

Internet Engineering Task Force (IETF)
Request for Comments: 7209
Category: Informational
ISSN: 2070-1721

A. Sajassi
Cisco
R. Aggarwal
Arktan
J. Uttaro
AT&T
N. Bitar
Verizon
W. Henderickx
Alcatel-Lucent
A. Isaac
Bloomberg
May 2014

Requirements for Ethernet VPN (EVPN)

Требования к Ethernet VPN (EVPN)

Аннотация

Широкое распространение услуг Ethernet L2VPN и появление новых применений технологии (например, соединение ЦОД) привели к возникновению набора новых требований, которые не всегда выполняются современными решениями для виртуальных частных ЛВС (Virtual Private LAN Service или VPLS). В частности, не поддерживается многодомность с пересылкой всем активным (all-active) и нет решения для использования путей с коммутацией по меткам (Label Switched Path или LSP) «многие со многими» (Multipoint-to-Multipoint или MP2MP) для оптимизации доставки кадров с множеством получателей. Кроме того, предоставление услуг VPLS даже в контексте основанного на BGP автоматического обнаружения требует от операторов сети указания различных сетевых параметров в дополнение к конфигурации доступа. Этот документ задаёт требования к решениям Ethernet VPN (EVPN) для решения этих проблем.

Статус документа

Этот документ не является спецификацией проекта стандарта Internet и публикуется с информационными целями.

Документ является результатом работы IETF¹ и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG². Не все одобренные IESG документы претендуют на статус Internet Standard (см. раздел 2 в RFC 5741).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <http://www.rfc-editor.org/info/rfc7209>.

Авторские права

Авторские права (Copyright (c) 2014) 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. Терминология.....	2
4. Требования к избыточности.....	3
4.1. Распределение нагрузки по потокам.....	3
4.2. Множество путей по потокам.....	3
4.3. Географически распределенные узлы PE.....	3
4.4. Оптимальная пересылка трафика.....	4
4.5. Поддержка гибкой группировки избыточности.....	4
4.6. Многодомная сеть.....	4
5. Требования к оптимизации групповой передачи.....	4
6. Требования к простоте предоставления.....	4
7. Новые требования к интерфейсу службы.....	5
8. Быстрое схождение.....	5
9. Подавление лавинной рассылки.....	6
10. Гибкая поддержка топологии и политики VPN.....	6
11. Вопросы безопасности.....	6
12. Нормативные документы.....	6
13. Дополнительная литература.....	6
14. Участники работы.....	7

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

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

1. Введение

Виртуальные частные ЛВС (VPLS), определённые в [RFC4664], [RFC4761] и [RFC4762], являются проверенной и широко развёрнутой технологией. Однако у имеющихся решений есть много ограничений в части резервирования, оптимизации групповой передачи и простоты предоставления. Кроме того, новые применения внесли дополнительные требования для других услуг L2VPN, таких как деревья Ethernet (Ethernet Tree или E-Tree) и виртуальные частные провода (Virtual Private Wire Service или VPWS).

В части многодомности современные VPLS могут поддерживать несколько адресов лишь в режиме резервирования single-active (активен один), например, как описано в [VPLS-BGP-MH]. Гибкая многодомность в режиме all-active (активны все) не поддерживается в имеющихся решениях VPLS.

В части оптимизации групповой передачи [RFC7117] описывает способ применения групповых LSP в сочетании с VPLS. Однако это решение ограничено LSP «один со многими» (Point-to-Multipoint или P2MP), поскольку нет определения для многоточечных (Multipoint-to-Multipoint или MP2MP) LSP с VPLS.

В части простоты предоставления текущие VPLS не предлагают механизма одностороннего предоставления, полагаясь на автоматическое обнаружение служб на основе BGP [RFC4761] [RFC6074]. Однако это требует от оператора настройки множества параметров на стороне сети в дополнение к настройке Ethernet на стороне доступа.

