Internet Engineering Task Force (IETF)
Request for Comments: 9305
Category: Standards Track
ISSN: 2070-1721

F. Maino, Ed.
Cisco
J. Lemon
P. Agarwal
Innovium
D. Lewis
M. Smith
Cisco

October 2022

Locator/ID Separation Protocol (LISP) Generic Protocol Extension

Расширение базового протокола LISP

Аннотация

В этом документе описаны расширения плоскости данных протокола разделения локаторов и идентификаторов (Locator/ID Separation Protocol или LISP) путём изменения заголовка LISP для поддержки многопротокольной инкапсуляции и расширения возможностей протокола.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. 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/rfc9305.

Оглавление

1. Введение....1
1.1. Уровни требований....2
1.2. Определения терминов....2
2. Заголовок LISP без расширений протокола....2
3. Расширение базового протокола LISP (LISP-GPE)....2
4. Вопросы реализации и внедрения....3
4.1. Заявление о применимости....3
4.2. Функциональность контроля перегрузок....3
4.3. Контрольная сумма UDP....4
4.3.1. Обработка нулевой контрольной суммы UDP для IPv6....4
4.4. DSCP, ECN, TTL, 802.1Q....5
5. Совместимость с прежними версиями....5
5.1. Обнаружение возможностей ETR....5
6. Взаимодействие с IANA....5
6.1. Реестр LISP-GPE Next Protocol....5
7. Вопросы безопасности....5
8. Литература....6
8.1. Нормативные документы....6
8.2. Дополнительная литература....6
Благодарности....6
Участники работы....7
Адреса авторов....7

1. Введение

Плоскость данных LISP задана в [RFC9300] и определяет формат инкапсуляции для передачи пакетов IPv4 и IPv6 (далее IP) с использованием заголовка LISP и внешнего транспорта UDP/IP.

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

Заголовок плоскости данных LISP не указывает инкапсулируемый протокол, поэтому в настоящее время инкапсуляция применяется лишь для пакетов IP. Другие протоколы, прежде всего, VXLAN[1] [RFC7348] (определяющий формат заголовка, аналогичный LISP) применяются для инкапсуляции протоколов канального уровня (Layer 2 или L2), таких как Ethernet.

Этот документ залает расширение заголовка LISP, определённого в [RFC9300], для указания внутреннего протокола, что позволяет инкапсулировать Ethernet, IP или иной нужный протокол, сохраняя совместимость с имеющимися развёртываниями LISP.

Применяется флаг заголовка LISP (бит P) для указания наличия 8-битового поля Next Protocol. При наличии этого поля оно занимает 8 битов, выделенных в [RFC9300] для функций Echo-Noncing и Map-Versioning. Эти две функции становятся недоступными при использовании бита P. Однако можно задать подходящий промежуточные (shim) заголовки расширения базового протокола LISP (LISP Generic Protocol Extension или LISP-GPE) для задания возможностей, эквивалентных Echo-Noncing и Map-Versioning.

Поскольку все резервные биты заголовка плоскости данных LISP уже заняты, LISP-GPE можно использовать также для расширения заголовка плоскости данных LISP путём задания промежуточных заголовокв Next Protocol, реализующих новые функции плоскости данных, не поддерживаемые в заголовке LISP. Например, используя заголовок основанных на группах правил (Group-Based Policy или GBP) header [VXLAN-LISP] или IOAM[2] [VXLAN-GPE] с LISP-GPE, можно рассмотреть расширение для поддержки в плоскости данных функций GBP или метаданных IOAM.

1.1. 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.

1.2. Определения терминов

В этом документе используются термины, определённые в [RFC9300].

2. Заголовок LISP без расширений протокола

Как описано в разделе 1, заголовок LISP не включает идентификатор протокола, указывающий тип передаваемого содержимого (payload). Поэтому в LISP передаются только пакеты IP.

