литература

- [AFN] IANA, "Address Family Numbers", <<http://www.iana.org/assignments/address-family-numbers/>>.
- [ECDSA-AUTH] Farinacci, D. and E. Nordmark, "LISP Control-Plane ECDSA Authentication and Authorization", Work in Progress, Internet-Draft, draft-ietf-lisp-ecdsa-auth-09, 11 September 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-lisp-ecdsa-auth-09>>.
- [EID-ANONYMITY] Farinacci, D., Pillay-Esnault, P., and W. Haddad, "LISP EID Anonymity", Work in Progress, Internet-Draft, draft-ietf-lisp-eid-anonymity-13, 11 September 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-lisp-eid-anonymity-13>>.
- [EID-MOBILITY] Portoles, M., Ashtaputre, V., Maino, F., Moreno, V., and D. Farinacci, "LISP L2/L3 EID Mobility Using a Unified Control Plane", Work in Progress, Internet-Draft, draft-ietf-lisp-eid-mobility-10, 10 July 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-lisp-eid-mobility-10>>.
- [GTP-3GPP] 3GPP, "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)", TS.29.281, June 2022, <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1699>>.
- [INTAREA-ILA] Herbert, T. and P. Lapukhov, "Identifier-locator addressing for IPv6", Work in Progress, Internet-Draft, draft-herbert-intarea-ila-01, 5 March 2018, <<https://datatracker.ietf.org/doc/html/draft-herbert-intarea-ila-01>>.
- [LISP-MN] Farinacci, D., Lewis, D., Meyer, D., and C. White, "LISP Mobile Node", Work in Progress, Internet-Draft, draft-ietf-lisp-mn-12, 24 July 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-lisp-mn-12>>.
- [LISP-PUBSUB] Rodriguez-Natal, A., Ermagan, V., Cabellos-Aparicio, A., Barkai, S., and M. Boucadair, "Publish/Subscribe Functionality for LISP", Work in Progress, Internet-Draft, draft-ietf-lisp-pubsub-09, 28 June 2021, <<https://datatracker.ietf.org/doc/html/draft-ietf-lisp-pubsub-09>>.
- [NVO3-VXLAN-GPE] Maino, F., Ed., Kreeger, L., Ed., and U. Elzur, Ed., "Generic Protocol Extension for VXLAN (VXLAN-GPE)", Work in Progress, Internet-Draft, draft-ietf-nvo3-vxlan-gpe-12, 22 September 2021, <<https://datatracker.ietf.org/doc/html/draft-ietf-nvo3-vxlan-gpe-12>>.
- [OPSEC-ICMP-FILTER] Gont, F., Gont, G., and C. Pignataro, "Recommendations for filtering ICMP messages", Work in Progress, Internet-Draft, draft-ietf-opsec-icmp-filtering-04, 3 July 2013, <<https://datatracker.ietf.org/doc/html/draft-ietf-opsec-icmp-filtering-04>>.
- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), DOI 10.17487/RFC1035, November 1987, <<https://www.rfc-editor.org/info/rfc1035>>.
- [RFC1071] Braden, R., Borman, D., and C. Partridge, "Computing the Internet checksum", [RFC 1071](#), DOI 10.17487/RFC1071, September 1988, <<https://www.rfc-editor.org/info/rfc1071>>.
- [RFC2890] Dommety, G., "Key and Sequence Number Extensions to GRE", [RFC 2890](#), DOI 10.17487/RFC2890, September 2000, <<https://www.rfc-editor.org/info/rfc2890>>.
- [RFC4984] Meyer, D., Ed., Zhang, L., Ed., and K. Fall, Ed., "Report from the IAB Workshop on Routing and Addressing", [RFC 4984](#), DOI 10.17487/RFC4984, September 2007, <<https://www.rfc-editor.org/info/rfc4984>>.
- [RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", [RFC 6830](#), DOI 10.17487/RFC6830, January 2013, <<https://www.rfc-editor.org/info/rfc6830>>.