В части соединений между ЦОД приложения требуют новых типов интерфейсов служб, комбинирующих свойства интерфейсов со связкой VLAN (bundling) и интерфейсов на основе VLAN. Их называют интерфейсами связывания с поддержкой VLAN (VLAN-aware bundling).

Приложения виртуализации повышают число MAC¹-адресов, обрабатываемых в сети, и это требует, чтобы повторное схождение сети после отказа не зависело от числа MAC-адресов, узанных границей провайдера (Provider Edge или PE).

Имеются требования по минимизации лавинных рассылок кадров с множеством получателей и локализации лавинной рассылки в пределах данного сайта.

Имеются требования по поддержке гибкости топологии и политики VPN сверх доступной сегодня в VPLS и Hierarchical VPLS (H-VPLS).

Основное внимание в этом документе уделено заданию требований к новому решению - Ethernet VPN (EVPN), которое преодолет упомянутые проблемы. В разделе 4 рассмотрены требования к резервированию, в разделе 5 - к оптимизации групповой передачи. В разделе 5 сформулированы требования к предоставлению услуг, а раздел 7 посвящён новым требованиям к интерфейсу сервиса. В разделе 8 рассмотрены требования к быстрому схождению, в разделе 9 - к подавлению лавинной рассылки, а в разделе 10 - к поддержке гибкости топологии и правил VPN.

2. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с [RFC2119].

Этот документ не является спецификацией протокола и уровни требований здесь применяются для ясности и подчёркивания языка требований.

3. Терминология

AS

Автономная система.

CE

Граница клиента.

E-Tree

Дерево Ethernet.

MAC address

Адрес управления доступом к среде - MAC-адрес.

LSP

Путь с коммутацией по меткам.

PE

Граница провайдера.

MP2MP

Многие со многими.

VPLS

Служба виртуальной частной ЛВС.

Single-Active Redundancy Mode

Когда многодомное устройство или сеть подключены к группе из двух или более PE и лишь одно из устройств PE в этой группе может пересылать трафик многодомному устройству или сети (и от них) для данной VLAN, такую многодомную систему называют Single-Active (активен один).

All-Active Redundancy Mode

Когда многодомное устройство или сеть подключены к группе из двух или более PE и все PE группы могут пересылать трафик многодомному устройству или сети (и от них) для данной VLAN, такую многодомную систему называют All-Active (активны все).

¹Media Access Control - управление доступом к среде.

4. Требования к избыточности

4.1. Распределение нагрузки по потокам

Базовый механизм работы многодомного узла CE с набором узлов PE включает применение групп агрегирования каналов Ethernet (link aggregation group или LAG) с несколькими шасси на основе [802.1AX]. В [PWE3-ICCP] описана одна из таких схем. При объединении каналов Ethernet алгоритмы распределения нагрузки, с помощью которых CE распределяет трафик между устройствами подключения (AC) к разным PE, достаточно гибки. Единственным требованием к алгоритмам является обеспечения упорядоченной доставки кадров данного потока трафика. В типичных реализациях эти алгоритмы включают выбор исходящего канала внутри группы на основе хэш-функции, указывающей поток по одному или нескольким полям, указанным ниже.

- i. L2: MAC-адреса отправителя и получателя, VLAN.
- ii. L3: IP-адреса отправителя и получателя.
- iii. L4: порты UDP или TCP у отправителя и получателя.

Важно отметить, что [802.1AX] не определяет стандартный алгоритм распределения нагрузки для связки каналов Ethernet, поэтому поведение разных реализаций различается. На деле связка каналов корректно работает даже при неравномерной загрузке каналов. В этом случае первым требованием для режима all-active является способность обеспечивать гибкое распределение нагрузки на основе потоков от узла CE по полям заголовков L2, L3, L4.

(R1a) Решение **должно** поддерживать гибкое распределение нагрузки по потокам от CE, как указано выше.