Заголовок LISP [RFC9300] содержит набор флагов (часть их зарезервирована), поле Nonce/Map-Version и поле Instance ID/Locator-Status-Bits. Флаги обеспечивают гибкое кодирование полей. Отметим, что бит 5 остался последним резервным флагом заголовка LISP.

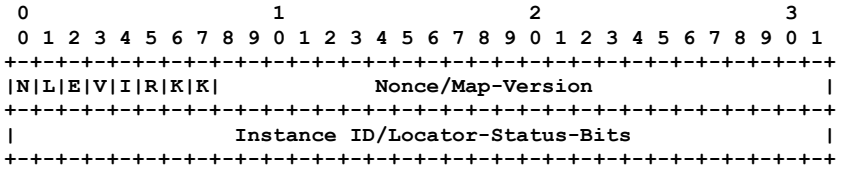

Рисунок 1. Заголовок LISP.

3. Расширение базового протокола LISP (LISP-GPE)

Этот документ задаёт два изменения заголовков LISP для поддержки многопротокольной инкапсуляции - флаг P и поле Next Protocol. Документ задаёт поведение протокола при установленном (1) флаге P, а сброшенный (0) бит P прежнее поведение. Заголовок LISP-GPE показан на рисунке 2 и описан ниже.

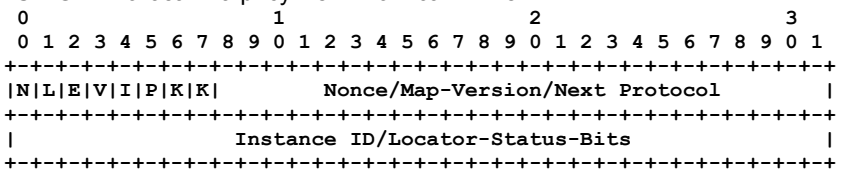

Рисунок 2. Заголовок LISP-GPE.

P

Бит 5 задан как флаг Next Protocol, установка (1) которого говорит о наличии 8-битового поля Next Protocol. Сброшенный (0) бит указывает, что заголовок LISP полностью соответствует определению [RFC9300].

При установленном флаге P биты N, E, V и биты 8-23 поля Nonce/Map-Version/Next Protocol **должны** сбрасываться (0) при отправке, а получатель **должен** игнорировать их. Свойства, эквивалентные реализованным с помощью битов N, E, и V в [RFC9300], такие как Echo-Noncing и Map-Versioning, можно обеспечить путём задания подходящих промежуточных заголовков LISP-GPE.

Заголовок LISP-GPE с установленным флагом P показан на рисунке 3.

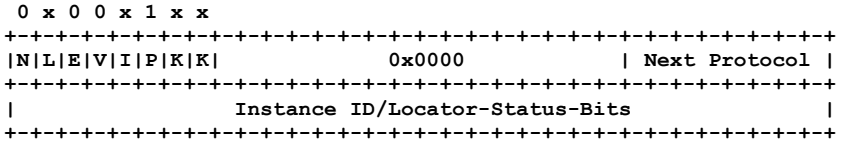

Рисунок 3. LISP-GPE с установленным битом P.

[1]Virtual eXtensible Local Area Network - виртуальная расширяемая ЛВС.
[2]In situ Operations, Administration, and Maintenance - операции, администрирование и поддержка на месте.

Next Protocol

При установленном (1) флаге P младшие 8 битов первого 32-битового слова служат полем Next Protocol, указывающим протокол, инкапсулируемый в поле данных пакета.

Этот документ определяет указанные ниже значения Next Protocol.

```
0x00:  резерв
0x01:  IPv4
0x02:  IPv6
0x03:  Ethernet
0x04:  Network Service Header (NSH) [RFC8300]
0x05 - 0x7D:  не распределены
0x7E и 0x7F:  эксперименты и тестирование
0x80 - 0xFD:  не распределены (shim-заголовки)
0xFE, 0xFF:  эксперименты и тестирование (shim-заголовки)
```

Эти значения внесены в реестр IANA LISP-GPE Next Protocol, как указано в параграфе 6.1.