- [RFC6831] Farinacci, D., Meyer, D., Zwiebel, J., and S. Venaas, "The Locator/ID Separation Protocol (LISP) for Multicast Environments", [RFC 6831](#), DOI 10.17487/RFC6831, January 2013, <<https://www.rfc-editor.org/info/rfc6831>>.
- [RFC6832] Lewis, D., Meyer, D., Farinacci, D., and V. Fuller, "Interworking between Locator/ID Separation Protocol (LISP) and Non-LISP Sites", [RFC 6832](#), DOI 10.17487/RFC6832, January 2013, <<https://www.rfc-editor.org/info/rfc6832>>.
- [RFC6836] Fuller, V., Farinacci, D., Meyer, D., and D. Lewis, "Locator/ID Separation Protocol Alternative Logical Topology (LISP+ALT)", RFC 6836, DOI 10.17487/RFC6836, January 2013, <<https://www.rfc-editor.org/info/rfc6836>>.
- [RFC6837] Lear, E., "NERD: A Not-so-novel Endpoint ID (EID) to Routing Locator (RLOC) Database", RFC 6837, DOI 10.17487/RFC6837, January 2013, <<https://www.rfc-editor.org/info/rfc6837>>.
- [RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <<https://www.rfc-editor.org/info/rfc6973>>.
- [RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", [RFC 7348](#), DOI 10.17487/RFC7348, August 2014, <<https://www.rfc-editor.org/info/rfc7348>>.
- [RFC7835] Saucez, D., Iannone, L., and O. Bonaventure, "Locator/ID Separation Protocol (LISP) Threat Analysis", RFC 7835, DOI 10.17487/RFC7835, April 2016, <<https://www.rfc-editor.org/info/rfc7835>>.
- [RFC8060] Farinacci, D., Meyer, D., and J. Snijders, "LISP Canonical Address Format (LCAF)", [RFC 8060](#), DOI 10.17487/RFC8060, February 2017, <<https://www.rfc-editor.org/info/rfc8060>>.
- [RFC8061] Farinacci, D. and B. Weis, "Locator/ID Separation Protocol (LISP) Data-Plane Confidentiality", [RFC 8061](#), DOI 10.17487/RFC8061, February 2017, <<https://www.rfc-editor.org/info/rfc8061>>.
- [RFC8111] Fuller, V., Lewis, D., Ermagan, V., Jain, A., and A. Smirnov, "Locator/ID Separation Protocol Delegated Database Tree (LISP-DDT)", RFC 8111, DOI 10.17487/RFC8111, May 2017, <<https://www.rfc-editor.org/info/rfc8111>>.
- [RFC8378] Moreno, V. and D. Farinacci, "Signal-Free Locator/ID Separation Protocol (LISP) Multicast", RFC 8378, DOI 10.17487/RFC8378, May 2018, <<https://www.rfc-editor.org/info/rfc8378>>.
- [RFC8402] Filts, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", [RFC 8402](#), DOI 10.17487/RFC8402, July 2018, <<https://www.rfc-editor.org/info/rfc8402>>.
- [RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", [RFC 9147](#), DOI 10.17487/RFC9147, April 2022, <<https://www.rfc-editor.org/info/rfc9147>>.
- [RFC9299] Cabellos, A. and D. Saucez, Ed., "An Architectural Introduction to the Locator/ID Separation Protocol (LISP)", [RFC 9299](#), DOI 10.17487/RFC9299, October 2022, <<https://www.rfc-editor.org/info/rfc9299>>.
- [RFC9305] Maino, F., Ed., Lemon, J., Agarwal, P., Lewis, D., and M. Smith, "Locator/ID Separation Protocol (LISP) Generic Protocol Extension", [RFC 9305](#), DOI 10.17487/RFC9305, October 2022, <<https://www.rfc-editor.org/info/rfc9305>>.

Благодарности

Авторы исходного документа благодарны Greg Schudel, Darrel Lewis, John Zwiebel, Andrew Partan, Dave Meyer, Isidor Kouvellas, Jesper Skriver и участникам почтовой конференции lisp@ietf.org за их отклики и полезные предложения.

Отдельная благодарность Noel Chiappa за обширную работу и размышления о кэшировании в Map-Resolver.

Нынешние авторы выражают свою искреннюю благодарность людям, которые помогли провести LISP через процедуры Standards Track в IETF. Это Joel Halpern, Luigi Iannone, Deborah Brungard, Fabio Maino, Scott Bradner, Kyle Rose, Takeshi Takahashi, Sarah Banks, Pete Resnick, Colin Perkins, Mirja Kühlewind, Francis Dupont, Benjamin Kaduk, Eric Rescorla, Alvaro Retana, Alexey Melnikov, Alissa Cooper, Suresh Krishnan, Alberto Rodriguez-Natal, Vina Ermagan, Mohamed Boucadair, Brian Trammell, Sabrina Tanamal, John Drake. Их вклад существенно улучшил безопасность, расширяемость и отказоустойчивость архитектуры и протоколов LISP.

Адреса авторов

Dino Farinacci
lispers.net
San Jose, CA
United States of America
Email: farinacci@gmail.com

Fabio Maino
Cisco Systems
San Jose, CA
United States of America
Email: fmaino@cisco.com

Vince Fuller

vaf.net Internet Consulting
Email: vince.fuller@gmail.com

Albert Cabellos (editor)
Universitat Politecnica de Catalunya
c/ Jordi Girona s/n
08034 Barcelona
Spain
Email: acabello@ac.upc.edu

Перевод на русский язык

Николай Малых
nmalykh@protokols.ru