(R1b) Решение **должно** поддерживать распределение по потокам трафика, направленного в CE, даже при подключении CE к нескольким PE. Таким образом, решение **должно** быть способно использовать несколько каналов, подключённых к CE, независимо от числа PE, с которыми соединён узел CE.

Следует отметить, что при соединении CE с несколькими PE, возможны равноценные (Equal-Cost Multipath или ECMP) пути от каждого удалённого PE к каждому многодомному PE. Кроме того, для многодомных CE в режиме all-active удалённый PE может выбрать любой из многодомных узлов PE для передачи трафика, адресованного многодомному CE. Следовательно, при поддержке решением режима all-active оно **должно** использовать как можно больше таких путей для трафика к многодомному CE.

(R1c) Решению **следует** поддерживать распределение нагрузки по потокам среди PE, являющихся членами группы резервирования, охватывающей несколько автономных систем (AS).

4.2. Множество путей по потокам

Любое решение, соответствующее режиму избыточности all-active (например, распределение нагрузки по потокам), описанному в параграфе 4.1, должно также использовать множество путей между данной парой PE. Например, при наличии 2 или более LSP между удалённым PE и парой PE в группе all-active, решение должно поддерживать распределение нагрузки этих LSP по потокам для трафика, направленного PE из группы с избыточностью. Кроме того, при наличии 2 или более путей ECMP между удалённым PE и одним из PE в группе с избыточностью решение должно использовать все равноценные LSP. В последнем случае решение может также применять распределение нагрузки на основе меток энтропии [RFC6790].

(R2a) Решение **должно** быть способно использовать все LSP между удалённым PE и всеми PE из группы с избыточностью в режиме all-active.

(R2b) Решение **должно** быть способно использовать все пути ECMP между удалённым PE и любым PE из группы с избыточностью в режиме all-active.

Рассмотрим как пример систему, где устройство CE1 подключено к PE1 и PE2, а CE2 - к PE3 и PE4 в режиме all-active. Кроме того, имеется три пути ECMP между PE устройств CE1 и CE2. Трафик от CE1 к CE2 может пересылаться по 12 разным путям через ядро MPLS/IP. CE1 распределяет нагрузку между PE1 и PE2, у каждого из которых имеется 3 пути ECMP к PE3 и PE4, что даёт 12 путей в целом. Когда трафик прибывает на PE3 и PE4, он пересылается CE2 по каналу Ethernet (связка каналов).

Следует отметить, что поддержка множества путей по потокам дополняет описанное в предыдущем параграфе распределение нагрузки по потокам.

4.3. Географически распределенные узлы PE

Узлы PE, предоставляющие многодомную связность CE или сети доступа, могут размещаться в одном месте (co-located) или быть распределены географически (например, в разных CO¹ или POP²). Последнее требуется для предоставления географической избыточности, которая обеспечивает непрерывность бизнеса при критических повреждениях в случае отключения питания, стихийных бедствий и т. п. Многодомный режим all-active нужен для поддержки обоих вариантов размещения PE. При географическом удалении выделенный канал между PE зачастую не является привлекательным решением с точки зрения расходов. Кроме того, нельзя предполагать, что стоимость IGP от удалённых PE к паре PE в двудомной будет одинаковой при географическим разделении этих PE.

(R3a) Решение должно поддерживать многодомный режим all-active, не требуя выделенного канала данных-управления между PE многодомной группы.

(R3b) Решение должно поддерживать разную стоимость IGP от удалённого PE к каждому из PE многодомной группы.

(R3c) Решение должно поддерживать многодомность через разные домены IGP в одной AS.

(R3d) Решение должно поддерживать многодомность через разные AS.

¹Central Office - центральный офис.

²Point of Presence - точка присутствия.

4.4. Оптимальная пересылка трафика

В типичной сети при рассмотрении назначенной пары PE обычно обнаруживаются подключённые к ним однодомные и многодомные CE.

- (R4) Многодомным решениям all-active **следует** поддерживать оптимальную пересылку индивидуального трафика для всех указанных ниже случаев. Оптимальной считается пересылка, где трафик не пересылается между устройствами PE одной многодомной группы, пока целевое устройство CE не подключено к одному из многодомных PE.
- От однодомного CE к многодомному CE.
 - От многодомного CE к однодомному CE.
 - От многодомного CE к многодомному CE

Это особенно важно в случаях географически разнесённых PE, где пересылка трафика от одного PE к другому в той же многодомной группе вносит дополнительную задержку в добавок к неэффективному использованию пересылки узла PE и ядра. Многодомной (используется также термин multi-chassis LAG) считается группа PE, поддерживающих многодомный CE.

4.5. Поддержка гибкой группировки избыточности

- (R5) Для поддержки гибкой группировки избыточности многодомному механизму следует разрешать произвольную группировку узлов PE в группы с избыточностью, каждая из которых представляет все многодомные устройства/сети, использующие общую группу PE.

Это лучше всего объяснить на примере. Рассмотрим 3 узла PE - PE1, PE2, PE3. Многодомный механизм должен позволять данному PE, скажем PE1, входить одновременно в разные группы с избыточностью. Например, могут быть группы (PE1, PE2), (PE1, PE3), (PE2, PE3), где узлы CE могут быть подключены к любой из этих трёх групп с избыточностью.

4.6. Многодомная сеть

Имеются приложения, которым для подключения к многодомной группе PE нужна сеть Ethernet, а не отдельное устройство. Сеть Ethernet обычно использует механизмы избыточности, такие как протокол MSTP¹ [802.1Q] или защитное переключение в кольце Ethernet (Ring Protection Switching) [G.8032]. PE могут (но не обязаны) принимать участие в работе протокола управления сетью Ethernet. Для многодомных сетей, применяющих [802.1Q] или [G.8032], эти протоколы требуют, чтобы каждая сеть VLAN была активна лишь на одном из многодомных каналов.

- (R6a) Решение **должно** поддерживать подключение к многодомной сети в режиме single-active redundancy, где все VLAN активны на одном PE.
- (R6b) Решение **должно** поддерживать многодомные сети в режиме single-active, где неперекрывающиеся наборы VLAN активны на разных PE.
- (R6c) Решению **следует** поддерживать режим single-active среди PE, принадлежащими к группе с избыточностью, охватывающей несколько AS.
- (R6d) Решение **может** поддерживать режим all-active для многодомной сети с распределением нагрузки на основе MAC (т. е. разные MAC-адреса в VLAN доступны через разные PE).

5. Требования к оптимизации групповой передачи

Имеются среды, где использование MP2MP LSP может быть желательно для оптимизации группового, широковещательного и индивидуального трафика с неизвестным адресатом для снижения числа групповых состояний в маршрутизаторах ядра. [RFC7117] исключает применение MP2MP LSP поскольку текущие решения VPLS требуют от входного PE обучения при получении через LSP индивидуальных пакетов с неизвестным адресатом. Это сложно при использовании MP2MP LSP, поскольку здесь нет унаследованного механизма идентификации отправителя. Применение MP2MP LSP для групповой оптимизации становится приемлемым, если отпадает необходимость определять отправителя при обучении.

- (R7a) Решение **должно** быть способно предоставить механизм, не требующий обучения MAC для MPLS LSP при получении пакетов через MP2MP LSP.
- (R7b) Решение **должно** быть способно предоставить процедуры использования MP2MP LSP для оптимизации доставки группового, широковещательного и индивидуального трафика с неизвестным получателем.

6. Требования к простоте предоставления

По мере внедрения технологий L2VPN в сети предприятий простота предоставления становится первостепенной задачей. Хотя современные VPLS имеют механизм автоматического обнаружения, позволяющий находить PE данного экземпляра VPN через сеть ядра MPLS/IP, требуется дальнейшее упрощение.

- (R8a) Решение **должно** поддерживать автоматическое обнаружение PE в VPN через сеть ядра MPLS/IP подобно механизму автоматического обнаружения VPLS, описанному в [RFC4761] и [RFC6074].
- (R8b) Решению **следует** поддерживать автоматическое обнаружение PE данной группы с избыточностью или многодомной группы.
- (R8c) Решению **следует** поддерживать автоматическое определение идентификатора сайта для многодомного устройства или сети и поддерживать автоматическую генерацию идентификатора группы с избыточностью на основе идентификатора сайта.

¹Multiple Spanning Tree Protocol.

(R8d) Решению **следует** поддерживать автоматизированный выбор DF² среди PE, участвующей в группе с избыточностью (многодомной) и обеспечивать возможность делить экземпляры службы (например, VLAN) между PE в группе с избыточностью.

(R8e) Для развёртываний, где идентификаторы VLAN глобальны в масштабе сети MPLS (т. е. сеть поддерживает не более 4K служб), устройствам PE **следует** выводить относящиеся к MPLS атрибуты (например, VPN ID, BGP Route Target и т. п.) из идентификатора VLAN. Таким образом, сетевому оператору достаточно задать идентификаторы VLAN для устройств доступа, и все параметры MPLS и BGP, требуемые для организации сервиса через сеть ядра, будут выведены автоматически и не потребуют явной настройки.

(R8f) Реализациям **следует** возвращаться к принятым по умолчанию значениям параметров, для которых новые значения не заданы.

7. Новые требования к интерфейсу службы

Для [MEF] и [802.1Q] заданы приведённые ниже службы.

- Режим порта - весь трафик на порту отображается в один домен мостов и один соответствующий экземпляр сервиса L2VPN. Для клиентских VLAN гарантируется сквозная прозрачность.
- Режим VLAN - каждая сеть VLAN на порту отображается в уникальный домен мостов и соответствующий экземпляр сервиса L2VPN. Это позволяет мультиплексировать услуги через один порт и поддерживать необязательную трансляцию VLAN.
- Связка VLAN (bundling) - группа VLAN на порту коллективно отображается в уникальный домен мостов и соответствующий экземпляр сервиса L2VPN. Клиентские адреса MAC должны быть уникальными во всех VLAN, отображаемых в один экземпляр сервиса.

Для каждой из указанных служб назначается один домен мостов на экземпляр сервиса на PE, поддерживающем соответствующую службу. Например, в режиме порта назначается один домен мостов для всех портов, относящихся к этому экземпляру службы, независимо от числа VLAN, проходящих через эти порты.

Следует отметить, что термин домен мостов (bridge domain) относится к таблице пересылки MAC определённой в модели моста IEEE, и не означает и не предполагает определённой реализации.

В [RFC4762] определены два типа служб VPLS на основе неквалифицированного и квалифицированного обучения, которые, в свою очередь делятся на режим порта и VLAN.

(R9a) Решение **должно** поддерживать 3 указанных выше типа служб (порт, VLAN, связка VLAN).

Для размещённых приложений соединения ЦОД сетевым операторам нужна возможность расширять Ethernet VLAN через каналы WAN с использованием обного экземпляра L2VPN, сохраняя при этом разделение плоскостей данных разных VLAN в этом экземпляре. Это называется связкой с поддержкой VLAN (VLAN-aware bundling).

(R9b) Решение **может** поддерживать услугу VLAN-aware bundling.

Это ведёт к появлению двух новых типов интерфейсов сервиса: VLAN-aware bundling с трансляцией и без таковой.

Сервисный интерфейс для VLAN-aware bundling без трансляции имеет указанные ниже характеристики.

- Обеспечивает связывание клиентских VLAN в один экземпляр сервиса L2VPN.
- Гарантирует сквозную прозрачность для клиентских VLAN.
- Поддерживает разделение плоскостей данных между клиентскими VLAN (т. е. создаёт выделенный домен мостов на VLAN).

В особом случае связывания всех с одним (all-to-one) интерфейсу сервиса недопустимо предполагать заранее какие-либо сведения о клиентских VLAN. Иными словами, VLAN клиента не нужно настраивать на PE, а вместо этого интерфейс настраивается как для услуги на основе порта.

Сервисный интерфейс для VLAN-aware bundling с трансляцией имеет указанные ниже характеристики.

- Обеспечивает связывание клиентских VLAN в один экземпляр сервиса L2VPN.
- Поддерживает разделение плоскостей данных между клиентскими VLAN (т. е. создаёт выделенный домен мостов на VLAN).
- Поддерживает трансляцию клиентских VLAN ID для работы в случаях, когда применяются разные идентификаторы VLAN (VID) на разных интерфейсах для обозначения одной клиентской VLAN.

Основным различием в плане выделения ресурсов сервис-провайдером между этими новыми типами услуг и определёнными ранее тремя типами является то, что новым службам нужно выделять несколько доменов мостов (по одному на VLAN клиента) на экземпляр сервиса L2VPN, а прежним достаточно одного домена на экземпляр L2VPN.

8. Быстрое схождение

(R10a) Решение **должно** обеспечивать возможность восстановления после отказов устройства соединения PE-CE, а также отказов узлов PE для многодомного устройства и многодомной сети.

(R10b) Механизм восстановления **должен** обеспечивать время схождения, не зависящее от числа MAC-адресов, изученных PE. Это особенно важно в контексте приложений виртуализации, которые способствуют росту числа MAC-адресов, обрабатываемых сетью L2.

(R10c) Кроме того, механизму восстановления **следует** обеспечивать время схождения, не зависящее от числа экземпляров сервиса, связанных с устройством подключения или PE.

²Designated Forwarder - назначенный узел пересылки.

9. Подавление лавинной рассылки

(R11a) Решению **следует** разрешать оператору сети выбирать, отбрасывание или лавинную рассылку индивидуальных кадров с неизвестным адресатом. Этот атрибут должен быть настраиваемым на уровне экземпляра службы.

(R11b) При использовании решения для соединения ЦОД ему **следует** минимизировать лавинную рассылку широковещательных кадров за пределы данного сайта. Особенный интерес представляет периодический трафик протокола распознавания адресов (Address Resolution Protocol или ARP).

(R11c) Кроме того, решению **следует** избегать ненужной лавинной рассылки индивидуального трафика при изменении топологии, особенно в случае многодомного сайта, где PE заранее знают резервные пути для данного MAC.

10. Гибкая поддержка топологии и политики VPN

(R12a) Решение **должно** поддерживать гибкость топологии VPN, не ограниченной базовыми механизмами решения.

Одним из примеров является топология E-Tree, где один или несколько сайтов в VPN являются корнями, а другие - листьями. Корням можно передавать трафик в другие корни и листья, а листьям разрешено взаимодействовать лишь с корнями. Решение **должно** обеспечивать возможность поддержки топологии E-Tree.

(R12b) Решение **может** обеспечивать возможность применения правил на уровне MAC-адресов, чтобы контролировать, какие PE в VPN узнают о каких MAC-адресах и как пересылается трафик для конкретного MAC. Следует предусматривать возможность применения правил, позволяющих лишь некоторым PE в VPN передавать или принимать трафик для конкретных MAC-адресов.

(R12c) Решение **должно** быть способно поддерживать между AS варианты С и В, описанные в разделе 10 [RFC4364].

11. Вопросы безопасности

Расширениям протоколов для EVPN нужно включать подходящий анализ безопасности. Помимо требований безопасности, описанных в [RFC4761] и [RFC4762] для изучения MAC в плоскости данных и [RFC4364] для изучения MAC в плоскости управления, нужно охватывать указанные ниже аспекты.

(R13) Решение **должно** быть способно обнаруживать и должным образом обрабатывать ситуации, когда один адрес MAC появляется в двух разных сегментах Ethernet (намеренно или случайно).

(R14) Решение **должно** быть способно связывать MAC-адрес с конкретным сегментом Ethernet (sticky MAC), чтобы помочь ограничить вредоносный трафик в сеть для данного MAC. Эта возможность позволит ограничить появление в сети обманных MAC-адресов. При включении этой функции мобильность MAC для таких «липких» (sticky) MAC-адресов будет запрещена и трафик для них из любого другого сегмента Ethernet **должен** отбрасываться.

12. Нормативные документы

[802.1AX] IEEE, "IEEE Standard for Local and metropolitan area networks - Link Aggregation", Std. 802.1AX-2008, IEEE Computer Society, November 2008.

[802.1Q] IEEE, "IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks", Std. 802.1Q-2011, 2011.

[G.8032] ITU-T, "Ethernet ring protection switching", ITU-T Recommendation G.8032, February 2012.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](#), March 1997.

[RFC4364] Rosen, E. and Rekhter, Y., "BGP/MPLS IP Virtual Private Networks (VPNs)", [RFC 4364](#), February 2007¹.

[RFC4761] Kompella, K., Ed., and Y. Rekhter, Ed., "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling", [RFC 4761](#), January 2007.

[RFC4762] Lasserre, M., Ed., and V. Kompella, Ed., "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling", [RFC 4762](#), January 2007.

[RFC6074] Rosen, E., Davie, B., Radoaca, V., and W. Luo, "Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)", [RFC 6074](#), January 2011.

13. Дополнительная литература

[VPLS-BGP-MH] Kothari, B., Kompella, K., Henderickx, W., Balue, F., Uttaro, J., Palislamovic, S., and W. Lin, "BGP based Multi-homing in Virtual Private LAN Service", Work in Progress, July 2013.

[PWE3-ICCP] Martini, L., Salam, S., Sajassi, A., and S. Matsushima, "Inter-Chassis Communication Protocol for L2VPN PE Redundancy", Work in Progress², March 2014.

[MEF] Metro Ethernet Forum, "Ethernet Service Definitions", MEF 6.1 Technical Specification, April 2008.

[RFC4664] Andersson, L., Ed., and E. Rosen, Ed., "Framework for Layer 2 Virtual Private Networks (L2VPNs)", [RFC 4664](#), September 2006.

[RFC6790] Kompella, K., Drake, J., Amante, S., Henderickx, W., and L. Yong, "The Use of Entropy Labels in MPLS Forwarding", RFC 6790, November 2012.

[RFC7117] Aggarwal, R., Ed., Kamite, Y., Fang, L., Rekhter, Y., and C. Kodeboniya, "Multicast in Virtual Private LAN Service (VPLS)", RFC 7117, February 2014.

¹В оригинале ошибочно приведены сведения о RFC 4764, см. <https://www.rfc-editor.org/errata/eid7151>. Прим. перев.

²Опубликовано в RFC 7275. Прим. перев.

14. Участники работы

Samer Salam, Cisco, ssalam@cisco.com

John Drake, Juniper, jdrake@juniper.net

Clarence Filsfils, Cisco, cfilsfil@cisco.com

Адреса авторов

Ali Sajassi

Cisco

E-Mail: sajassi@cisco.com

Rahul Aggarwal

Arktan

E-Mail: raggarwa_1@yahoo.com

James Uttaro

AT&T

E-Mail: uttaro@att.com

Nabil Bitar

Verizon Communications

E-Mail: nabil.n.bitar@verizon.com

Wim Henderickx

Alcatel-Lucent

E-Mail: wim.henderickx@alcatel-lucent.com

Aldrin Isaac

Bloomberg

E-Mail: aisaac71@bloomberg.net

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru