

Internet Engineering Task Force (IETF)
Request for Comments: 9300
Obsoletes: 6830
Category: Standards Track
ISSN: 2070-1721

D. Farinacci
lispers.net
V. Fuller
vaf.net Internet Consulting
D. Meyer
1-4-5.net
D. Lewis
Cisco Systems
A. Cabellos, Ed.
Universitat Politecnica de Catalunya
October 2022

The Locator/ID Separation Protocol (LISP)

Протокол разделения локаторов и идентификаторов (LISP)

Аннотация

Этот документ описывает протокол плоскости данных для разделения локаторов и идентификаторов (Locator/ID Separation Protocol или LISP). LISP определяет два пространства имён - идентификаторы конечных точек (Endpoint Identifier или EID), указывающие конечные точки, и локаторы маршрутизации (Routing Locator или RLOC), которые указывают точки подключения к сети. При этом LISP эффективно разделяет управление и данные, что позволяет маршрутизаторам создавать наложенные сети. Маршрутизаторы с поддержкой LISP обмениваются инкапсулированными пакетами в соответствии с отображениями EID на RLOC, хранящимися в локальном кэше Map-Cache.

LISP не требует менять стеки протоколов на конечных хостах и маршрутизаторах базовых сетей и, среди прочего, поддерживает организацию трафика (Traffic Engineering или TE), многодомность и мобильность.

Этот документ отменяет RFC 6830.

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/rfc9300>.

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.....	2
3. Определения терминов.....	2
4. Базовый обзор.....	4
4.1. Развёртывание в общедоступной сети Internet.....	5
4.2. Порядок потока пакетов.....	5
5. Детали инкапсуляции LISP.....	5
5.1. Формат заголовка LISP IPv4-in-IPv4.....	6
5.2. Формат заголовка LISP IPv6-in-IPv6.....	7
5.3. Описание полей туннельного заголовка.....	7
6. Кэш сопоставлений EID с RLOC в LISP.....	9
7. Обработка больших инкапсулированных пакетов.....	9
7.1. Решение для обработки MTU без учёта состояний.....	9
7.2. Решение для обработки MTU с учётом состояний.....	10
8. Использование виртуализации и разделения с LISP.....	10
9. Выбор локатора маршрутизации.....	10

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

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

10. Доступность локатора маршрутизации.....	11
10.1. Алгоритм Echo-Nonce.....	12
11. Доступность EID на сайте LISP.....	12
12. Хэширование локаторов маршрутизации.....	12
13. Изменение содержимого отображений EID на RLOC.....	13
13.1. Locator-Status-Bits.....	13
13.2. Версии базы данных отображений.....	13
14. Групповая передача.....	13
15. Работа маршрутизаторов.....	14
16. Вопросы безопасности.....	14
17. Вопросы управления сетью.....	14
18. Отличия от RFC 6830.....	14
19. Взаимодействие с IANA.....	15
19.1. Номера портов LISP UDP.....	15
20. Литература.....	15
20.1. Нормативные документы.....	15
20.2. Дополнительная литература.....	15
Благодарности.....	16
Адреса авторов.....	17

1. Введение

Этот документ описывает LISP - протокол инкапсуляции, основанный на фундаментальной идее разделения топологического местоположения точки присоединения к сети и отождествления узла [CHIAPPA]. В результате LISP создаёт два пространства имён - идентификаторы конечных точек (EID), служащие для указания конечных хостов (например, узлов или виртуальных машин), и маршрутизируемых локаторов (RLOC), указывающих точки подключения к сети. LISP также задаёт функции для сопоставления между этими пространствами имён и инкапсуляции трафика от устройств, использующих немаршрутизируемые EID, для транспортировки через сетевую инфраструктуру, которая обеспечивает маршрутизацию и пересылку с использованием RLOC. Инкапсуляция LISP применяет динамическую форму туннелирования, где не требуется статическое обеспечение.

LISP является наложенным протоколом, отделяющим управление от данных и этот документ задаёт плоскость данных, а также способы обмена пакетами между маршрутизаторами с поддержкой LISP (туннельные маршрутизаторы) за счёт инкапсуляции. Туннельные маршрутизаторы включают кэш отображения (Map-Cache), который содержит сопоставления EID с RLOC. Map-Cache заполняется с помощью протокола плоскости управления LISP [RFC9301].

LISP не требует менять стек протоколов на хостах или базовых маршрутизаторах. Отделяя EID от RLOC, LISP поддерживает естественную организацию трафика (TE), многодомность, мобильность и иные возможности.

Разработка LISP была инициирована дискуссиями во время организованного IAB семинара Routing and Addressing в Амстердаме в октябре 2006 г. (см. [RFC4984]).

Этот документ задаёт инкапсуляцию плоскости данных LISP и другую функциональность пересылки на узлах LISP, а в [RFC9301] определена плоскость управления LISP. Рекомендации по развёртыванию LISP приведены в [RFC7215], а в [RFC6835] рассмотрены соображения по управлению сетями. В [RFC9299] описана архитектура LISP.

Этот документ отменяет RFC 6830.

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.

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

Address Family Identifier (AFI)

Термин AFI служит для описания кодирования адреса в пакете. Семейство адреса - это формат адреса, найденный в заголовках пакетов плоскости данных, например, адреса IPv4 или IPv6. Дополнительные подробности приведены в [AFN], [RFC2453], [RFC2677], [RFC4760]. AFI = 0 в этой спецификации указывает незаданное представление адреса, занимающего 0 октетов и имеющего 16-битовое поле AFI со значением 0.

Anycast Address

Anycast-адрес - это один адрес IPv4 или IPv6, настроенный и применяемый на нескольких системах одновременно. EID и RLOC могут быть anycast-адресами в своих пространствах адресов.

Client-side

Клиентской стороной в этом документе называется предпринимающая попытку инициировать соединение конечная система, представленная EID.

Egress Tunnel Router (ETR) - выходной маршрутизатор туннеля

ETR - это маршрутизатор, воспринимающий пакеты IP, где адресом получателя во внешнем заголовке IP служит один из его RLOC. Маршрутизатор «вырезает» внешний заголовок и пересылает пакет по адресу IP из следующего

заголовка. В общем случае ETR получает пакеты IP с инкапсуляцией LISP из Internet на одной стороне и передаёт декапсулированные пакеты IP конечным системам сайта на другой стороне. Функциональность ETR может реализовываться не только маршрутизаторами, но и серверными хостами, служащими точками завершения туннелей LISP.

EID-to-RLOC Database - база данных отображений

Распределенная база данных, содержащая все известные отображения EID-Prefix на RLOC. Каждый возможный ETR обычно содержит небольшую часть этой базы - отображения EID на RLOC для префиксов EID, находящихся за маршрутизатором. Эти префиксы сопоставляются с одним из IP-адресов маршрутизатора, маршрутизируемых в базовой сети. Отметим, что **возможны** временные условия, когда EID-Prefix для сайта LISP и Locator-Set для каждого EID-Prefix могут не совпадать на всех ETR. Это не оказывает негативного влияния, поскольку можно применять неполный набор локаторов.

EID-to-RLOC Map-Cache - кэш данных отображений

Обычно это краткосрочная таблица, создаваемая по запросу на входном маршрутизаторе туннеля (ITR), которая сохраняет, отслеживает, отвечает за синхронизацию и иные проверки отображения EID-RLOC. Этот кэш отличается от «полной» базы отображений EID на RLOC, он является динамическим, локальным для ITR и относительно небольшим, тогда как база данных распределена, относительно статична и действует для большого числа узлов LISP.

EID-Prefix - префикс EID

EID-Prefix - это блок EID размером в степень числа 2, выделяемый сайту органом по распределению адресов. Префиксы EID-Prefix связываются с наборами адресов RLOC. EID-Prefix может делиться на более мелкие блоки, когда RLOC-Set связывается с более крупным блоком EID-Prefix.

End-System - конечная система

Устройство IPv4 или IPv6, выдающее пакеты с одним заголовком IPv4 или IPv6. Конечная система представляет значение EID в поле адреса получателя в заголовке IP при взаимодействии, выходящем из домена маршрутизации. Конечной системой может быть хост-компьютер, коммутатор или маршрутизатор, сетевая платформа.

Endpoint ID (EID) - идентификатор конечной точки

EID - 32-битовое (IPv4) или 128-битовое (IPv6) значение, идентифицирующее хост. Значения EID обычно присутствуют лишь в полях адресов отправителя и получателя первого (внутреннего) заголовка LISP в пакете. Хост получает EID адресата от поиска в DNS¹ [RFC1034] или обмена по протоколу инициирования сессии (Session Initiation Protocol или SIP) [RFC3261]. Их поведение не меняется при использовании LISP. EID отправителя получается с помощью имеющихся механизмов, применяемых для установки «локального» IP-адреса хоста. EID для использования в общедоступной сети Internet **должен** иметь такие же свойства, как другие адреса IP, используемые в таких случаях. Это означает, в том числе, что идентификатор **должен** быть уникальным. Значения EID выделяются хостам из блока EID-Prefix, связанного с сайтом, где размещён хост. EID может использоваться хостом для указания других хостов. Отметим, что блоки EID **могут** назначаться иерархически, независимо от топологии сети, для упрощения расширения база данных отображений. Кроме того, назначенный сайту блок EID **может** иметь локальную для сайта структуру (подсети) для маршрутизации внутри сайта, эта структура не будет видна базовой структуре маршрутизации. В теории битовая строка EID для одного устройства может представлять RLOC для другого устройства. При обсуждении других приложений по разделению Locator и ID все упоминания EID в этом документе относятся к LISP EID.

Ingress Tunnel Router (ITR) - входной маршрутизатор туннеля

ITR - это маршрутизатор, размещённый на сайте LISP. Пакеты с отправителями сайта LISP для внешних получателей являются кандидатами для инкапсуляции маршрутизатором ITR. ITR рассматривает IP-адрес получателя как EID и выполняет поиск отображения EID на RLOC. Маршрутизатор добавляет в начало пакета (prepend) «внешний» заголовок IP с одним из маршрутизируемых RLOC (в пространстве RLOC) в поле адреса отправителя и результатом поиска отображения в поле адреса получателя. Отметим, что RLOC получателя может быть промежуточным устройством-посредником (проху), которому лучше известно отображение EID на RLOC ближе к EID адресата. В общем случае ITR получает пакеты IP от конечной системы сайта на одной стороне и передаёт пакет IP с инкапсуляцией LISP в направлении Internet на другой стороне.

LISP Header - заголовок LISP

Заголовком LISP в этом документе называется внешний заголовок IPv4 или IPv6, заголовок UDP и связанный с LISP 8-октетный заголовок, которые следуют после заголовка UDP. ITR помещает заголовок LISP перед пакетом, а ETR «вырезает» его.

LISP Router - маршрутизатор LISP

Маршрутизатором LISP называется маршрутизатор, выполняющий функции ITR, ETR, RTR, PITRs или PETR.

LISP Site - сайт LISP

Сайтом LISP считается набор маршрутизаторов на периметре сети, находящихся под единым техническим администрированием. Маршрутизаторы LISP на периметре отделяют периметр сети от её ядра.

Locator-Status-Bits (LSBs) - биты статуса локатора

Биты статуса локатора представляются в заголовке LISP и используются маршрутизаторами ITR для информирования ETR о состоянии up/down всех маршрутизаторов ETR на локальном сайте. Эти биты служат подсказками о состоянии маршрутизаторов, а не путей. LSB можно проверить с помощью одного из алгоритмов обнаружения доступности Locator, описанных в разделе 10. Доступность локатора маршрутизации. ETR **должен** ограничивать частоту применяемых действий при обнаружении смены битов статуса локаторов.

Proxy-ETR (PETR) - ETR-посредник

Определение и описание PETR приведено в [RFC6832]. PETR действует подобно ETR, но делает это от имени сайтов LISP, которые передают пакеты адресатам, не находящимся на сайтах LISP.

Proxy-ITR (PITR) - ITR-посредник

Определение и описание PITR приведено в [RFC6832]. PITR действует подобно ITR, но делает это от имени сайтов LISP, которые передают пакеты адресатам, находящимся на сайтах LISP.

Recursive Tunneling - рекурсивное туннелирование

Рекурсивное туннелирование возникает, когда пакет имеет более одного заголовка LISP IP. Дополнительные уровни туннелирования **могут** реализовываться для организации трафика (Traffic Engineering) или иных изменений маршрутизации (rerouting). При этом добавляется новый «внешний» заголовок LISP, а исходные RLOC сохраняются во «внутреннем» заголовке.

¹Domain Name System - система доменных имён.

Re-encapsulating Tunneling Router (RTR) - туннельный маршрутизатор смены инкапсуляции

RTR выступает как ETR для удаления заголовка LISP, затем как ITR для включения нового заголовка LISP в начале. Это называется туннелированием со сменой инкапсуляции, что позволяет перемаршрутизировать пакет на RTR без добавления ещё одного туннельного заголовка. При использовании нескольких систем (баз данных) отображения нужно соблюдать осторожность, чтобы не возникло петель смены инкапсуляции в результате конфигурационных ошибок.

Route-Returnability - возвратность маршрута

Допущение о том, что базовая система маршрутизации доставляет пакеты адресату. В сочетании со значением попсе, которое представляет отправитель и возвращает получатель это ограничивает возможность вставки данных вне пути. Проверка возвратности маршрута выполняется передачей сообщения с попсе и возвратом другого сообщения с тем же попсе и указанием получателя исходного сообщения как отправителя отклика.

Routing Locator (RLOC) - локатор маршрутизации

RLOC - это адрес IPv4 [RFC0791] или IPv6 [RFC8200] выходного маршрутизатора туннеля (ETR). Значение RLOC является результатом поиска отображения EID на RLOC. EID может (необязательно) сопоставляться с несколькими RLOC. Обычно значения RLOC берутся из блоков, назначенных сайту для каждой точки соединения с внешними базовыми сетями, где топология определяется связностью сетей провайдеров. Несколько RLOC можно назначить одному или нескольким маршрутизаторам ETR на сайте.

Server-side - серверная сторона

Серверной в этом документе называется сторона, воспринимающая попытку соединения с EID получателя.

xTR

xTR указывает ITR или ETR, когда направление потока данных не является частью описания контекста. xTR указывает маршрутизатор, являющийся конечной точкой туннеля, и применяется как синоним термина «туннельный маршрутизатор» (Tunnel Router). Например, фраза «xTR может размещаться на граничном маршрутизаторе клиента (Customer Edge или CE)» указывает, что маршрутизатор CE может быть ITR и ETR.

4. Базовый обзор

Одной из важных концепций LISP является независимость работы конечных точек от применения LISP. Адреса IP, применяемые хостами для отслеживания хостов и соединений, а также для передачи и приёма сообщений не меняются. В терминах LISP эти адреса называются идентификаторами конечных точек (EID).

Маршрутизаторы по-прежнему пересылают пакеты по IP-адресам получателей. Для пакетов с инкапсуляцией LISP эти адреса называются локаторами (RLOC). Большинство маршрутизаторов на пути между хостами также сохраняются и выполняют поиск для маршрутизации и пересылки по адресам получателей. Для маршрутизаторов между хостом-источником и ITR целевого хоста, а также между ETR целевого хоста и получателем адресом получателя служит EID. Для маршрутизаторов между ITR и ETR адресом получателя является RLOC.

Другой важной концепцией LISP является туннельный маршрутизатор (Tunnel Router). Этот маршрутизатор добавляет в начало (prepend) заголовок LISP созданных хостом пакетов и вырезает эти заголовки перед доставкой конечному получателю. Адресами IP в этих «внешних» заголовках являются локаторы RLOC. При сквозном обмене пакетами между хостами Internet маршрутизатор ITR добавляет заголовок LISP, а ETR удаляет его. ITR выполняет поиск отображения EID на RLOC для определения пути к ETR, имеющему RLOC в качестве одного из адресов IP.

Некоторые базовые правила LISP перечислены ниже.

- Конечные системы передают пакеты лишь по EID, которыми обычно служат адреса IP, назначенные хостам (другие типа EID, поддерживаемые LISP, описаны в [RFC8060]). Конечные системы не знают, что адреса являются EID, а не RLOC, и предполагают, что пакеты приходят к адресату. В системах с LISP маршрутизаторы LISP перехватывают пакеты с адресами EID и помогают доставлять их через ядро сети, где EID не маршрутизируются. Процедура отправки хостом пакетов IP не меняется.
- Маршрутизаторы LISP добавляют в начало пакета или вырезают внешние заголовки с адресами RLOC, как описано в параграфе 4.2. Порядок потока пакетов.
- RLOC всегда являются адресами IP, назначенными маршрутизаторам, которые предпочтительно привязывать к топологии провайдерских бесклассовых блоков (Classless Inter-Domain Routing или CIDR).
- Когда маршрутизатор создаёт пакеты, он **может** использовать в качестве адреса отправителя EID или RLOC. Выступая в качестве хоста (например, в транспортной сессии SSH, TELNET или SNMP), он **может** использовать EID, явно выделенный для этих целей. EID, указывающий маршрутизатор, **недопустимо** применять в качестве RLOC, поскольку EID маршрутизируется лишь внутри сайта. В типичной конфигурации BGP может встречаться такое «гибридное» использование EID/RLOC, где маршрутизатор может применять EID для внутренних сессий BGP (iBGP) с маршрутизаторами внутри сайта и RLOC для внешних сессий BGP (eBGP) с маршрутизаторами других сайтов.
- Предполагается, что пакеты с EID не будут доставляться «насквозь» при отсутствии отображения EID на RLOC. Ожидается, что они будут применяться для взаимодействий внутри сайта или инкапсулироваться для передачи на другие сайты.
- EID **могут** структурироваться (подсети) для маршрутизации внутри локальной автономной системы (Autonomous System или AS).

Дополнительный заголовок LISP **могут** добавлять в начало пакета маршрутизаторы TE-ITR для изменения пути доставки пакета. Возможным вариантом использования является маршрутизатор провайдера (ISP), которому нужно организовать трафик (Traffic Engineering) для пакетов, проходящих через сеть провайдера. В таких ситуациях, называемых рекурсивным туннелированием (Recursive Tunneling), транзитный ISP выступает дополнительным ITR, а применяемый им целевой RLOC для этого добавленного заголовка будет TE-ETR внутри ISP (на его внутреннем пути организации трафика) или TE-ETR у другого ISP (организация трафика между ISP при согласовании такого пути).

Для предотвращения избыточных издержек, а также возможных петель инкапсуляции **рекомендуется** добавлять в пакет не более 2 заголовков LISP. Для первоначального развёртывания LISP предполагается, что двух заголовков

будет достаточно и первый из этих заголовков применяется на сайте для разделения местоположения и идентификации, а второй используется внутри сервис-провайдера для организации трафика.

Туннельные маршрутизаторы можно достаточно свободно размещать в топологии с множеством AS. Например, ITR для определённого сквозного обмена пакетами может быть первым (first-hop) или принятым по умолчанию (default) маршрутизатором внутри сайта хоста-источника. ETR может быть последним (last-hop) маршрутизатором, напрямую соединённым с хостом-получателем. Другим примером может служить передача сайтом услуг VPN своему ISP, который будет применять в качестве ITR свой граничный маршрутизатор в точке присоединения. Для максимальной гибкости допускается смешивание туннельных маршрутизаторов на сайте, у ISP и в других местах.

4.1. Развёртывание в общедоступной сети Internet

Некоторые из описанных в документе механизмов предназначены для контролируемых, доверенных сред и небезопасны для использования в общей сети Internet. В частности, в Internet узлы xTRs

- **должны** сбрасывать (0) биты N, L, E, V в заголовке LISP (5.1. Формат заголовка LISP IPv4-in-IPv4);
- им **недопустимо** использовать LSB и Echo-Nonce (10. Доступность локатора маршрутизации) для доступности RLOC, а взамен они **должны** полагаться исключительно на методы плоскости управления;
- им **недопустимо** использовать сбор LSB и версий отображения (13. Изменение содержимого отображений EID на RLOC) для обновления отображений EID на RLOC и взамен они **должны** полагаться исключительно на методы плоскости управления.

4.2. Порядок потока пакетов

В этом параграфе приведён пример потока индивидуальных (unicast) пакетов, включая сведения плоскости управления, как указано в [RFC9301]. Ниже приведены условия, предполагающиеся в этом примере.

- Хост host1.abc.example.com передаёт пакеты хосту host2.xyz.example.com так же, как при отсутствии LISP.
- Каждый сайт является многодомным, поэтому каждый туннельный маршрутизатор имеет адрес (RLOC) из блока сервис-провайдера, к которому этот маршрутизатор подключён.
- Маршрутизаторы ITR и ETR подключены напрямую к источнику и получателю, соответственно, но отправители и получатели могут размещаться в любом месте сайтов LISP.
- Передаётся Map-Request для внешнего адресата, когда получатель не найден в таблице пересылки и не соответствует заданному по умолчанию маршруту. Эти запросы передаются в базу данных отображений с помощью протокола плоскости управления LISP, описанного в [RFC9301].
- Отклики Map-Replies передаются в топологию базовой системы маршрутизации и помощью протокола плоскости управления [RFC9301].

Клиент host1.abc.example.com хочет взаимодействовать с сервером host2.xyz.example.com.

1. host1.abc.example.com хочет организовать соединение TCP с host2.xyz.example.com и выполняет поиск DNS для host2.xyz.example.com, который возвращает запись A/AAAA. Это будет EID получателя, а заданный локально адрес host1.abc.example.com служит EID отправителя. Пакеты IPv4 или IPv6 создаются и пересылаются через сайт LISP как обычные пакеты IP, пока они не почтуют на LISP ITR.
2. LISP ITR должен быть способен отобразить EID получателя на RLOC одного из ETR на сайте адресата. Это делается с помощью отправки LISP Map-Request, как описано в [RFC9301].
3. Система отображения (Mapping System) помогает переслать Map-Request соответствующему ETR. При поступлении Map-Request на один из ETR целевого сайта пакет обрабатывается как управляющее сообщение.
4. ETR просматривает EID получателя в Map-Request и сопоставляет его с префиксами в настроенной на ETR базы отображения EID-RLOC. Это список префиксов EID, которые ETR поддерживает для своего сайта. Если совпадения не найдено, Map-Request отбрасывается. В ином случае ITR возвращается LISP Map-Reply.
5. ITR принимает сообщение Map-Reply, анализирует его и сохраняет сведения об отображении из пакета в своём кэше отображений EID на RLOC (Map-Cache). Отметим, что это кэширование выполняется по запросам, а ITR поддерживает Map-Cache с учётом своих ограничений на ресурсы.
6. В последующие пакеты от host1.abc.example.com к host2.xyz.example.com маршрутизатор ITR включает заголовок LISP, используя подходящий локатор RLOC от ETR в качестве адреса получателя в заголовке LISP. Отметим, что пакет **может** передаваться разным ETR, которые могут быть указаны в Map-Reply, из-за политики хэширования сайта-источника или политики Locator-Set у получателя.
7. ETR получает пакеты напрямую (поскольку адресом получателя является один из его адресов IP), проверяет пригодность адреса, вырезает заголовок LISP и пересылает пакеты подключённому целевому хосту.
8. Чтобы отложить поиск сопоставления в обратном направлении ETR **может** создавать запись в кэше, отображающую EID источника (внутренний IP-адрес отправителя) на RLOC источника (IP-адрес отправителя из внешнего заголовка) из принятого пакета LISP. Такие записи называют отображениями сбора (glean mapping) и они включают лишь 1 RLOC для EID. Более полные сведения о дополнительных RLOC **следует** получать, передавая запрос LISP Map-Request для EID. Маршрутизаторы ITR и ETR **могут** влиять на решение, принимаемые другим при выборе RLOC.

5. Детали инкапсуляции LISP

Поскольку в начало пакета добавляются туннельные заголовки, пакет становится больше и его размер может превысить значение MTU на каком-либо канале между ITR и ETR. Для пакетов IPv4 **рекомендуется** не выполнять фрагментацию пакетов, поскольку они инкапсулированы ITR, а вместо этого отбрасывать такие пакеты и возвращать

отправителю сообщение ICMPv4 Unreachable / Fragmentation Needed. Если требуется фрагментировать пакет, реализациям **рекомендуется** поддерживать одну из предложенных схем фрагментации и сборки. Две имеющихся схемы описаны в разделе 7. Обработка больших инкапсулированных пакетов.

Поскольку адреса IPv4 и IPv6 могут быть идентификаторами EID или локаторами RLOC, архитектура LISP поддерживает IPv4 EID с IPv6 RLOC (внутренний заголовок имеет формат IPv4, а внешний - IPv6) и IPv6 EID с IPv4 RLOC (внутренний заголовок IPv6 и внешний IPv4). В последующих параграфах показаны форматы пакетов для однородных вариантов (IPv4 в IPv4 и IPv6 в IPv6), но **должны** поддерживаться все 4 комбинации. Дополнительные типы EID определены в [RFC8060].

LISP использует инкапсуляцию UDP для передачи трафика между xTRs через Internet и разработчикам следует учитывать положения [RFC8085], особенно параграф 3.1.11, где описан контроль перегрузок для туннелей UDP. Разработчикам рекомендуется учитывать рекомендации параграфа 3.4 из [RFC8085] для контрольных сумм UDP, когда желательно защитить заголовки UDP и LISP от повреждений.

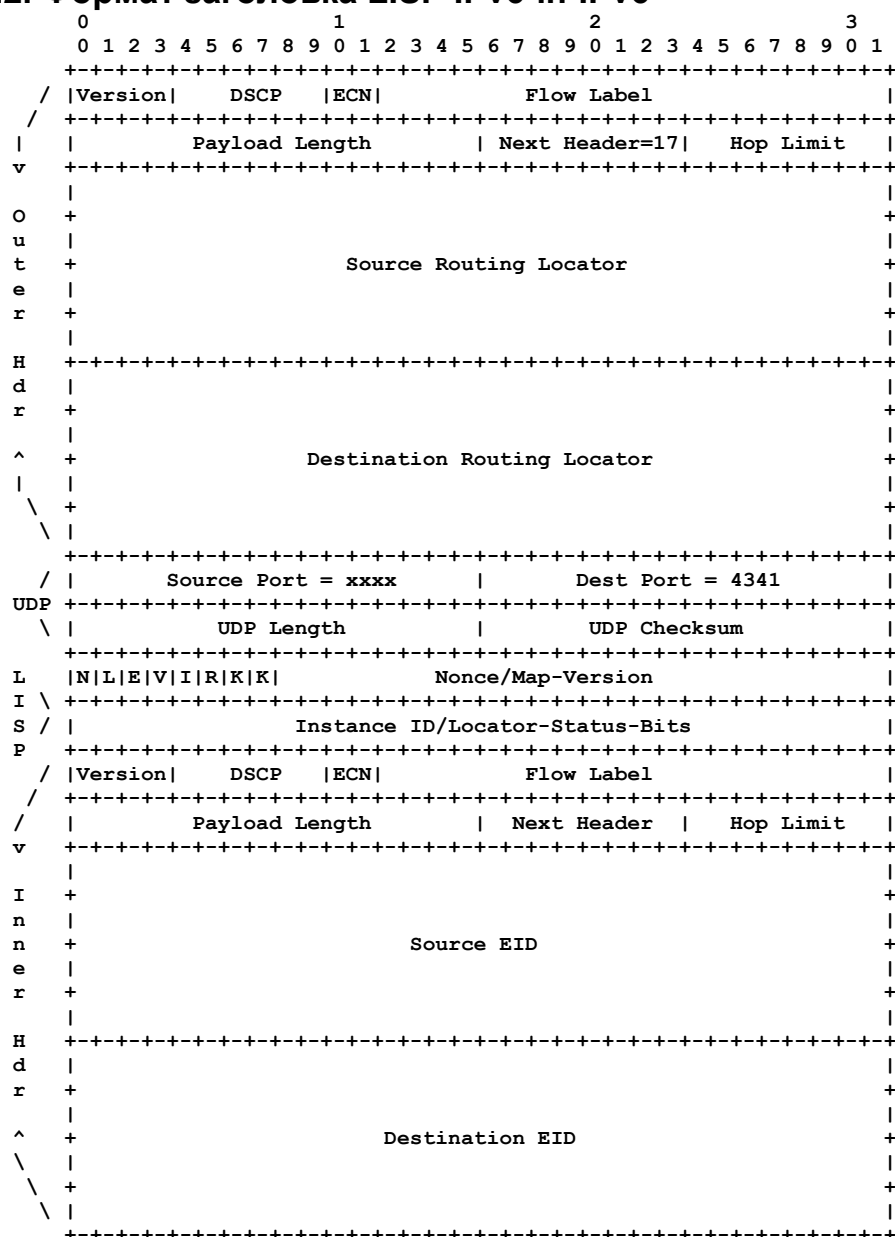
5.1. Формат заголовка LISP IPv4-in-IPv4

```

      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
+-----+-----+-----+-----+-----+-----+-----+-----+
/ |Version| IHL | DSCP |ECN| Total Length |
/ +-----+-----+-----+-----+-----+-----+-----+
| | Identification |Flags| Fragment Offset |
+-----+-----+-----+-----+-----+-----+-----+
OH | Time to Live | Protocol = 17 | Header Checksum |
| +-----+-----+-----+-----+-----+-----+-----+
| | Source Routing Locator |
\ +-----+-----+-----+-----+-----+-----+-----+
\ | Destination Routing Locator |
+-----+-----+-----+-----+-----+-----+-----+
/ | Source Port = xxxx | Dest Port = 4341 |
UDP +-----+-----+-----+-----+-----+-----+-----+
\ | UDP Length | UDP Checksum |
+-----+-----+-----+-----+-----+-----+-----+
L |N|L|E|V|I|R|K|K| Nonce/Map-Version |
I \ +-----+-----+-----+-----+-----+-----+-----+
S / | Instance ID/Locator-Status-Bits |
P +-----+-----+-----+-----+-----+-----+-----+
/ |Version| IHL | DSCP |ECN| Total Length |
/ +-----+-----+-----+-----+-----+-----+-----+
| | Identification |Flags| Fragment Offset |
| +-----+-----+-----+-----+-----+-----+-----+
IH | Time to Live | Protocol | Header Checksum |
| +-----+-----+-----+-----+-----+-----+-----+
| | Source EID |
\ +-----+-----+-----+-----+-----+-----+-----+
\ | Destination EID |
+-----+-----+-----+-----+-----+-----+-----+
IHL = IP-Header-Length

```

5.2. Формат заголовка LISP IPv6-in-IPv6



5.3. Описание полей туннельного заголовка

Inner Header (IH)

Внутренним является заголовок дейтаграммы, полученной от хоста-источника [RFC0791] [RFC8200] [RFC2474]. IP-адреса отправителя и получателя являются EID.

Outer Header (OH)

Внешний заголовок добавляется в начало маршрутизатором ITR и адресные поля в нем являются RLOC, полученные из кэша EID-to-RLOC Map-Cache входного маршрутизатора. Номер протокола IP является UDP (17) из [RFC0768]. Бит запрета фрагментирования (Don't Fragment или DF) в поле Flags устанавливается по правилам параграфов 7.1 и 7.2.

UDP Header

Заголовок UDP содержит выбранный ITR при инкапсуляции порт источника. В разделе 12 указаны детали алгоритма хэширования при выборе номера порта на основе квинтета (5-tuple) из внутреннего заголовка. В качестве порта получателя **должен** указываться выделенный IANA порт 4341.

UDP Checksum

В поле UDP Checksum маршрутизатору ITR **следует** помещать 0 для инкапсуляции IPv4 [RFC0768] или IPv6 [RFC6935] [RFC6936]. При получении пакета с нулевым значением UDP Checksum маршрутизатором ETR тот **должен** воспринимать пакет для декапсуляции. Когда ITR передаёт ненулевое значение UDP Checksum, он **должен** помещать в это поле корректно рассчитанную контрольную сумму. Когда ETR получает такой пакет, он **может** проверить значение контрольной суммы и при несовпадении **должен** отбросить пакет без уведомления отправителя. Если ETR не проверяет контрольную сумму, он **должен** воспринять пакет для декапсуляции. Обработка нулевой контрольной суммы UDP при использовании IPv6 для всех протоколов туннелирования, включая LISP, выполняется в соответствии с [RFC6936].

UDP Length

Поле UDP Length для инкапсулированного в IPv4 пакета содержит сумму значения поля IPv4 Total Length во внутреннем заголовке и размеров заголовков UDP и LISP. При инкапсуляции IPv6 в поле UDP Length указывается сумма значения поля IPv6 Payload во внутреннем заголовке, размера заголовка IPv6 (40 октетов), а также размера заголовков UDP и LISP.

N

Бит присутствия nonce. Установленный (1) бит указывает, что 24 младших бита из первого 32-битового слова в заголовке LISP содержат nonce (см. 10.1. Алгоритм Echo-Nonce). Биты N и V **недопустимо** устанавливать в одном пакете. При получении такого пакета ETR **должен** трактовать поле Nonce/Map-Version как значение nonce.

L

Флаг включения поля Locator-Status-Bits. При установленном бите второе 32-битовое слово заголовка LISP содержит Locator-Status-Bits.

```

x 1 x x 0 x x x
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|N|L|E|V|I|R|K|K|      Nonce/Map-Version      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Locator-Status-Bits      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

E

Флаг запроса Echo-Nonce, который **должен** игнорироваться и не имеет значения при сброшенном (0) флаге N. При установленных (1) флагах N и E маршрутизатор ITR запрашивает возврат значения поля Nonce в пакетах с инкапсуляцией LISP, когда ITR выступает также и в качестве ETR (см. 10.1. Алгоритм Echo-Nonce).

V

Флаг присутствия поля Map-Version, при установке (1) которого бит N **должен** быть сброшен (0). Детали версий отображения описаны в [RFC9302]. Установка (1) этого бита показывает, что заголовок LISP имеет формат

```

0 x 0 1 x x x x
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|N|L|E|V|I|R|K|K| Source Map-Version | Dest Map-Version |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Instance ID/Locator-Status-Bits      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

I

Флаг Instance ID (см. 8. Использование виртуализации и разделения с LISP). При установленном (1) бите поле Locator-Status-Bits сокращается до 8 битов, а 24 старших бита второго слова содержат Instance ID. При сброшенном (0) бите L младшие 8 битов передаются сброшенными (0) и игнорируются при получении. Формат заголовка LISP показан ниже.

```

x x x x 1 x x x
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|N|L|E|V|I|R|K|K|      Nonce/Map-Version      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Instance ID      |      LSBs      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

R

Резерв на будущее. При передаче бит **должен** сбрасываться (0), а при получении **должен** игнорироваться.

KK

Два бита KK указывают использование шифрования для инкапсулированных пакетов. Значение 00 указывает, что пакет не шифруется. Подробности описаны в [RFC8061].

LISP Nonce

Поле LISP Nonce представляет собой 24-битовое случайное значение, создаваемое ITR при установленном (1) бите N. Алгоритм создания Nonce определяется реализацией, но требуется генерировать разные значения при передаче по разным RLOC. Nonce применяется также при установленном (1) бите E для запроса возврата значения другой стороной в ответных пакетах. Если бит E сброшен (0), а N установлен (1), удаленный маршрутизатор ITR возвращает (эхо) запрошенное ранее значение Echo-Nonce или указывает случайное значение (см. 10.1. Алгоритм Echo-Nonce). Когда сброшены оба флага N и V (N=0, V=0), поля Nonce и Map-Version заполняются нулями, а при получении игнорируются.

LISP Locator-Status-Bits (LSBs)

При установленном (1) флаге L поле Locator-Status-Bits в заголовке LISP устанавливается ITR для указания маршрутизатору ETR состояния up/down для локаторов на сайте источника. Каждому RLOC в Map-Reply назначается номер от 0 до n-1 (n - число RLOC в записи отображения). Биты Locator-Status-Bits нумеруются от 0 до n-1, начиная с младшего бита поля. Поле имеет размер 32 бита при сброшенном (0) флаге I и 8 битов при I=1. Когда бит в Locator-Status-Bits установлен (1), ITR указывает маршрутизатору ETR, что локатор RLOC, связанный с этим битом, активен (up). В разделе 10 описано, как ITR может определить статус маршрутизаторов ETR на том же сайте. При наличии у сайта множества EID-Prefix, приводящего к множеству отображений (каждое может иметь свой набор Locator-Set), установка Locator-Status-Bits в инкапсулированном пакете **должна** соответствовать отображению для EID-Prefix, соответствующего адресу EID во внутреннем заголовке (по максимальному совпадению). Если LSB для индивидуального локатора имеет значение 1, существует хотя бы один RLOC с этим адресом и ETR считается работающим (up).

При инкапсуляции маршрутизаторы ITR и PITR выполняют указанные ниже правила.

- Поле TTL (Hop Limit для IPv6) **следует** копировать из поля TTL во внутреннем заголовке.
- В поле DSCP (Traffic Class для IPv6) **следует** копировать значение поля IPv4 DSCP (Traffic Class для IPv6) из внутреннего заголовка. Рекомендации для этого даны в [RFC2983].
- Биты явного уведомления о перегрузке IPv4 (Explicit Congestion Notification или ECN) и биты 6 - 7 поля IPv6 Traffic Class требуют особой обработки для предотвращения игнорирования индикации перегрузки, как указано в [RFC6040].

При декапсуляции маршрутизаторы ETR и PETR выполняют указанные ниже правила.

- В поле внутреннего заголовка IPv4 TTL (Hop Limit для IPv6) **должно** копироваться значение TTL (Hop Limit) из внешнего заголовка, если значение во внешнем заголовке меньше значения во внутреннем. Отказ от такой проверки может приводить к росту TTL (Hop Limit) во внутреннем заголовке в результате цикла инкапсуляции-декапсуляции. Проверка также выполняется при начальной инкапсуляции, когда пакет приходит в ITR или PITR для сайта LISP.

- Поле IPv4 DSCP (Traffic Class для IPv6) из внешнего заголовка **следует** копировать во внутренний заголовок. Рекомендации для этого даны в [RFC2983].
- Биты явного уведомления о перегрузке IPv4 (Explicit Congestion Notification или ECN) и биты 6 - 7 поля IPv6 Traffic Class требуют особой обработки для предотвращения игнорирования индикации перегрузки, как указано в [RFC6040]. Отметим, что имеются реализации, копирующие поле ECN из внешнего заголовка во внутренний, хотя [RFC6040] рекомендует не делать этого. Реализациям **рекомендуется** следовать поведению, описанному в [RFC6040].

Отметим, что в случаях, когда ETR/PETR является также ITR/PITR и заново инкапсулирует пакеты после декапсуляции, поле TTL во внешнем заголовке в результате будет уменьшаться на 1.

Копирование TTL служит двум целям - во-первых, это сохраняет дистанцию, предполагаемую для прохождения пакетом, во-вторых, что более важно, позволяет предотвратить петли в случае заикливания туннелей при ошибочной настройке.

Некоторые xTR, PETR и PITR выполняют повторную инкапсуляцию и им нужна особая обработка полей ECN. Поскольку повторная инкапсуляция состоит из декапсуляции и последующей новой инкапсуляции, биты ECN **должны** обрабатывать в каждой из операций, как указано выше.

Протокол плоскости данных LISP не совместим с [RFC6830] и не имеет явной поддержки будущих изменений протокола (например, явного поля версии). Однако плоскость управления LISP [RFC9301] позволяет ETR регистрировать возможности плоскости данных с помощью новых типов канонического формата адресов (LISP Canonical Address Format или LCAF) [RFC8060]. За счёт этого ITR может узнать возможности плоскости данных ETR и применять соответствующую инкапсуляцию. Спецификация новых типов и механизмов LCAF, а также их применения выходит за рамки этого документа.

6. Кэш сопоставлений EID с RLOC в LISP

ITR и PITR поддерживают кэширование по запросам в LISP EID-to-RLOC Map-Cache, куда включаются отображения EID-Prefix на Locator-Set. Кэш применяется для инкапсуляции пакетов из пространства EID в RLOC точки присоединения к сети. Когда ITR или PITR получает пакет со своего сайта LISP для внешнего адресата, выполняется поиск по максимальному соответствию с EID в Map-Cache. При успешном поиске Locator-Set из Map-Cache применяется для передачи пакета в топологическое местоположение EID. Если поиск не даёт результата ITR/PITR требуется найти отображение с помощью протокола плоскости управления LISP [RFC9301]. Пока отображение отыскивается и извлекается, ITR/PITR может отбрасывать или буферизовать пакеты. Этот документ не даёт конкретных рекомендаций для таких случаев и разработчики должны решать этот вопрос самостоятельно, обеспечивая желаемое поведение реализации LISP. После распознавания отображения оно сохраняется в локальном Map-Cache для пересылки последующих пакетов в тот же EID-Prefix.

Map-Cache - это локальный кэш отображений, записи в котором сохраняются в течение заданного срока (Time to Live). Записи могут обновляться более свежими данными, как описано в разделе 13. Изменение содержимого отображений EID на RLOC. Кроме того, Map-Cache содержит сведения о доступности EID и RLOC, а также использует механизмы сведений о доступности LISP для проверки достижимости RLOC (см. 10. Доступность локатора маршрутизации).

7. Обработка больших инкапсулированных пакетов

В этом разделе предлагаются два механизма работы с пакетами, размер которых превышает Path MTU (PMTU) между ITR и ETR.

Разработчикам **следует** самостоятельно выбирать реализацию механизма с поддержкой состояния или без такой поддержки. Можно применять оба варианта или ни одного, поскольку решение вопросов, связанных с MTU, принимается ITR локально, а сайты с разными механизмами могут взаимодействовать между собой.

Оба механизма применимы к повторной инкапсуляции и рекурсивным туннелям, поскольку действия для ITR применимы и на TE-ITR.

7.1. Решение для обработки MTU без учёта состояний

Решение без учёта состояний при обработке ITR проблем с MTU описано ниже.

1. Определяется число октетов H, добавляемых ITR во внешний заголовок перед пакетом, с учётом размера заголовков UDP и LISP.
2. Определяется число октетов L для максимального размера пакетов, которые ITR может передавать ETR без необходимости их фрагментирования на ITR и промежуточных маршрутизаторах. Сетевой администратор сайта LISP должен выбрать значение L, позволяющее избежать проблем с MTU.
3. Определяется архитектурная константа S для максимального размера пакетов (в октетах), которые ITR **должен** воспринимать от источника с учётом эффективного значения MTU. $L = S + H$.

Когда ITR получает пакет от интерфейса в сторону сайта и добавка H октетов инкапсуляции ведёт к превышению L (размер пакета от источника больше S), он решает проблему MTU, деля исходный пакет на два фрагмента одинаковых размеров, а затем добавляет в начало каждого фрагмента заголовок LISP. Размер инкапсулированных фрагментов составит $(S/2 + H)$, что меньше оценки ITR для PMTU между ITR и соответствующим ETR.

ETR считает принятые инкапсулированные фрагменты отдельными инкапсулированными пакетами и вырезает из них заголовки LISP, а затем пересылает каждый фрагмент целевому получателю на своём сайте. Этот сайт собирает фрагменты в одну дейтаграмму IP, соответствующую переданной источником. Отметим, что сборка может выполняться на ETR, если инкапсулированный пакет был фрагментирован маршрутизатором ITR или после него.

Это поведение **должно** быть реализовано в ITR лишь для исходных пакетов со сброшенным (0) битом запрета фрагментирования. Если бит DF установлен в заголовке IP или пакет относится к протоколу IPv6, ITR будет

отбрасывать пакет, если его размер превышает L (после добавления заголовка инкапсуляции) и передавать источнику сообщение ICMPv4 Unreachable/Fragmentation Needed или ICMPv6 Packet Too Big (PTB) со значением $S = (L - H)$.

При использовании для инкапсуляции внешнего заголовка IPv4 **следует** устанавливать (1) в нем флаг DF, чтобы избежать сборки на маршрутизаторе ETR. Реализация **может** сбрасывать (0) флаг DF в таких заголовках, если имеются веские основания предполагать наличие неразрешимых проблем с PMTU между ITR и принимающим ETR.

Рекомендуется устанавливать $L = 1500$. Дополнительные сведения о MTU в сети и вопросах фрагментации приведены в [RFC4459].

7.2. Решение для обработки MTU с учётом состояний

Решение с учётом состояний при обработке ITR проблем с MTU описано ниже.

1. ITR сохраняет эффективное состояние MTU для каждого локатора в записи Map-Cache. Эффективным значением MTU является размер пакета, который ядро сети может доставить по пути между ITR и ETR.
2. Когда инкапсулированный в IPv4 пакет с $DF = 1$ превышает размер, поддерживаемый ядром сети, один из промежуточных маршрутизаторов пути передаёт ITR сообщение ICMPv4 Unreachable/Fragmentation Needed. ITR анализирует сообщение ICMP для определения локатора, на который влияет смена эффективного MTU и записывает новое значение MTU в Map-Cache.
3. Когда ITR получает из внутренней сети сайта пакет с размером больше эффективного MTU в записи Map-Cache, связанной с EID получателя пакета, ITR передаёт источнику этого пакета сообщение ICMPv4 Unreachable/Fragmentation Needed. Размер пакета, анонсируемый ITR в сообщении ICMP, составляет эффективное значение MTU за вычетом заголовка инкапсуляции LISP.

Хотя этот механизм требует отслеживать состояния, он превосходит механизм фрагментации IP без учёта состояния, поскольку не требует от получателя сборки фрагментированных ITR пакетов.

Следует отметить, что применение пакетов ICMP для определения PMTU, как описано в [RFC1191] и [RFC8201], может приводить к неоптимальному поведению при потере пакетов ICMP или наличии за пределами пути злоумышленников, передающих обманные пакеты ICMP. Возможные меры снижения негативного влияния включают взаимодействие ITR и ETR с тестовыми пакетами [RFC4821] [RFC8899] или сохранение на ITR больших пакетов для проверки их соответствия пакетам, указанным в сообщениях ICMP Fragmentation Needed или PTB.

8. Использование виртуализации и разделения с LISP

В некоторых случаях требуется разделение на уровне EID. Например, это относится к развёртываниям с перекрывающимися адресами, правилами изоляции трафика или виртуализацией со множеством арендаторов. Для таких случаев применяются идентификаторы экземпляров - Instance ID.

Instance ID можно передавать в пакетах с инкапсуляцией LISP. ITR, добавляющий заголовок LISP будет копировать 24-битовое значение, используемое маршрутизатором LISP для однозначного указания пространства адресов. Значение копируется в поле Instance ID заголовка LISP а для флага I устанавливается значение 1.

Когда ETR декапсулирует пакет Instance ID из заголовка LISP используется в качестве идентификатора таблицы пересылки, применяемой для поиска EID получателя.

В качестве Instance ID может служить, например, тег 802.1Q VLAN или идентификатор VPN, помещаемый в 24-битовое поле Instance ID. Применение LISP в VPN подробно рассмотрено в [LISP-VPN]. Отметим, что поле Instance ID не защищено и находящийся на пути злоумышленник может менять его и, например, разрешать взаимодействие между изолированными VLAN.

Участники развёртывания LISP должны согласовать между собой применение значений Instance ID. EID источника и получателя **должны** относиться к одному Instance ID.

Instance ID **не следует** применять с перекрывающимися адресами IPv6 EID.

9. Выбор локатора маршрутизации

Map-Cache содержит состояние, используемое ITR и PITR для инкапсуляции пакетов. Когда ITR или PITR принимает пакет с сайта LISP для внешнего адресата выполняется поиск по максимальному совпадению EID в Map-Cache (см. 6. Кэш сопоставлений EID с RLOC в LISP). Поиск возвращает набор Locator-Set со списком RLOC, соответствующих топологическому расположению EID. С каждым RLOC в Locator-Set связан приоритет (Priority) и вес (Weight), используемые для выбора RLOC при инкапсуляции.

Выбирается RLOC с наименьшим значением Priority. RLOC с Priority=255 **недопустимо** использовать для пересылки. При наличии RLOC с одинаковым приоритетом значение Weight задаёт распределение трафика между ними. Значение Weight представляет относительный вес общего числа пакетов, соответствующих записи отображения.

Ниже рассмотрено несколько вариантов выбора RLOC и доступные элементы управления.

- Серверная сторона возвращает 1 локатор RLOC и клиентская сторона применяет лишь его. Выбор локатора полностью принадлежит серверной стороне.
- Серверная сторона возвращает список RLOC, часть которых имеет одинаковое (лучшее) значение Priority. Клиент может использовать эти локаторы с весовыми коэффициентами, заданными на стороне сервера. В этом случае сервер контролирует набор локаторов и распределение трафика между ними. Клиентская сторона может выбрать RLOC (с приоритетом, отличным от 255) не из подмножества списка, если она решает, что это подмножество недоступно. Здесь имеется некоторое распределение управления - сервер определяет список RLOC и распределение нагрузки между ними, а клиент может использовать другие локаторы, если RLOC из списка недоступны.

- Серверная сторона устанавливает Weight=0 для списка подмножества RLOC. В этом случае клиентская сторона выбирает способ распределения трафика между элементами подмножества. Механизмы распределения трафика рассмотрены в разделе 12. Хэширование локаторов маршрутизации. Управление распределено между серверной стороной, задающей список, и клиентской стороной, определяющей распределение нагрузки. Клиент и в этом случае может использовать другие локаторы, если RLOC из предоставленного сервером списка недоступны.
- Любая из сторон (наиболее вероятно, ETR на стороне сервера) решает «собрать» RLOC. Например, если ETR серверной стороны собирает RLOC, ITR на стороне клиента возлагает на этот ETR ответственность за двухстороннюю доступность и предпочтения RLOC. ETR на стороне сервера собирает RLOC клиентского ITR, кэшируя EID источника из внутренних заголовков и RLOC источника из внешних заголовков принятых пакетов. ITR на стороне клиента контролирует возврат трафика и может, как вариант, использовать RLOC источника из внешнего заголовка, который может затем добавляться в список, используемый ETR на серверной стороне для возврата трафика. Поскольку в этом случае Priority и Weights не предоставляются, ETR на стороне сервера **должен** предполагать, что RLOC, применяемые ITR на стороне клиента имеют наилучшее значение Priority с Weight = 0.

Поскольку кодирование EID-Prefix не может передаваться в пакетах данных, EID-to-RLOC Map-Cache на туннельных маршрутизаторах может стать чрезмерно большим. Со сбором связано несколько важных соображений. «Собранная» запись Map-Cache сохраняется и применяется лишь в течение **рекомендованного** интервала в 3 секунды, ожидая проверки, которая **должна** выполняться путём отправки Map-Request по EID источника (IP-адрес отправителя во внутреннем заголовке) полученного инкапсулированного пакета. Отклик на проверочный Map-Request служит для заполнения записи Map-Cache для «собранного» EID с сохранением и использованием её в течение интервала, заданного полем Time to Live в полученном Map-Reply. При сохранении проверенной записи Map-Cache сбор данных больше не выполняется для последующих пакетов с EID источника, соответствующим EID-Prefix в проверенной записи. Этот механизм «сбора» **недопустимо** применять через общедоступную сеть Internet и **следует** использовать лишь в доверенных, изолированных развёртываниях. Безопасность механизма обсуждается в разделе 16.

RLOC из сообщений EID-to-RLOC предполагаются достижимыми, если бит R [RFC9301] для записи Locator имеет значение 1. При сброшенном (0) бите R маршрутизаторам ITR и PITR **недопустимо** инкапсулировать в этот RLOC. Ни сведения из Map-Reply, ни данные, сохранённые в базе отображений не обеспечивают информации о достижимости RLOC. Отметим, что достижимость не является частью системы отображения и определяется с использованием одного или нескольких алгоритмов проверки доступности RLOC, описанных в следующем разделе.

10. Доступность локатора маршрутизации

В настоящее время имеется несколько механизмов плоскости данных для определения доступности RLOC. Отметим, что в [RFC9301] описаны другие механизмы, основанные на плоскости управления.

1. ETR **может** проверить биты LSB в заголовке LISP инкапсулированного пакета данных, принятого от ITR. Если ETR выступает также в качестве ITR и имеет трафик для возврата сайту исходного ITR, он может использовать эти сведения при выборе RLOC.
2. Когда ETR получает инкапсулированный пакет от ITR, RLOC источника из внешнего заголовка, вероятно, будет доступен. Отметим, что в некоторых случаях RLOC во внешнем заголовке может быть обманным полем.
3. Пара ITR - ETR может использовать алгоритмы определения доступности, описанные в этом параграфе.

При определении статуса up/down для локатора путём проверки LSB из пакета данных с инкапсуляцией LISP маршрутизатор ETR будет получать от инкапсулирующего ITR актуальное состояние доступности всех ETR на сайте. Основанные на CE маршрутизаторы ITR на сайте источника могут определить достижимость друг друга, используя IGP, как указано ниже.

- При нормальных условиях каждый ITR будет анонсировать принятый по умолчанию маршрут в IGP сайта.
- При отказе ITR или восходящего канала к устройству PE для принятого по умолчанию маршрута будет возникать тайм-аут или он будет отзван.

Таким образом, каждый ITR может видеть наличие или отсутствие принятых по умолчанию маршрутов, созданных другими, чтобы определить установку LSB для них.

Когда ITR сайта не развёрнуты на маршрутизаторах CE, IGP всё равно можно использовать для определения доступности локаторов при условии их внедрения в IGP. Обычно это делается с помощью адреса /32 (хост) на интерфейсе loopback.

RLOC, указанные в Map-Reply, имеют номера от 0 до n-1. Биты LSB в пакете с инкапсуляцией LISP нумеруются от 0 до n-1, начиная с младшего. Например, если RLOC в третьей позиции (порядковый номер 2) Map-Reply не активен, все ITR сайта будут сбрасывать этот бит (xxxx x0xx) в поле Locator-Status-Bits инкапсулируемых пакетов.

Когда xTR решает применять Locator-Status-Bits для воздействия на сведения о достижимости, он выполняет соответствующие действия. ETR, деинкапсулирующие пакеты, проверяют наличие изменений в поле Locator-Status-Bits. Если бит сбрасывается (переход от 1 к 0), ETR, выступающий также в качестве ITR, будет воздерживаться от инкапсуляции пакетов для RLOC, указанного как недоступный (down). Использование этого RLOC будет возобновлено лишь при возврате соответствующего бита LSB в состояние 1. Биты LSB связываются с Locator-Set по префиксам EID, поэтому когда локатор становится недоступным, бит LSB, соответствующий позиции этого локатора в списке из последнего Map-Reply, сбрасывается (0) для данного EID-Prefix.

Locator-Status-Bits **недопустимо** использовать через общую сеть Internet и **следует** применять лишь в доверенных, изолированных средах. Кроме того, Locator-Status-Bits **следует** сочетать с Map-Versioning [RFC9302] для предотвращения «состязания», когда биты LSB интерпретируются не для того локатора RLOC, которому они предназначены. Связанные с этим вопросы безопасности рассмотрены в разделе 16.

Если ITR инкапсулирует пакет для ETR и пакет принимается и декапсулируется ETR, предполагается (но не подтверждается ITR), что RLOC маршрутизатора ETR достижим. В большинстве случаев ETR может также достичь ITR, но не может считать это истинным, поскольку путь может быть асимметричным. При одностороннем потоке трафика от ITR к ETR маршрутизатору ITR **не следует** считать отсутствие обратного трафика указанием недоступности ETR. Вместо этого он **должен** использовать другой механизм определения достижимости.

Соображения безопасности из раздела 16, относящиеся к достижимости плоскости данных, применимы и к описанным здесь механизмам определения доступности RLOC.

10.1. Алгоритм Echo-Nonce

Когда данные передаются в двух направлениях между локаторами разных сайтов, может применяться механизм плоскости данных «попсе-эхо» (nonce echoing) для определения достижимости между ITR и ETR. Если ITR хочет запросить попсе-эхо, он устанавливает флаги N и E, а также помещает 24-битовое значение [RFC4086] в заголовок LISP следующего инкапсулируемого пакета данных. Когда этот пакет приходит к ETR, инкапсулированный пакет пересылается обычным путём. Если ETR является xTR (совмещён с ITR), он затем передаёт пакет данных ITR (когда тот является xTR, совмещённым с ETR), включая в него полученное значение попсе, устанавливая бит N и сбрасывая бит E. ITR видит отражённое значение попсе и понимает, что путь между ним и ETR доступен.

ITR будет устанавливать биты E и N в каждом пакете, пока он находится в состоянии Echo-Nonce-request. Время, в течение которого ITR ожидает обработки отражённого попсе, определяющей доступность пути, является переменным и зависит от реализации.

Если ITR получает пакеты от ETR, но не видит в них отражённых попсе, находясь в состоянии Echo-Nonce-request, это говорит о недоступности пути к ETR. Это решение **может** быть отменено другим алгоритмом проверки доступности локаторов. После того, как ITR определит, что путь к ETR не работает, он может переключиться на другой Locator для этого EID-Prefix.

Отметим, что термины ITR и ETR здесь относительны и оба устройства **должны** реализовать функции ITR и ETR для работы механизма Echo-Nonce.

ITR и ETR **могут** одновременно оказаться в состоянии Echo-Nonce-request. Число передаваемых пакетов или время, в течение которого передаются пакеты Echo-Nonce, зависит от настроек реализации. Маршрутизатор xTR, получающий пакеты с запросом Echo-Nonce, выходит из состояния Echo-Nonce и устанавливает таймер Echo-Nonce-request-state, а по завершении его отсчёта возвращается в состояние Echo-Nonce.

Этот механизм не решает полностью проблему проверки доступности прямого пути, поскольку трафик может быть односторонним. Т. е. маршрутизатор ETR, получающий трафик на сайте, **может** не совпадать с ITR, передающим трафик с этого сайта, или возвращаемый сайтом трафик может просто отсутствовать.

Алгоритм Echo-Nonce является двухсторонним, т. е. если одна сторона устанавливает флаг E, а другая не включила Echo-Noncing, кодирование попсе не выполняется и запрашивающая сторона будет ошибочно считать, что локатор недоступен. ITR **следует** устанавливать бит E в инкапсулированных пакетах данных, когда ему известно, что на ETR включено Echo-Noncing. Это указывается флагом E в сообщении Map-Reply.

Многие реализации не анонсируют поддержку Echo-Nonce в сообщениях Map-Reply, поэтому для проверки доступности RLOC обычно применяется RLOC-Probing.

Механизм Echo-Nonce **недопустимо** применять в общедоступной сети Internet и он **должен** использоваться лишь в изолированных, доверенных средах (см. 16. Вопросы безопасности).

11. Доступность EID на сайте LISP

Сайт **может** быть многодомным и использовать два или более ETR. Хосты и инфраструктура сайта будут адресоваться с использованием одного или нескольких EID-Prefix, отображённых на RLOC соответствующих ETR в системе отображения. Одним из возможных вариантов отказа ETR является потеря связности с одним или несколькими EID-Prefix своего сайта. В таких случаях при отправке пакетов Map-Reply маршрутизатор ETR может сбрасывать (0) бит R, связанный с его локатором. Когда ETR служит также в качестве ITR, он может сбросить свой бит LSB в заголовке инкапсуляции данных.

Отмечено, что нет простых решений проблемы разделения сайта, поскольку трудно понять, какая часть EID-Prefix отделена и какие локаторы будут доступны в каждой из частей EID-Prefix. Отметим, что эта проблема присуща не только архитектуре LISP и на момент создания этого документа она существовала для многодомных сайтов, анонсирующих BGP в восходящем направлении.

12. Хэширование локаторов маршрутизации

Когда ETR представляет в сообщении Map-Reply отображение EID-RLOC, сохраняемое в Map-Cache запрашивающего ITR, Locator-Set для EID-Prefix **может** содержать разные значения Priority и Weight для каждого адреса локатора маршрутизации (Routing Locator Address). При наличии нескольких локаторов с лучшим приоритетом ITR может распределять трафик между соответствующими локаторами. Ниже приведён алгоритм, который ITR может использовать для пакета, адресованного EID, в отображении EID-RLOC.

1. Можно использовать хэш адреса отправителя и получателя или обычного квинтета (5-tuple). Обычно используемый хэш 5-tuple включает адреса отправителя и получателя, их номера портов TCP, UDP или SCTP¹ и поле протокола IP или следующего протокола IPv6 из пакета, созданного хостом сайта LISP. Если пакет не относится к TCP, UDP, SCTP, для расчёта хэш-значения применяются лишь адреса отправителя и получателя.
2. Хэш-значение делится на число локаторов в Locator-Set для отображения EID-RLOC.
3. Остаток будет иметь значение от 0 до числа локаторов минус 1 и применяется для выбора локатора из Locator-Set.

¹Stream Control Transmission Protocol - протокол управления потоковой передачей.

Выбор конкретного алгоритма, применяемого ITR для распределения нагрузки, выходит за рамки этого документа и не препятствует совместимости. Порт источника **следует** сохранять одинаковым для всех пакетов одного потока. Отметим также, что при инкапсуляции пакетов в LISP нужно устанавливать номер порта во внешнем заголовке UDP. Выбор хэшированного значения позволяет маршрутизаторам ядра, соединенным с агрегатом каналов (Link Aggregation Group или LAG) распределять инкапсулированные пакеты между каналами LAG. В противном случае маршрутизаторы ядра будут лишь видеть один поток, поскольку в пакетах указан адрес ITR как отправителя для пакетов, исходящих от разных EID на сайте. Предлагается использовать в качестве порта источника, рассчитанное ITR хэш-значение 5-tuple из внутреннего заголовка, как указано выше. Порт отправителя **следует** сохранять для всех пакетов одного потока.

Многие реализации маршрутизаторов ядра применяют хэш 5-tuple для распределения нагрузки между каналами LAG. 5-tuple включает адреса и порты отправителя и получателя, когда номер протокола в пакете указывает TCP или UDP. Поэтому для инкапсуляции LISP применяется UDP. Когда внешним заголовком является IPv6, **может** устанавливаться также метка потока, как задано в [RFC6438]. Когда внутренним заголовком является IPv6 и метка потока отлична от 0, она **может** включаться в расчёт хэш-значения.

13. Изменение содержимого отображений EID на RLOC

Поскольку в архитектуре LISP для хранения и извлечения сопоставлений EID-RLOC применяется схема кэширования, ITR может получить более своевременное отображение только путём повторения запроса. ITR могут не знать о смене отображения, а ETR не отслеживают, какие ITR запрашивали отображения. Для расширяемости такой подход желательно сохранить, но разработчикам нужно предоставить ETR способ смены их отображений и информирования о такой смене сайты, взаимодействующие с сайтом ETR.

В этом разделе описаны два механизма плоскости данных для обновления отображений EID-RLOC. Кроме того, в [RFC9301] задан механизм запросов (Solicit-Map-Request или SMR).

13.1. Locator-Status-Bits

Биты состояния локаторов (LSB) могут служить для отслеживания статуса локаторов (up-down) при изменении отображений EID-RLOC. При использовании LSB в системе LISP все туннельные маршрутизаторы LISP **должны** реализовать возможности как ITR, так и ETR (т. е. фактически быть xTR). В этом параграфе термин xTR-источник указывает xTR, передающий LSB, а xTR-получатель - xTR, принимающий LSB. Процедура описана ниже.

1. При добавлении или удалении записи для локатора в Locator-Set xTR-источник будет сообщать об этом, передавая сообщение уровня управления SMR [RFC9301] xTR-получателю. В этот момент xTR-источнику **недопустимо** использовать поле LSB, если флаг L сброшен (0), поскольку сайт xTR-получателя имеет устаревшие сведения. Отправитель xTR устанавливает таймер use-LSB.
2. При получении сообщения SMR, как указано в [RFC9301], получатель xTR извлекает обновлённые отображения EID-RLOC путём отправки сообщений Map-Request.
3. По завершении отсчёта таймера use-LSB отправитель xTR снова может использовать LSB с xTR-получателем для информирования о статусе локаторов (up или down). Значение таймера use-LSB зависит от развёртывания LISP, но оно должно быть достаточно велико, чтобы xTR-получатель мог извлечь обновлённые отображения EID-RLOC. **Рекомендуется** устанавливать для таймера use-LSB значение 5 минут.

13.2. Версии базы данных отображений

Когда имеется односторонний поток данных между ITR и ETR, а отображения EID-RLOC на ETR меняются, нужно сообщить ITR, чтобы тот мог прекратить инкапсуляцию для удалённых локаторов и начать использовать добавленные в Locator-Set.

ETR может передать сообщения Map-Reply с номером Map-Version [RFC9302] в EID-Record. Этот номер называют Destination Map-Version Number. Маршрутизаторы ITR включают Destination Map-Version Number в пакеты, инкапсулируемые для сайта.

ITR при инкапсуляции пакетов для ETR может указать свой номер Map-Version - Source Map-Version Number.

При наличии в записях EID-Record сообщений Map-Register [RFC9301] номера Map-Version он является для Map-Server [RFC9301] хорошим способом обеспечить для всех зарегистрированных на нем ETR синхронизацию версий отображения.

Более подробно версии базы данных рассмотрены в [RFC9302].

14. Групповая передача

Адрес multicast-группы, как задано в исходной архитектуре Internet, является идентификатором группы топологически независимых хостов-получателей. Представление такого адреса не задаёт местоположения получателей и для его указания нужен протокол групповой маршрутизации и создаваемое протоколом состояние сети.

В контексте LISP групповой адрес является сразу EID и RLOC, поэтому для адреса получателя не требуется особой семантики, поскольку он указан в заголовке IP. Таким образом, групповой адрес IP, указанный во внутреннем заголовке хостом-источником, будет служить EID получателя. Внешний заголовок IP (RLOC получателя), добавляемый маршрутизатором LISP, может использовать в качестве RLOC получателя тот же групповой адрес, а также групповой или индивидуальный локатор RLOC, полученный при поиске в системе отображения или иным способом.

В качестве RLOC источника ITR использует свой адрес IP во внешнем заголовке IP, как при обмене с обычными EID. Этот адрес RLOC, как и все остальные RLOC, **должен** быть глобально маршрутизируемым.

Имеется два подхода к LISP-Multicast [RFC6831] - один на основе обычной multicast-маршрутизации в базовой сети без Mapping System, другой с использованием в базовой сети индивидуальной маршрутизации с поддержкой Mapping System (они описаны в [RFC6831] и [RFC8378], соответственно). Детали LISP-Multicast и взаимодействия с сайтами без поддержки LISP рассмотрены в [RFC6831] и [RFC6832], соответственно.

15. Работа маршрутизаторов

Протокол LISP разработан для аппаратной реализации, дружественной к пересылке (hardware based and forwarding friendly). Для поэтапного внедрения LISP имеется несколько методов.

- Когда ETR принимает инкапсулированный в туннель пакет, внешний адрес получателя может не быть адресом этого маршрутизатора. Это осложняет плоскости управления получение пакетов от оборудования. Проблему можно смягчить созданием специальных записей таблицы пересылки (Forwarding Information Base или FIB) для EID-Prefix адресов EID, обслуживаемых ETR (тех, для которых маршрутизатор транслирует RLOC). Эти записи FIB помечаются флагом, указывающим, что пакет **следует** обработать в плоскости пересылки. Логика пересылки для проверки конкретного номера протокола IP не требуется. Есть несколько подтверждённых вариантов, где не потребовалось менять имеющееся оборудование для поддержки плоскости данных LISP.
- На ITR добавление в начало нового заголовка IP состоит из добавления октетов в строку кода аутентификации сообщения (Message Authentication Code или MAC) и добавление этой строки в начало в процессе исходящей инкапсуляции. Маршрутизаторы с поддержкой туннелей GRE¹ [RFC2784] или 6to4 [RFC3056] могут уже поддерживать это.
- Адрес источника пакета или интерфейс, на котором пакет был принят, могут служить для выбора экземпляра виртуальной маршрутизации и пересылки (Virtual Routing and Forwarding или VRF). Таблица маршрутизации VRF может служить для поиска отображений EID-RLOC.

Вопросы, связанные с управлением кэшем отображений, рассмотрены в разделе 16.

16. Вопросы безопасности

Далее рассматриваются соображения безопасности, применимые при внедрении LISP в средах, подробно описанным в параграфе 1.1. Сфера применимости.

Предложен необязательный механизм сбора (gleaning) для прямого получения сопоставлений из пакетов с инкапсуляцией LISP. В частности, xTR может изучать отображения EID-RLOC, просматривая RLOC и EID источника в инкапсулированных пакетах и помещая найденные сопоставления в свой Map-Cache. Атакующий извне пути может подменить EID источника, чтобы направить переданный трафик на EID жертвы. Если атакующий подменит RLOC, он сможет организовать DoS-атаку перенаправляя трафик на RLOC, возможно, перегружая её.

Плоскость данных LISP задаёт несколько механизмов отслеживания доступности RLOC. В этом контексте биты статуса локаторов (LSB), присутствия попсо и Echo-Nonсе в заголовке инкапсуляции LISP атакующий может изменять для организации DoS-атаки. Атакующий извне пути может подменить RLOC и или попсо маршрутизатора xTR жертвы для анонсирования ложных сведений о статусе доступности RLOC.

Примером таких атак является случай, когда размещённый вне пути злоумышленник может использовать механизм Echo-Nonсе, передавая маршрутизатору ITR пакеты данных со случайным значением попсо от фиктивного RLOC маршрутизатора ETR. Отметим, что у атакующего имеется лишь небольшой интервал времени, в течение которого ему нужно угадать значение попсо, отражение которого запросил маршрутизатор ITR. Цель заключается в том, чтобы убедить ITR, что RLOC маршрутизатора ETR доступен, даже если это не так. При успешной атаке ITR будет полагаться на ложный статус доступности RLOC маршрутизатора ETR, пока RLOC-Probing не обнаружит реальный статус. Этот интервал имеет порядок десятков секунд. Такие атаки можно смягчить предотвращая подмену RLOC в сети за счёт развёртывания uRPF² в соответствии с BCP 84 [RFC8704]. Для использования этой уязвимости расположенный вне пути злоумышленник должен передавать пакеты Echo-Nonсе с высокой скоростью. Если ITR не запрашивает попсо, он может защитить себя от ложных сведений о доступности.

Возможна проверка uRPF для LISP. При декапсуляции ETR может проверять корректность EID и RLOC по отображению EID-RLOC в Mapping System.

Map-Versioning - это механизм плоскости данных, используемый для сигнализации xTR-партнерам о смене локального отображения EID-RLOC, чтобы партнёры xTR использовали сигнальные сообщения плоскости управления LISP для извлечения свежего сопоставления. Злоумышленник может подменить поле Map-Version в заголовке инкапсуляции LISP и вызвать избыточную сигнализацию между xTR с целью их перегрузки. Вопросы безопасности использования Map-Versioning рассмотрены в [RFC9302].

Биты LSB, механизм Echo-Nonсе и Map-Versioning **недопустимо** применять в общедоступной сети Internet и **следует** использовать лишь в изолированных, доверенных средах. Кроме того, LSB **следует** сочетать с Map-Versioning для предотвращения состязаний, когда биты LSB относятся не к тем RLOC, для которых предназначены.

Реализациям и внедрениям LISP, допускающим фрагменты внешних заголовков пакетов IPv6 с инкапсуляцией LISP в качестве средства решения вопросов MTU, следует использовать в ETR методы, предотвращающие использования этого для DoS-атак. Можно использовать ограничение числа фрагментов, ожидающих сборки в ETR, RTR, PETR, и скорости восприятия таких пакетов.

17. Вопросы управления сетью

Соображения по инструментам оперативного управления стеком протоколов LISP приведены в [RFC7052] и [RFC6835].

18. Отличия от RFC 6830

С учётом опыта реализации после публикации [RFC6830] в документ были внесены указанные ниже изменения.

- Больше не используется ограничение на число заголовков LISP, добавляемых в начало пакета. Если приложению нужно более 2 заголовков LISP, реализация может поддерживать это. Однако **рекомендуется** применять не более 2 заголовков LISP.

¹Generic Routing Encapsulation - базовая инкапсуляция маршрутных данных.

²Unicast Reverse Path Forwarding - индивидуальная пересылка по обратному пути.

- Используются резервные флаги в заголовке LISP для [RFC8061]. Два младших бита 3-битового поля (KK) служат идентификатором ключа, а оставшийся бит сохранён как резервный.
- Сбор в плоскости данных для создания записей Map-Cache сделана необязательной. Любым реализациям ITR, которые зависят от сборки или предполагают, что удалённый ETR выполняет сбор, следует отказаться от этого. Проблем функциональной совместимости не возникает, поскольку процедуры заполнения Map-Cache в плоскости управления являются односторонними и служат типовым методом заполнения Map-Cache.
- Большинство изменений в этом документе, которые сократили его размер, связаны с переносом сообщений и процедур плоскости управления LISP в [RFC9301].

19. Взаимодействие с IANA

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

19.1. Номера портов LISP UDP

Агентство IANA выделило номер порта UDP 4341 для плоскости данных LISP с показанным ниже обновлением описания этого порта в реестре.

Таблица 1.

Имя службы	Номер порта	Транспортный протокол	Описание	Документ
lisp-data	4341	udp	Пакеты данных LISP	RFC 9300

20. Литература

20.1. Нормативные документы

- [RFC0768] Postel, J., "User Datagram Protocol", STD 6, [RFC 768](#), DOI 10.17487/RFC0768, August 1980, <<https://www.rfc-editor.org/info/rfc768>>.
- [RFC0791] Postel, J., "Internet Protocol", STD 5, [RFC 791](#), DOI 10.17487/RFC0791, September 1981, <<https://www.rfc-editor.org/info/rfc791>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", [RFC 2474](#), DOI 10.17487/RFC2474, December 1998, <<https://www.rfc-editor.org/info/rfc2474>>.
- [RFC2983] Black, D., "Differentiated Services and Tunnels", RFC 2983, DOI 10.17487/RFC2983, October 2000, <<https://www.rfc-editor.org/info/rfc2983>>.
- [RFC6040] Briscoe, B., "Tunnelling of Explicit Congestion Notification", RFC 6040, DOI 10.17487/RFC6040, November 2010, <<https://www.rfc-editor.org/info/rfc6040>>.
- [RFC6438] Carpenter, B. and S. Amante, "Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels", RFC 6438, DOI 10.17487/RFC6438, November 2011, <<https://www.rfc-editor.org/info/rfc6438>>.
- [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>>.
- [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>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, [RFC 8200](#), DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.
- [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>>.
- [RFC8704] Sriram, K., Montgomery, D., and J. Haas, "Enhanced Feasible-Path Unicast Reverse Path Forwarding", BCP 84, RFC 8704, DOI 10.17487/RFC8704, February 2020, <<https://www.rfc-editor.org/info/rfc8704>>.
- [RFC9301] Farinacci, D., Maino, F., Fuller, V., and A. Cabellos, Ed., "Locator/ID Separation Protocol (LISP) Control Plane", [RFC 9301](#), DOI 10.17487/RFC9301, October 2022, <<https://www.rfc-editor.org/info/rfc9301>>.
- [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>>.

20.2. Дополнительная литература

- [AFN] IANA, "Address Family Numbers", <<http://www.iana.org/assignments/address-family-numbers>>.
- [CHIAPPA] Chiappa, J., "Endpoints and Endpoint Names: A Proposed Enhancement to the Internet Architecture", 1999, <<http://mercury.lcs.mit.edu/~jnc/tech/endpoints.txt>>.
- [LISP-VPN] Moreno, V. and D. Farinacci, "LISP Virtual Private Networks (VPNs)", Work in Progress, Internet-Draft, draft-ietf-lisp-vpn-10, 3 October 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-lisp-vpn-10>>.

- [RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, [RFC 1034](#), DOI 10.17487/RFC1034, November 1987, <<https://www.rfc-editor.org/info/rfc1034>>.
- [RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", [RFC 1191](#), DOI 10.17487/RFC1191, November 1990, <<https://www.rfc-editor.org/info/rfc1191>>.
- [RFC2453] Malkin, G., "RIP Version 2", STD 56, [RFC 2453](#), DOI 10.17487/RFC2453, November 1998, <<https://www.rfc-editor.org/info/rfc2453>>.
- [RFC2677] Greene, M., Cucchiara, J., and J. Luciani, "Definitions of Managed Objects for the NBMA Next Hop Resolution Protocol (NHRP)", RFC 2677, DOI 10.17487/RFC2677, August 1999, <<https://www.rfc-editor.org/info/rfc2677>>.
- [RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", [RFC 2784](#), DOI 10.17487/RFC2784, March 2000, <<https://www.rfc-editor.org/info/rfc2784>>.
- [RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, DOI 10.17487/RFC3056, February 2001, <<https://www.rfc-editor.org/info/rfc3056>>.
- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <<https://www.rfc-editor.org/info/rfc3261>>.
- [RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, [RFC 4086](#), DOI 10.17487/RFC4086, June 2005, <<https://www.rfc-editor.org/info/rfc4086>>.
- [RFC4459] Savola, P., "MTU and Fragmentation Issues with In-the-Network Tunneling", RFC 4459, DOI 10.17487/RFC4459, April 2006, <<https://www.rfc-editor.org/info/rfc4459>>.
- [RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", [RFC 4760](#), DOI 10.17487/RFC4760, January 2007, <<https://www.rfc-editor.org/info/rfc4760>>.
- [RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", [RFC 4821](#), DOI 10.17487/RFC4821, March 2007, <<https://www.rfc-editor.org/info/rfc4821>>.
- [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>>.
- [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>>.
- [RFC6835] Farinacci, D. and D. Meyer, "The Locator/ID Separation Protocol Internet Groper (LIG)", RFC 6835, DOI 10.17487/RFC6835, January 2013, <<https://www.rfc-editor.org/info/rfc6835>>.
- [RFC6935] Eubanks, M., Chimento, P., and M. Westerlund, "IPv6 and UDP Checksums for Tunneled Packets", RFC 6935, DOI 10.17487/RFC6935, April 2013, <<https://www.rfc-editor.org/info/rfc6935>>.
- [RFC6936] Fairhurst, G. and M. Westerlund, "Applicability Statement for the Use of IPv6 UDP Datagrams with Zero Checksums", RFC 6936, DOI 10.17487/RFC6936, April 2013, <<https://www.rfc-editor.org/info/rfc6936>>.
- [RFC7052] Schudel, G., Jain, A., and V. Moreno, "Locator/ID Separation Protocol (LISP) MIB", RFC 7052, DOI 10.17487/RFC7052, October 2013, <<https://www.rfc-editor.org/info/rfc7052>>.
- [RFC7215] Jakab, L., Cabellos-Aparicio, A., Coras, F., Domingo-Pascual, J., and D. Lewis, "Locator/Identifier Separation Protocol (LISP) Network Element Deployment Considerations", RFC 7215, DOI 10.17487/RFC7215, April 2014, <<https://www.rfc-editor.org/info/rfc7215>>.
- [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>>.
- [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>>.
- [RFC8201] McCann, J., Deering, S., Mogul, J., and R. Hinden, Ed., "Path MTU Discovery for IP version 6", STD 87, [RFC 8201](#), DOI 10.17487/RFC8201, July 2017, <<https://www.rfc-editor.org/info/rfc8201>>.
- [RFC8899] Fairhurst, G., Jones, T., Tüxen, M., Rüngeler, I., and T. Völker, "Packetization Layer Path MTU Discovery for Datagram Transports", [RFC 8899](#), DOI 10.17487/RFC8899, September 2020, <<https://www.rfc-editor.org/info/rfc8899>>.
- [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>>.

Благодарности

Первая благодарность Dave Oran за посеянные семена исходных идей LISP. Его консультации продолжают приносить пользу авторам LISP.

Особая признательность выражается Noel Chiappa за многолетнее подталкивание к архитектуре отделения местоположения от идентификации, а также за подробные обзоры архитектуры и документов LISP в сочетании с энтузиазмом, направленным на то, чтобы сделать LISP практичным для постепенного внедрения в Internet.

Первоначальные авторы благодарят множество людей, которые внесли свой вклад в обсуждение идей при подготовке этого предложения. Среди них Scott Brim, Andrew Partan, John Zwiebel, Jason Schiller, Lixia Zhang, Dorian Kim, Peter Schoenmaker, Vijay Gill, Geoff Huston, David Conrad, Mark Handley, Ron Bonica, Ted Seely, Mark Townsley, Chris Morrow,

Brian Weis, Dave McGrew, Peter Lothberg, Dave Thaler, Eliot Lear, Shane Amante, Ved Kifle, Olivier Bonaventure, Luigi Iannone, Robin Whittle, Brian Carpenter, Joel Halpern, Terry Manderson, Roger Jorgensen, Ran Atkinson, Stig Venaas, Iljitsch van Beijnum, Roland Bless, Dana Blair, Bill Lynch, Marc Woolward, Damien Saucez, Damian Lezama, Attila De Groot, Parantap Lahiri, David Black, Roque Gagliano, Isidor Kouvellas, Jesper Skriver, Fred Templin, Margaret Wasserman, Sam Hartman, Michael Hofling, Pedro Marques, Jari Arkko, Gregg Schudel, Srinivas Subramanian, Amit Jain, Xu Xiaohu, Dhirendra Trivedi, Yakov Rekhter, John Scudder, John Drake, Dimitri Papadimitriou, Ross Callon, Selina Heimlich, Job Snijders, Vina Ermagan, Fabio Maino, Victor Moreno, Chris White, Clarence Filsfils, Alia Atlas, Florin Coras, Alberto Rodriguez.

Эта работа началась в исследовательской группе Routing (RRG) под эгидой IRTF. Индивидуальное представление превратилось в документ рабочей группы IETF LISP, который стал этим RFC.

Рабочая группа LISP хотела бы выразить особую благодарность Jari Arkko (Internet Area AD во время подготовки документов LISP к IESG Last Call) за его детальные обзоры и комментарии на 7 Working Group Last Call при подготовке документов в качестве Standards Track RFC.

Текущие авторы хотели бы выразить искреннюю признательность всем, кто помогал представить LISP в процессе IETF Standards Track. Среди них 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 архитектуру и протоколы LISP в плане безопасности, расширяемости и отказоустойчивости.

Адреса авторов

Dino Farinacci

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

Vince Fuller

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

Dave Meyer

1-4-5.net
Email: dmm@1-4-5.net

Darrel Lewis

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

Albert Cabellos (редактор)

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