

Internet Engineering Task Force (IETF)
Request for Comments: 9302
Obsoletes: 6834
Category: Standards Track
ISSN: 2070-1721

L. Iannone
Huawei Technologies France
D. Saucez
Inria
O. Bonaventure
Universite catholique de Louvain
October 2022

Locator/ID Separation Protocol (LISP) Map-Versioning

Версии отображений протокола LISP

Аннотация

Этот документ описывает механизм версий отображений (Map-Versioning) протокола LISP¹, который позволяет указывать в пакетах отображения идентификаторов конечных точек на локаторы маршрутизации (Endpoint-ID-to-Routing-Locator или EID-RLOC), применяемые при инкапсуляции пакетов данных LISP. Этот подход основан на связывании номера версии с отображениями EID-RLOC и доставки этого номера в заголовке LISP пакетов, инкапсулированных в LISP. Версии отображений LISP особенно полезны для информирования входных (Ingress Tunnel Router или ITR) и выходных (Egress Tunnel Router или ETR) маршрутизаторов о смене версии отображения, применяемого при инкапсуляции пакетов. Механизм необязателен и не мешает не поддерживающим его реализациям, поскольку в заголовках LISP и записях отображений биты Map-Versioning можно без опаски игнорировать в маршрутизаторах ITR и ETR, не поддерживающих или не желающих использовать этот механизм.

Этот документ отменяет RFC 6834, где была задана исходная, экспериментальная спецификация механизмов.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF² и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG³. 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/rfc9302>.

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
2. Уровни требований.....	2
3. Определения терминов.....	2
4. Заголовки LISP и номера Map-Version.....	2
5. Запись отображения и Map-Version.....	3
6. Номер EID-RLOC Map-Version.....	3
6.1. Null Map-Version.....	3
7. Работа с номерами Map-Version.....	4
7.1. Обработка Map-Version получателя.....	4
7.2. Обработка Map-Version источника.....	4
8. Вопросы безопасности.....	5
9. Вопросы внедрения.....	5
10. Взаимодействие с IANA.....	5
11. Литература.....	5
11.1. Нормативные документы.....	5
11.2. Дополнительная литература.....	6
Приложение А. Преимущества и применение Map-Versioning.....	6
А.1. Map-Versioning и односторонний трафик.....	6
А.2. Map-Versioning и межсетевое взаимодействие Interworking.....	6
А.2.1. Map-Versioning и Proxy-ITR.....	6
А.2.2. Map-Versioning и LISP-NAT.....	6
А.2.3. Map-Versioning и Proxy-ETR.....	7

¹Locator/ID Separation Protocol - протокол разделения локаторов и идентификаторов.

²Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

³Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

А.3. Отключение и отзыв RLOC.....	7
Адреса авторов.....	7

1. Введение

Этот документ описывает механизм Map-Versioning, используемый для информирования об изменениях сопоставлений идентификаторов конечных точек с локаторами маршрутизаторов (EID-RLOC), применяемых в контексте протокола LISP [RFC9300] [RFC9301] для инкапсуляции пакетов. Механизм не препятствует работе входных (Ingress) и выходных (Egress) маршрутизаторов туннелей (xTRs), не поддерживающих или не использующих эту функциональность. Архитектура LISP описана [RFC9299] и предполагается знакомство читателя с этим вводным документом.

Этот документ отменяет [RFC6834], где была задана исходная, экспериментальная спецификация механизмов.

Базовым механизмом является связывание номера версии (Map-Version) с каждым отображением LISP EID-RLOC и доставка этого номера в связанном с LISP заголовке. При смене отображения ему назначается новый номер версии. Сменой сопоставления EID-RLOC может быть изменение набора RLOC, такое как добавление, удаление, изменение приоритета или веса одного или нескольких RLOC.

При использовании Map-Versioning пакеты данных с инкапсуляцией LISP содержат номера версий двух отображений, используемых для выбора RLOC во внешнем заголовке (RLOC источника и получателя). Эти сведения имеют два применения.

1. Map-Versioning позволяет выходному маршрутизатору туннеля (Egress Tunnel Router или ETR), принимающему пакет, знать, использует ли входной маршрутизатор туннеля (Ingress Tunnel Router или ITR) последнюю версию отображения для EID получателя. Если это не так, ETR может напрямую передать Map-Request с обновлённым отображением маршрутизатору ITR для информирования о последней версии. ETR может также запросить у ITR инициирование Map-Request для получения последнего отображения путём отправки сообщения SMR (Solicit Map-Request). Оба варианта определены в [RFC9301].
2. Map-Versioning позволяет ETR, принимающему пакет, знать, содержится ли в его EID-RLOC Map-Cache последнее отображение для EID источника. Если это не так, может быть передан Map-Request.

Вопросы развёртывания LISP Map-Versioning рассмотрены в разделе 9. Вопросы внедрения, а преимущества Map-Versioning в некоторых распространённых вариантах применения LISP описаны в Приложении А.

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

В этом документе используются термины, определённые в основной спецификации LISP ([RFC9300] и [RFC9301]). Ниже определены термины, связанные с механизмом Map-Versioning. В документе применяется порядок битов big-endian (сначала старший).

Map-Version number - номер версии отображения

12-битовое целое число без знака, назначенное отображению EID-RLOC и указывающее номер версии (раздел 6).

Null Map-Version - нулевая (пустая) версия отображения

Номер Map-Version со значением 0x000, который применяется для информирования о том, что свойство Map-Version не используется и отображению EID-RLOC не назначается номер версии (параграф 6.1).

Dest Map-Version number - номер версии отображения у получателя

Map-Version для отображения в EID-RLOC Map-Cache, используемого ITR при выборе RLOC, помещаемого в поле Destination Routing Locator внешнего заголовка IP пакетов с инкапсуляцией LISP (параграф 7.1).

Source Map-Version number - номер версии отображения у отправителя

Map-Version для отображения в EID-to-RLOC Database, используемого ITR при выборе RLOC для включения в поле Source Routing Locator внешнего заголовка IP пакетов с инкапсуляцией LISP (параграф 7.2).

4. Заголовок LISP и номера Map-Version

Для работы с номерами версий заголовков LISP передаёт значения Source Map-Version и Dest Map-Version. Это делается путём установки бита V в заголовке LISP, как описано в [RFC9300] и показано на рисунке 1. Разрешённые комбинации флагов с установленным (1) битом V описаны в [RFC9300]. Номера версий не требуется передавать во всех пакетах с инкапсуляцией LISP. Формат заголовка LISP при установленном флаге V показан на рисунке 1.

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|N|L|E|V|I|R|K|K| Source Map-Version | Dest Map-Version |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Рисунок 1. Пример заголовка LISP при использовании Map-Versioning.

Source Map-Version number (12 битов)

См. раздел 3. Определения терминов.

Dest Map-Version number (12 битов)

См. раздел 3. Определения терминов.

5. Запись отображения и Map-Version

Чтобы приспособиться к этому механизму, записи Map Record, доставляемые в сообщениях Map-Request, Map-Reply, Map-Register должны содержать номер Map-Version. Map Record (см. [RFC9301]) приводится здесь в качестве примера на рисунке 2. Этот документ не меняет назначение сообщений Map-Request, Map-Reply, Map-Register, они по-прежнему применяются в соответствии с [RFC9301].

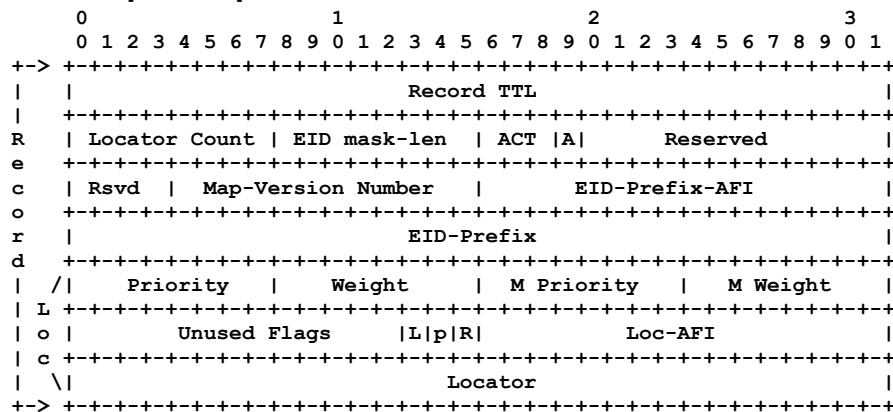


Рисунок 2. Пример формата Map-Record.

Map-Version Number

Номер Map-Version для отображения, содержащегося в Record. Как указано в параграфе 6.1, это поле может иметь значение 0, указывающее, что с отображением не связано Map-Version.

Этот формат пакета совместим с xTR, не поддерживающими Map-Versioning, поскольку они могут просто игнорировать биты.

Map-Server, получивший неожиданный номер Map-Version (например, старый), **должен** отбросить сообщение без уведомления отправителя и **следует** внести соответствующую запись в журнал.

6. Номер EID-RLOC Map-Version

Номер EID-RLOC Map-Version представляется 12-битовым целым числом без знака. Номер версии назначается по отображениям, что означает разные номера у отображений, изменяемых независимо. Обновление версии (т. е. создание новой) **должно** увеличивать номер версии по сравнению с прежним (исключением является лишь Null Map-Version, как указано в конце параграфа 6.1. Null Map-Version).

Пространство номеров версий является кольцевым, при котором половина номеров будут меньше текущего номера Map-Version, а вторая половина - больше (новее). По сути, это порядковый номер, к которому применяется арифметика, описанная в [RFC1982]. Порядок позволяет по-разному реагировать на более старые и более новые номера Map-Version с отбрасыванием старых номеров и отправке Map-Request по новым (см. 7. Работа с номерами Map-Version). Предположим, что имеется два номера V1 и V2, отличных от Null Map-Version (6.1. Null Map-Version) и заданных 12 битами. Тогда для определения порядка этих номеров **должны** выполняться приведённые ниже процедуры (с соблюдением их порядка).

1. V1 = V2 - номера Map-Version совпадают.
2. V2 > V1, тогда и только тогда, когда V2 > V1 и (V2 - V1) <= 2⁽¹²⁻¹⁾ или V1 > V2 и (V1 - V2) > 2⁽¹²⁻¹⁾
3. V1 > V2 в остальных случаях.

Для Map-Version = 69 номера Map-Version из диапазона [70; 69 + 2048] будут больше 69, а номера из диапазона [69 + 2049; (69 + 4095) mod 4096] - меньше чем 69.

Исходный номер Map-Version для нового отображения EID-RLOC **следует** задавать случайным, но **недопустимо** устанавливать значение Null Map-Version (0x000), поскольку этот номер имеет особое значение (см. параграф 6.1). Можно задавать начальный номер Map-Version в конфигурации.

При перезагрузке ETR будет использовать сопоставления, настроенные в его базе EID-RLOC. Если эти отображения имеют номер Map-Version, они будут применяться в соответствии с описанным в этом документе механизмом. ETR **недопустимо** автоматически создавать и назначать номера Map-Version для отображений в базе EID-RLOC.

6.1. Null Map-Version

Значение 0x000 (0) является особым номером Map-Version, указывающим, что на деле с отображением EID-RLOC не связано номера версии. Это значение применяется в особых случаях и называется Null Map-Version.

Запись отображений с номером Null Map-Version указывает, что с отображением не связано номера Map-Version. Это означает, что пакетам с инкапсуляцией LISP, адресованным в EID-Prefix, указанный отображением, **недопустимо** включать номер Map-Version (бит V сброшен - 0). Если ETR получает пакет с инкапсуляцией LISP и установленным битом V, когда исходное отображение в EID-RLOC Database имеет значение Null Map-Version, пакет **должен** отбрасываться без уведомления отправителя.

Null Map-Version может указываться в заголовке LISP как номер версии Source Map-Version (7.2. Обработка Map-Version источника), что указывает отсутствие сведений о версии отображения на сайте источника. Это означает, что при наличии отображения EID источника в EID-RLOC Map-Cache маршрутизатору ETR **недопустимо** сравнивать полученное значение Null Map-Version с содержимым EID-RLOC Map-Cache (параграф 7.2).

Особый смысл значения 0 для номера Map-Version означает, что при обновлении номера Map-Version в результате изменения содержимого отображения значение 0 **должно** пропускаться и взамен должно устанавливаться значение 1.

7. Работа с номерами Map-Version

Основная идея использования номеров Map-Version заключается в том, что при каждом изменении отображения (например, добавлении или удалении RLOC, смене веса в соответствии с правилами организации трафика, смене приоритета) или утрате на сайте LISP доступности одного или нескольких RLOC с локальной точки зрения (например, от IGP или при смене политики), сайт LISP назначает новый номер Map-Version. Действительным считается лишь последний номер Map-Version. Обновления отображений и соответствующих номеров Map-Version должны выполняться так, чтобы самая старая версия не могла быть спутана с последней (новой) по причине использования кольцевой нумерации. Для этого могут быть приняты простые меры, такие как обновление отображений лишь при условии использования для всего активного трафика последней версии или достаточно долгое ожидание, чтобы срок действия кэшированных записей LISP истёк (ожидание в течение времени не менее TTL, определённого в [RFC9301]).

ETR, получающий пакет LISP с номером Map-Version, выполняет указанные ниже проверки.

1. Проверяет, что ITR, передавший пакет, имеет актуальное отображение в своём EID-RLOC Map-Cache для EID получателя и корректно выполняет инкапсуляцию (см. 7.1. Обработка Map-Version получателя).
2. Для двухстороннего трафика проверяется, что отображение в EID-RLOC Map-Cache локального ETR для EID источника актуально (см. 7.2. Обработка Map-Version источника).

7.1. Обработка Map-Version получателя

Когда ETR получает пакет, номер Dest Map-Version относится к отображению EID получателя, для которого ETR является RLOC. Это отображение является частью базы данных ETR EID-RLOC. Поскольку ETR уполномочен для отображения, он будет корректировать и обновлять номер Dest Map-Version. Номер версии **должен** проверяться, как указано ниже.

1. Пакет приходит с номером Dest Map-Version, сохранённым в EID-RLOC Database (обычный случай). Передавший пакет ITR имеет в своём кэше EID-RLOC Map-Cache актуальное отображение, поэтому иных действий не требуется.
2. Пакет приходит с номером Dest Map-Version новее (см. 6. Номер EID-RLOC Map-Version) сохранённого в EID-RLOC Database. Поскольку ETR уполномочен для сопоставлений, что означает корректность его номера отображения, номер версии в прибывшем пакете считается недействительным и пакет **должен** отбрасываться без уведомления отправителя. **Следует** также сделать запись об этом в системном журнале.
3. Пакет приходит с номером Dest Map-Version старше (см. 6. Номер EID-RLOC Map-Version) сохранённого в EID-RLOC Database. Это означает, что у передающего пакет ITR имеется устаревшее отображение в его EID-to-RLOC Map-Cache. ETR **может** обычным способом обработать инкапсулированную дейтаграмму в соответствии с [RFC9300], однако передающий пакет ITR **должен** быть проинформирован о доступности нового отображения с учётом правил ограничения скорости, заданных в [RFC9301]. Это осуществляется отправкой сообщения Map-Request маршрутизатору ITR, как описано в [RFC9301]. Одним из свойств, добавленных номерами Map-Version, является возможность блокировать трафик, не использующий последнюю версию отображения. Это возникает в случаях, когда ITR не обновил отображение, для которого ETR является полномочным, или в некоторых вариантах атак. В соответствии с правилами ограничения частоты передачи Map-Request из [RFC9301] после 10 повторов сообщения Map-Request передаются каждые 30 секунд. Если после первых 10 попыток номер Dest Map-Version в пакетах не обновился, маршрутизатору ETR **следует** отбрасывать пакеты со старым номером Map-Version. Операторы могут задать исключения для этого правила, но они выходят за рамки документа.

Правило для случая 3 **может** быть более строгим. Если время Record TTL для предыдущего отображения уже истекло, все пакеты со старым номером Map-Version **должны** отбрасываться без уведомления отправителя и отправки Map-Request. Такое действие разрешается, поскольку в случае, когда отображение с новым номером версии не менялось в течение Record TTL старого отображения, все записи в EID-RLOC Map-Cache маршрутизаторов ITR должны были уже устареть. Действительно, все ITR, передающие трафик, должны уже иметь обновлённые отображения в соответствии с [RFC9301].

Наличие в пакетах с инкапсуляцией LISP номера Dest Map-Version со значением Null Map-Version является нарушением протокола (см. 6.1. Null Map-Version).

7.2. Обработка Map-Version источника

Когда ETR принимает пакет, номер Source Map-Version относится к отображению для EID источника, для которого отправивший пакет ITR является полномочным. Если у ETR есть в EID-RLOC Map-Cache запись для EID источника, должна выполняться проверка с учётом указанных ниже обстоятельств.

1. Пакет приходит с номером Source Map-Version, сохранённым в EID-RLOC Database (обычный случай). ETR имеет в своём кэше EID-RLOC Map-Cache актуальное отображение, поэтому иных действий не требуется.
2. Пакет приходит с номером Source Map-Version новее (см. 6. Номер EID-RLOC Map-Version) сохранённого в локальном EID-RLOC Map-Cache. Это означает, что EID-RLOC Map-Cache у ETR устарел и его нужно обновить. **Должно** передаваться сообщение Map-Request, чтобы получить новое отображение для EID и источника, с учётом правил ограничения скорости, описанных в [RFC9301].
3. Пакет приходит с номером Source Map-Version старше (см. 6. Номер EID-RLOC Map-Version) сохранённого в локальном EID-RLOC Map-Cache. Отметим, что при наличии отображения в EID-RLOC Map-Cache это означает, что было передано явное сообщение Map-Request и получено сообщение Map-Reply из полномочного источника. В такой ситуации пакет **следует** просто отбросить. Операторы могут задать исключения для этого правила, но они выходят за рамки документа.

Если у ETR нет записи в EID-RLOC Map-Cache для EID источника, номер Source Map-Version **должен** игнорироваться (см. Приложение A.1. Map-Versioning и односторонний трафик, где приведён пример такой ситуации).

8. Вопросы безопасности

Этот документ основан на спецификации и операциях плоскостей данных и управления LISP. Здесь применимо обсуждение вопросов безопасности из [RFC9300] и [RFC9301]. Номера Map-Version **недопустимо** применять в общедоступной сети Internet и они **должны** использоваться лишь в доверенных, изолированных средах. Тщательный анализ безопасности LISP приведён в [RFC7835].

Злоумышленники могут попытаться инициировать большое число Map-Request простой подделкой пакетов со случайными номерами Map-Version. Частота отправки Map-Request ограничена, как указано в [RFC9301]. При использовании Map-Version можно фильтровать пакеты с недействительными номерами до отправки Map-Request, что позволит снизить влияние DoS-атак, однако этого недостаточно для практической защиты от атак DDoS.

Этот документ включает записи в системный журнал при определённых событиях. В реализации рекомендуется включать механизмы для предотвращения атак на истощение ресурсов, связанных с системным журналом, но это выходит за рамки документа.

Спецификации в этом документе сравнительно консервативны в части отбрасывания пакетов в некоторых ситуациях. Такой подход основан на соображениях о возможных рисках использования для организации атак некоторых действий плоскости управления, вызываемых плоскостью данных. В некоторых случаях даже пересылка пакета с непригодным номером Map-Version может считаться безопасной, однако приоритет отдаётся управляемости системы в связи с необходимостью большого числа механизмов для идентификации легитимного трафика.

9. Вопросы внедрения

LISP требует от ETR одного сайта поддерживать идентичные отображения для данного EID-Prefix. Для Map-Versioning не требуется дополнительных механизмов синхронизации. Ясно, что все ETR должны возвращать одинаковые сопоставления, включая один номер Map-Version, поскольку в ином случае могут возникать несоответствия, создающие добавочный трафик управления, нестабильность и сбои.

Имеется два варианта применения Map-Versioning в плане синхронизации. С одной стороны, назначение отображения номеров версий помогает при отладке, поскольку позволяет быстро проверить согласованность сопоставлений на разных ETR по номерам Map-Version. С другой стороны, Map-Versioning можно использовать для управления трафиком в направлении ETR, анонсирующих наиболее свежее сопоставление.

Рассмотрим в качестве примера топологию, показанную на рисунке 3, где ITR A.1 в Domain A передаёт односторонний трафик в Domain B, а A.2 из Domain A обменивается в Domain B двухсторонним трафиком. В частности, ITR A.2 передаёт трафик ETR B, а ETR A.2 получает трафик от ITR B.

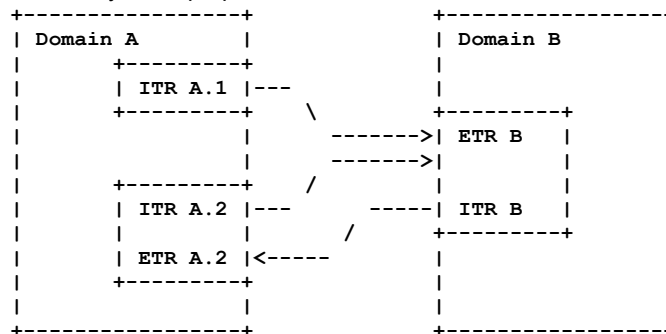


Рисунок 3. Пример топологии.

Очевидно, что при использовании Map-Versioning оба маршрутизатора ITR A.1 и ITR A.2 из Domain A должны указывать одно значение, иначе ETR и Domain B начнёт передавать сообщения Map-Request.

Такая же проблема может возникнуть и без Map-Versioning, например, если два ITR из Domain A будут передавать разные биты LSB. В этом случае трафик будет нарушаться, если ETR B не проверяет доступность, или ETR B начнёт передавать Map-Request для подтверждения каждого изменения доступности.

Пока LISP не предоставляет какого-либо конкретного механизма синхронизации, но предполагает, что синхронизация обеспечивается согласованной настройкой xTR. Это относится и к Map-Versioning. Если в будущем появится механизм синхронизации, Map-Versioning автоматически воспользуется им, поскольку это включено в формат Map Record, как описано в разделе 5. Запись отображения и Map-Version.

10. Взаимодействие с IANA

Этот документ не требует действий IANA.

11. Литература

11.1. Нормативные документы

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](https://www.rfc-editor.org/info/rfc2119), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, [RFC 8174](https://www.rfc-editor.org/info/rfc8174), 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](https://www.rfc-editor.org/info/rfc9300), DOI 10.17487/RFC9300, October 2022, <<https://www.rfc-editor.org/info/rfc9300>>.

[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>>.

11.2. Дополнительная литература

[RFC1982] Elz, R. and R. Bush, "Serial Number Arithmetic", RFC 1982, DOI 10.17487/RFC1982, August 1996, <<https://www.rfc-editor.org/info/rfc1982>>.

[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>>.

[RFC6834] Iannone, L., Saucez, D., and O. Bonaventure, "Locator/ID Separation Protocol (LISP) Map-Versioning", [RFC 6834](#), DOI 10.17487/RFC6834, January 2013, <<https://www.rfc-editor.org/info/rfc6834>>.

[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>>.

[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>>.

Приложение А. Преимущества и применение Map-Versioning

В последующих параграфах обсуждаются различные аспекты и вариант применения Map-Versioning. Вопросы безопасности рассмотрены в разделе 8.

А.1. Map-Versioning и односторонний трафик

При использовании Map-Versioning заголовок LISP содержит номера Map-Version для отображений источника и получателя. Может возникнуть вопрос для случая одностороннего потока, например, как показано на рисунке 4, поскольку спецификация LISP не требует от ETR наличия отображения от EID источника.

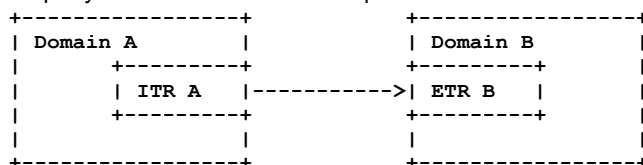


Рисунок 4. Односторонний трафик между доменами LISP.

ITR способен включить номера версий источника и получателя в заголовок LISP, поскольку номер Source Map-Version имеется в его базе данных, а номер Dest Map-Version - в кэше.

ETR проверяет лишь номер Dest Map-Version, игнорируя номер Source Map-Version, как указано в заключительном предложении параграфа 7.2. Обработка Map-Version источника.

А.2. Map-Versioning и межсетевое взаимодействие Interworking

Версии отображений совместимы с межсетевым взаимодействием LISP между сайтами с поддержкой и без поддержки LISP, как описано в [RFC6832]. Межсетевое взаимодействие LISP определяет три метода взаимодействия между сайтами с поддержкой и без поддержки LISP - Proxy-ITR, LISP-NAT, Proxy-ETR, описанные ниже для Map-Versioning.

А.2.1. Map-Versioning u Proxy-ITR

Назначением Proxy-ITR (PITR) является инкапсуляция трафика с сайта без поддержки LISP для доставки пакета одному из ETR сайта LISP (Рисунок 5). Этот случай очень похож на вариант с односторонним трафиком из Приложения А.1, поэтому к нему применимы те же правила.

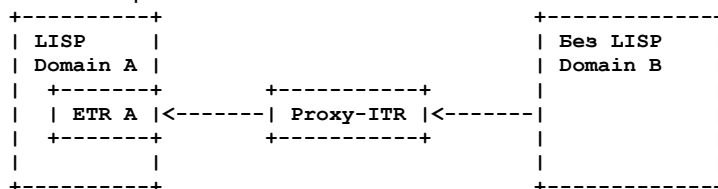


Рисунок 5. Односторонний трафик из домена без LISP в домен LISP.

Основное отличие состоит в том, что у Proxy-ITR нет никакого отображения, поскольку он просто инкапсулирует пакеты с сайта без LISP и не может поэтому предоставить Source Map-Version. В этом случае Proxy-ITR будет просто указывать Null Map-Version в качестве Source Map-Version, а принимающий ETR будет игнорировать это поле.

В этом примере LISP Domain A способен проверить, использует ли PITR последнее отображение. В поле Dest Map-Version Number заголовка LISP узел Proxy-ITR будет помещать номер версии отображения, используемого для инкапсуляции, а ETR A может использовать такое значение, как указано в параграфе 7. Работа с номерами Map-Version.

А.2.2. Map-Versioning u LISP-NAT

Механизм LISP-NAT основан на трансляции адресов немаршрутизируемых EID в маршрутизируемые EID без какой либо инкапсуляции, поэтому Map-Versioning в этом случае не применяется.

A.2.3. Map-Versioning u Proxy-ETR

Назначением Proxy-ETR (PETR) является декапсуляция трафика с сайта LISP для доставки пакетов на сайт без LISP (Рисунок 6). Одной из основных причин внедрения PETR является обход проверки индивидуальной пересылки по обратному пути (Unicast Reverse Path Forwarding).

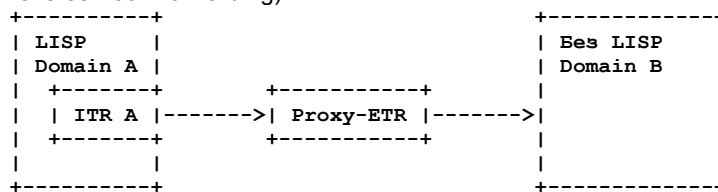


Рисунок 6. Односторонний трафик между из домена LISP в домен без LISP.

У Proxy-ETR нет каких-либо отображений, поскольку он просто декапсулирует пакеты от сайта LISP. В этом случае ITR может указывать значение Map-Version или Null Map-Version в качестве номера Dest Map-Version, поскольку принимающий Proxy-ETR игнорирует это поле.

При такой настройке Proxy-ETR, просматривая номер Source Map-Version Number, может проверить наличие изменений отображения EID источника. Это полезно для проверки RLOC источника. В приведённом выше примере трафик из домена LISP инкапсулируется в LISP с использованием в качестве адреса отправителя RLOC домена. Proxy-ETR может извлечь отображение, связанное с доменом LISP и проверить поступление входящих пакетов с инкапсуляцией LISP от действительного RLOC. Изменение в RLOC-Set, который может применяться для адреса источника, может быть указано номером версии, при этом Proxy-ETR способен при необходимости запросить последнее отображение, как описано в параграфе 7.2. Обработка Map-Version источника.

A.3. Отключение и отзыв RLOC

Map-Versioning можно использовать для аккуратного завершения работы или отзыва конкретного RLOC. Это достигается путём создания нового отображения с обновлением номера Map-Version, где адрес RLOC, подлежащий исключению, будет анонсирован как недоступный (через флаг R в Map Record, см. [RFC9301]) без его фактического отключения.

После обновления отображения RLOC будет получать всё меньше трафика, поскольку удалённые сайты LISP будут запрашивать обновлённое сопоставление и прекращать использовать этот адрес. Для безопасного завершения работы RLOC достаточно одного интервала TTL плюс небольшое время для трафика, находящегося в сети, поскольку все сайты, активно использующие отображение за это время получают обновление.

Отметим, что смена ETR для потока может приводить к изменению порядка доставки пакетов в потоке, как и другие изменения маршрутизации для потока.

Адреса авторов

Luigi Iannone
Huawei Technologies France
Email: luigi.iannone@huawei.com

Damien Saucez
Inria
2004 route des Lucioles - BP 93
Sophia Antipolis
France
Email: damien.saucez@inria.fr

Olivier Bonaventure
Universite catholique de Louvain
Email: olivier.bonaventure@uclouvain.be

Перевод на русский язык

Николай Малых
nmalykh@protokols.ru