Значения Next Protocol 0x7E, 0x7F, 0xFE, 0xFF выделены для экспериментов и тестирования в [RFC3692], значения 0x80 - 0xFD - для протоколов, кодируемых как промежуточные (shim) заголовки. Все такие протоколы **должны** использовать структуру заголовка, показанную на рисунке 4, которая включает поле Next Protocol. При использовании shim-заголовков с другими протоколами, указанными значениями Next Protocol от 0x00 до 0x7F, промежуточные заголовки должны быть первыми.

Промежуточные заголовки позволяют поэтапно внедрять новые функции GPE, сохраняя их понятную данной реализации туннельного маршрутизатора (Tunnel Router или xTR) обработку на «быстром» пути (обычно ASIC[1]) и переводя новые функции GPE на «медленный» путь.

Для промежуточных протоколов первые 32 бита **должны** включать указанные на рисунке 4 поля.

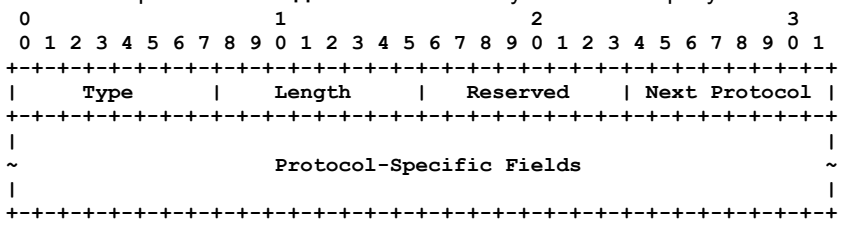

Рисунок 4. Shim-заголовок.

Type

Служит для идентификации различных сообщений данного протокола.

Length

Ращмер протокольного сообщения в 4-октетных блоках без учёта первых 4 октетов.

Reserved

Зарезервировано для протокола, определённого в этом сообщении.

Next Protocol

Указывает протокол для инкапсулируемых данных (payload). Значения протоколов указаны в реестре IANA LISP-GPE Next Protocol (параграф 6.1).

4. Вопросы реализации и внедрения

4.1. Заявление о применимости

LISP-GPE, как протокол инкапсуляции на обснове UDP, соответствует рекомендациям по использованию UDP из [RFC8085]. Применимость этих рекомендаций зависит от базовой сети IP и природы инкапсулируемых данных.

В [RFC8085] описано два варианта примерения приложений UDP для 1) общедоступной сети Internet и 2) контролируемой среды. Контролируемая среда предполагает один административный домен или набор смежных взаимодействующих доменов. Сетью в контролируемой среде можно управлять для создания определённых рабочих условий, а в общедоступной сети Internet это невозможно. Поэтому требования к туннельным протоколам для контролируемых сред задают меньше ограничений, чем для работы в общедоступной сети Internet.

Сфера применимости LISP-GPE совпадает с набором вариантов использования, указанных в [RFC9300] для протокола плоскости данных LISP. Общим свойством этих вариантов применения является наличие большого набора взаимодействующих элементов, стремящимися обмениваться данными через общедоступную сеть Internet или иные крупные инфраструктуры IP с отделением адресации и топологии взаимодействующих элементов от топологии, маршрутизации и адресации базовой сети и Internet.

Расширение LISP-GPE рассчитано на реализацию в сетевых средах, управляемых одним оператором или операторами взаимодействующих смежных сетей, которые соответствуют определению контролируемых сред в [RFC8085].

Для целей этого документа контролируемая среда с управляемым трафиком (Traffic-Managed Controlled Environment или TMCE), описанная в [RFC8086], рассматривается как сеть IP с организацией трафика (traffic-engineered) и/или иным управлением (например, применением ограничителей скорости трафика) для предотвращения перегрузки. Значительная часть текста этого разела заимствована из [RFC8086].

Операторы сетей отвечают за соблюдение требований и рекомендаций этого раздела в своих системах с LISP-GPE.

4.2. Функциональность контроля перегрузок

LISP-GPE не предоставляет функций контроля перегрузки и полагается в этом плане инкапсулированный протокол (payload). Поэтому **требуется** использовать LISP-GPE с трафиком, для которого имеется контроль перегрузок, или внутри сети с управлением трафиком для предотвращения перегрузок (TMCE). Оператор сети с управлением

[1]Application-Specific Integrated Circuit - специализированная интегральная схема.

трафиком (TMCE) может избежать перегрузок за счёт тщательной настройки своих сетей, ограничения скорости пользовательского трафика и его организации в соответствии с возможностями сетевых путей.

С учётом приведённых выше рекомендаций новые инкапсулируемые данные при регистрации в LISP-GPE **должны** сопровождаться набором рекомендаций, выведенных из раздела 5 в [RFC9300]. Такие новые протоколы следует разрабатывать с явными сигналами контроля перегрузки от нижележащего протокола в IP. После этого межсетевой уровень IP может выступать уровнем переноса для доставки уведомлений от перегруженных узлов, не понимающих бит IP, наверх до транспортного уровня (L4). Следуя рекомендациям [ENCAP-GUIDE], создатели подсетей могут разрешить протоколу L2 участие в контроле перегрузок без отбрасывания пакетов путём распространения получателям данных явного контроля перегрузок (Explicit Congestion Notification или ECN) [RFC3168].

4.3. Контрольная сумма UDP

Для данных IP (payload) в параграфе 5.3 [RFC9300] задана обработка контрольных сумм UDP с предложением к разработчикам учитывать рекомендации по контрольным суммам UDP из параграфа 3.4 в [RFC8085], когда они хотят защитить от повреждений заголовки UDP и LISP.

Для защиты целостности заголовков LISP-GPE, опций и данных (например, для предотвращения доставки данных в систему другого арендатора при повреждении поля данных) **следует** использовать внешнюю контрольную сумму UDP с LISP-GPE при транспортировке по протоколу IPv4. Контрольная сумма UDP обеспечивает статистические гарантии сохранности содержимого в процессе доставки. Такие проверки целостности не являются криптографически строгими и не предназначены для обнаружения ошибок на физическом уровне или враждебного изменения дейтаграмм (см. параграф 3.4 в [RFC8085]). В системах, где такой риск возникает, операторам **следует** использовать дополнительные механизмы защиты целостности данных, такие как IPsec.

Оператор **может** отказаться от применения контрольных сумм UDP (использовать нулевую сумму), если защита целостности пакетов LISP-GPE обеспечивается другими механизмами, такими как IPsec, или выполняется одно из условий параграфа 4.3.1 (a, b или c).

4.3.1. Обработка нулевой контрольной суммы UDP для IPv6

По умолчанию контрольная сумма UDP **должна** использоваться при доставке LISP-GPE по протоколу IPv6. Конечную точку туннеля **можно** настроить на использование нулевой контрольной суммы UDP, если выполняются дополнительные требования, указанные в этом параграфе.

При использовании LISP-GPE с протоколом IPv6 контрольная сумма UDP служит для защиты заголовков IPv6, UDP и LISP-GPE, а также данных от возможных повреждений. Таким образом, по умолчанию для LISP-GPE **должна** применяться контрольная сумма UDP при доставке через IPv6. Оператор **может** настроить работу с нулевой контрольной суммой UDP при работе в контролируемой среде с управлением трафиком, как указано в параграфе 4.1, если выполняется какое-либо из приведённых ниже условий.

a. Известно, что повреждение пакетов крайне маловероятно (возможно, на основе сведений оператора о применяемом в базовой сети оборудовании) и оператор принимает риск незамеченного повреждения пакетов.

b. Если на основе наблюдений (например, для прошлых или текущих потоков трафика с использованием ненулевой контрольной суммы) определено, что число повреждённых пакетов очень мало и оператор принимает риск незамеченного повреждения пакетов.

c. Данные LISP-GPE передаются приложениям, устойчивым к ошибочной доставке и повреждениям пакетов (возможно, за счёт проверки контрольных сумм вышележащих уровней или надёжного повтора передачи).

Кроме того, реализации туннелей LISP-GPE, использующие нулевые контрольные суммы UDP **должны** соблюдать приведённые ниже требования.

1. Использование контрольной суммы UDP при работе по протоколу IPv6 **должно** быть по умолчанию включено для всех туннелей LISP-GPE.

2. Если LISP-GPE применяется с нулевой контрольной суммой UDP по протоколу IPv6, реализации xTR **должны** соблюдать все требования, указанные в разделе 4 [RFC6936] и требование 1 из раздела 5 в [RFC6936].

3. Выходным маршрутизаторам туннелей (Egress Tunnel Router или ETR), декапсулирующим пакеты, **следует** проверять, что адреса отправителя и получателя IPv6 действительны для туннеля LISP-GPE, настроенного на использование нулевой контрольной суммы UDP, и отбрасывать не прошедшие проверку пакеты.

4. Входные маршрутизаторы туннелей (Ingress Tunnel Router или ITR), инкапсулирующие пакеты, **могут** использовать разные адреса отправителя IPv6 для каждого туннеля LISP-GPE с нулевой контрольной суммой UDP, чтобы усилить проверку адреса отправителя IPv6 декапсулятором (т. е. один и тот же адрес отправителя IPv6 не применяется для нескольких адресов получателей IPv6, как индивидуальных, так и групповых). Если это невозможно, **рекомендуется** применять каждый адрес отправителя для как можно меньшего числа туннелей LISP-GPE с нулевой контрольной суммой UDP.

5. Следует принимать меры для предотвращения выхода туннельного трафика LISP-GPE по протоколу IPv6 с нулевой контрольной суммой UDP в общедоступную сеть Internet. Такими мерами являются фильтры пакетов на выходных маршрутизаторах-посредниках (Proxy Egress Tunnel Router или PETR) и физическое или логическое отделение сети LISP от общедоступных сетей Internet.

Приведённые выше требования не меняют требований [RFC6935], [RFC6936], [RFC8200].

Требование проверки адреса отправителя IPv6 в дополнение к проверке адреса получателя IPv6, а также рекомендации не использовать один адрес отправителя IPv6 для разных туннелей LISP-GPE совместно несколько смягчают отсутствие охвата контрольной суммой UDP в заголовке IPv6. В среде с управляемым трафиком, соответствующей хотя бы 1 из приведённых в начале параграфа требований, обеспечиваются дополнительные гарантии.

4.4. DSCP, ECN, TTL, 802.1Q

При инкапсуляции пакетов IP (включая Ethernet) документ [RFC2983] обеспечивает руководство по отображению кодов дифференцированного обслуживания (Differentiated Services Code Point или DSCP) между внутренними и внешними заголовками IP. При использовании сетевой виртуализации обычно лучше всего подходит модель Pipe. Значение DSCP в туннельном заголовке устанавливается на основе правил (оно может быть фиксированным, зависеть от класса трафика во внутреннем заголовке или определяться иным механизмом группировки трафика). Могут быть применимы некоторые аспекты модели Uniform (она трактует внутреннее и внешнее значения DSCP как одно поле, выполняя копирование на входе и выходе), такие как возможность перемаркировки внутреннего заголовка на выходе туннеля на основе транзитной маркировки. Однако модель Uniform концептуально не согласуется с виртуализацией сети в части строгой изоляции инкапсулированного трафика от физической сети.

В [RFC6040] описан механизм раскрытия возможностей ECN в туннелях IP и распространения маркеров на внутренние пакеты. Такому поведению **должны** следовать пакеты IP, инкапсулированные в LISP-GPE.

Хотя обе модели Uniform и Pipe пригодны для TTL (Hop Limit для IPv6) при обработке туннельных пакетов IP, модель Pipe лучше подходит для виртуализации сетей. В [RFC2003] даны рекомендации по обработке TTL внутренних и внешних заголовков IP, этот подход ближе к модели Pipe и рекомендуется для приложений виртуализации сетей с использованием LISP-GPE.

При выполнении маршрутизатором LISP-GPE инкапсуляции Ethernet внутреннее значение 3-битового кода приоритета (Priority Code Point или PCP) 802.1Q [IEEE.802.1Q_2014] **может** отображаться в код DSCP поля дифференцированного обслуживания (Differentiated Services или DS) внешнего заголовка, определённое в [RFC2474]. Поле идентификатора VLAN 802.1Q (VLAN Identifier или VID) [IEEE.802.1Q_2014] **может** отображаться в поле идентификатора экземпляра LISP (Instance ID или IID) или применяться для его установки.

В разделе 7 рассмотрены вопросы защиты целостности для развёртываний, таких как общедоступная сеть Internet, связанные с атаками извне пути.

5. Совместимость с прежними версиями

LISP-GPE использует порт получателя UDP 4341, выделенный для LISP.

При инкапсуляции пакетов IP для маршрутизатора, не поддерживающего LISP-GPE, флаг P **должен** сбрасываться (0), т. е. заданный этим документом формат инкапсуляции **недопустимо** применять для маршрутизаторов, не указавших поддержку этой спецификации, поскольку такие маршрутизаторы будут игнорировать флаг P (как указано в [RFC9300]) и в результате ошибочно интерпретировать другие поля заголовка LISP, что может приводить к значимым ошибкам.

5.1. Обнаружение возможностей ETR

Обнаружение поддержки LISP-GPE маршрутизаторами xTR выходит за рамки этого документа. С учётом того, что областью применимости LISP-GPE являются контролируемые среды с управлением трафиком, для этого могут применяться механизмы настройки ITR и ETR (xTR).

6. Взаимодействие с IANA

6.1. Реестр LISP-GPE Next Protocol

Агентство IANA создало реестр LISP-GPE Next Protocol, содержащий 8-битовые значения. В таблице 1 приведены значения Next Protocol, заданные этим документом. Новые значения выделяются по процедуре Specification Required [RFC8126]. Протоколы, которым выделяются значения, не обязательно относятся к категории IETF Standards Track.

Таблица 1.

Next Protocol	***Описание***	***Документ***
0x00	Резерв	RFC 9305
0x01	IPv4	RFC 9305
0x02	IPv6	RFC 9305
0x03	Ethernet	RFC 9305
0x04	NSH	RFC 9305
0x05-0x7D	Не выделены	
0x7E-0x7F	Эксперименты и тестирование	RFC 9305
0x80-0xFD	Не выделены (shim-заголовки)	
0xFE-0xFF	Эксперименты и тестирование (shim-заголовки)	RFC 9305

7. Вопросы безопасности

Соображения безопасности для LISP-GPE похожи на вопросы безопасности и методы смягчения проблем для LISP, описанные в [RFC7835].

Как другие варианты инкапсуляции с применением необязательных расширений, LISP-GPE подвергается воздействию злоумышленников, размещённых на пути доставки, которые могут пытаться изменить пакеты (включая флаг P) для удаления или изменения частей данных (payload) или заявления инкапсуляции иного протокола. **Следует** применять типовые методы защиты целостности (например, IPsec) в сочетании с LISP-GPE для расширений протоколов, которым нужна защита от злоумышленников на пути доставки.

При использовании LISP-GPE такие проблемы, как подмена плоскости данных, лавинные атаки и перенаправление трафика, могут зависеть от конкретного инкапсулируемого протокола.

8. Литература

8.1. Нормативные документы

[IEEE.802.1Q_2014] IEEE, "IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks", IEEE Std 802.1Q-2014, December 2014, <https://ieeexplore.ieee.org/document/6991462>.

[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>.

[RFC6040] Briscoe, B., "Tunnelling of Explicit Congestion Notification", RFC 6040, DOI 10.17487/RFC6040, November 2010, <https://www.rfc-editor.org/info/rfc6040>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9300] Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos, Ed., "The Locator/ID Separation Protocol (LISP)", RFC 9300, DOI 10.17487/RFC9300, October 2022, <https://www.rfc-editor.org/info/rfc9300>.

8.2. Дополнительная литература

[ENCAP-GUIDE] Briscoe, B. and J. Kaippallimalil, "Guidelines for Adding Congestion Notification to Protocols that Encapsulate IP", Work in Progress, Internet-Draft, draft-ietf-tsvwg-ecn-encap-guidelines-17, 11 July 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-tsvwg-ecn-encap-guidelines-17>.

[RFC2003] Perkins, C., "IP Encapsulation within IP", RFC 2003, DOI 10.17487/RFC2003, October 1996, <https://www.rfc-editor.org/info/rfc2003>.

[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>.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, DOI 10.17487/RFC3168, September 2001, <https://www.rfc-editor.org/info/rfc3168>.

[RFC3692] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", BCP 82, RFC 3692, DOI 10.17487/RFC3692, January 2004, <https://www.rfc-editor.org/info/rfc3692>.

[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>.

[RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", RFC 7348, DOI 10.17487/RFC7348, August 2014, <https://www.rfc-editor.org/info/rfc7348>.

[RFC7835] Saucez, D., Iannone, L., and O. Bonaventure, "Locator/ID Separation Protocol (LISP) Threat Analysis", RFC 7835, DOI 10.17487/RFC7835, April 2016, <https://www.rfc-editor.org/info/rfc7835>.

[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>.

[RFC8086] Yong, L., Ed., Crabbe, E., Xu, X., and T. Herbert, "GRE-in-UDP Encapsulation", RFC 8086, DOI 10.17487/RFC8086, March 2017, <https://www.rfc-editor.org/info/rfc8086>.

[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>.

[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>.

[RFC8300] Quinn, P., Ed., Elzur, U., Ed., and C. Pignataro, Ed., "Network Service Header (NSH)", RFC 8300, DOI 10.17487/RFC8300, January 2018, <https://www.rfc-editor.org/info/rfc8300>.

[VXLAN-GPE] Brockners, F., Bhandari, S., Govindan, V., Pignataro, C., Gredler, H., Leddy, J., Youell, S., Mizrahi, T., Kfir, A., Gafni, B., Lapukhov, P., and M. Spiegel, "VXLAN-GPE Encapsulation for In-situ OAM Data", Work in Progress, Internet-Draft, draft-brockners-ippm-ioam-vxlan-gpe-03, 4 November 2019, <https://datatracker.ietf.org/doc/html/draft-brockners-ippm-ioam-vxlan-gpe-03>.

[VXLAN-LISP] Lemon, J., Ed., Maino, F., Smith, M., and A. Isaac, "Group Policy Encoding with VXLAN-GPE and LISP-GPE", Work in Progress, Internet-Draft, draft-lemon-vxlan-lisp-gpe-gbp-02, 30 April 2019, <https://datatracker.ietf.org/doc/html/draft-lemon-vxlan-lisp-gpe-gbp-02>.

Благодарности

Особая благодарность Dino Farinacci за руководство и детальный обзор. Спасибо Tom Herbert за обсуждение и назначение кодов для экспериментов и тестирования.

Участники работы

Редактор этого документа хотел бы поблагодарить и отметить перечисленных ниже участников работы. Эти соавторы и участники предоставили бесценные концепции и содержимое для создания документа.

Darrel Lewis
Cisco Systems, Inc.

Fabio Maino
Cisco Systems, Inc.

Paul Quinn
Cisco Systems, Inc.

Michael Smith
Cisco Systems, Inc.

Navindra Yadav
Cisco Systems, Inc.

Larry Kreeger

Jennifer Lemon
Broadcom

Puneet Agarwal
Innovium

Адреса авторов

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

Jennifer Lemon
Email: jalemon@meus.us

Puneet Agarwal
Innovium
United States of America
Email: puneet@acm.org

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

Michael Smith
Cisco Systems
San Jose, CA 95134
United States of America
Email: michsmit@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru