Network Working Group
Request for Comments: 4762
Category: Standards Track

M. Lasserre, Ed.
V. Kompella, Ed.
Alcatel-Lucent

January 2007

Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling

VPLS с использованием сигнализации LDP

Статус документа

В этом документе содержится спецификация протокола, предложенного сообществу Internet. Документ служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации протокола вы можете узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться без ограничений.

Авторские права

Copyright (C) The IETF Trust (2007).

Замечание IESG

Рабочая группа L2VPN создала два отдельных документа - RFC 4761 и этот документ, в которых реализованы похожие функции на основе разных протоколов сигнализации. Отметим, что оба метода обычно называют VPLS, хотя они отличаются и не совместимы друг с другом.

Аннотация

Этот документ описывает решение по организации с использованием псевдопроводов услуг VPLS[1], которые раньше предоставлялись на основе других технологий туннелирования, известных как TLS[2]. VPLS создаёт сегмент эмулируемой ЛВС для заданного множества пользователей, т. е. организуется широковещательный домен L2, поддерживающий обучение и пересылку по адресам Ethernet MAC и ограниченный заданным множеством пользователей. На одном краевом устройстве провайдера (PE[3]) может поддерживаться множество независимых служб VPLS.

Этот документ описывает функции уровня управления для сигнализации меток псевдопровода с использованием протокола LDP[4], расширяющего RFC 4447. Метод не зависит от протокола обнаружения. Описаны также функции пересылки на уровне данных с концентрацией на функциях обучения (learning) для MAC-адресов. Инкапсуляция пакетов VPLS описана в RFC 4448.

Оглавление

1. Введение....2
2. Термины....2
2.1. Уровни требований....2
3. Сокращения....2
4. Топологическая модель для VPLS....3
4.1. Пересылка и лавинная рассылка....3
4.2. Изучение адресов....3
4.3. Топология туннелей....4
4.4. VPLS без петель....4
5. Обнаружение....4
6. Уровень управления....4
6.1. Сигнализация демультиплексоров на базе LDP....4
6.1.1. Использование обобщённого элемента PWid FEC....4
6.2. Отзыв MAC-адресов....4
6.2.1. TLV со списком MAC....5
6.2.2. Сообщение об отзыве с TLV со списком MAC-адресов....5
7. Пересылка данных в Ethernet PW....5
7.1. Инкапсуляция VPLS....5
7.2. Обучение VPLS....6
8. Пересылка данных в Ethernet VLAN PW....6
8.1. Инкапсуляция VPLS....6
9. Работа VPLS....7
9.1. Старение MAC-адресов....7
10. Иерархическая модель VPLS....7
10.1. Иерархическая связность....7
10.1.1. Лучевая связность для устройств с функциями моста....7
10.1.1.1. Работа MTU-s....8
10.1.1.2. Работа PE-rs....8
10.1.2. Преимущества лучевых соединений....8

[1]Virtual Private LAN Service - услуги виртуальной частной ЛВС.
[2]Transparent LAN Services - услуги «прозрачной ЛВС».
[3]Provider Edge.
[4]Label Distribution Protocol.

10.1.3. Лучевые соединения для устройств, не являющихся мостами....8
10.2. Избыточные лучевые соединения....9
10.2.1. Двудомный MTU-s....9
10.2.2. Обнаружение отказов и восстановление....10
10.3. Многодоменный сервис VPLS....10
11. Иерархическая модель VPLS с сетями доступа Ethernet....10
11.1. Расширяемость....10
11.2. Двудомные устройства и восстановление при отказах....11
12. Участники работы....11
13. Благодарности....11
14. Вопросы безопасности....11
15. Взаимодействие с IANA....11
16. Литература....11
16.1. Нормативные документы....11
16.2. Дополнительная литература....12
Приложение A. Сигнализация VPLS с использованием PWid FEC....12

1. Введение

Технология Ethernet стала преобладающей в сфере локальных сетей (ЛВС) и получает признание в качестве технологии доступа, особенно в городских и распределенных сетях (MAN[1] и WAN[2], соответственно). Основным назначением служб VPLS является обеспечение связности между географически разделёнными пользовательскими сайтами через сети MAN и WAN, как будто эти сайты подключены к одной ЛВС. Предполагаемые применения для конечных пользователей можно разделить на две категории:

- соединение маршрутизаторов абонента - маршрутизация ЛВС;
- соединение коммутаторов абонента - коммутация ЛВС.

В традиционных ЛВС доступны широковещательные и групповые услуги. Сайты одного широковещательного домена, соединённые через сеть MPLS, ожидают корректной пересылки широковещательного, группового и индивидуального трафика. Это требует поддержки функций изучения и старения адресов MAC на уровне псевдопровода, репликации пакетов через псевдопровод для широковещательного и группового трафика, а также лавинной рассылки трафика для неизвестных индивидуальных адресов.

[RFC4448] определяет способ передачи кадров L2 через псевдопровод (PW) «точка-точка». Этот документ описывает расширение [RFC4447] для транспортировки трафика Ethernet/802.3 и VLAN [802.1Q] через множество сайтов, относящихся к одному широковещательному домену L2 или VPLS. Отметим, что та же модель может применяться к другим технологиям 802.1. Она описывает простой и расширяемый способ обеспечивать услуги виртуальных ЛВС, включая подобающую рассылку широковещательного, группового и индивидуального трафика неизвестных адресатов через сеть MPLS, без необходимости использовать серверы преобразования адресов или иные внешние серверы, как описано в [L2VPN-REQ].

Приведённое ниже обсуждение применимо к устройствам, способным поддерживать VPLS и туннелировать пакеты с метками между собой. Полученное в результате множество соединённых между собой устройств образует MPLS VPN.

2. Термины

Q-in-Q
Расширение 802.1ad Provider Bridge, известное также как стековые VLAN и Q-in-Q.

Qualified learning - квалифицированное обучение
Режим обучения, в котором каждая VLAN абонента отображается на свой экземпляр VPLS.

Service delimiter - указатель сервиса
Информация, используемая для идентификации конкретного экземпляра абонентского сервиса. Обычно представляется в заголовке инкапсуляции абонентских кадров (например, VLAN Id).

Tagged frame - кадр с тегом
Кадр с идентификатором 802.1Q VLAN.

Unqualified learning - неквалифицированное обучение
Режим обучения, в котором все VLAN одного абонента отображаются на один экземпляр VPLS.

Untagged frame - кадр без тега
Кадр, не имеющий идентификатора 802.1Q VLAN.

2.1. 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 интерпретируются в соответствии с RFC 2119 [RFC2119].

3. Сокращения

AC	Attachment Circuit (устройство подключения).
BPDU	Bridge Protocol Data Unit (блок данных протокола мостов).
CE	Customer Edge device (краевое устройство абонента).
FEC	Forwarding Equivalence Class (класс эквивалентности пересылки).
FIB	Forwarding Information Base (база информации для пересылки).
GRE	Generic Routing Encapsulation (базовая инкапсуляция маршрутных данных).

[1]Metropolitan Area Network.
[2]Wide Area Network.

IPsec	IP security (безопасность IP).
L2TP	Layer Two Tunneling Protocol (туннельный протокол уровня 2).
LAN	Local Area Network (локальная сеть, ЛВС).
LDP	Label Distribution Protocol (протокол распространения меток).
MTU-s	Multi-Tenant Unit switch (коммутатор для множества арендаторов).
PE	Provider Edge device (краевое устройство провайдера).
PW	Pseudowire (псевдопровод).
STP	Spanning Tree Protocol (протокол связующего дерева).
VLAN	Virtual LAN (виртуальная ЛВС).
VLAN tag	VLAN Identifier (идентификатор VLAN).

4. Топологическая модель для VPLS

Участвующий в VPLS интерфейс должен быть способен рассылать в лавинном режиме (flood), пересылать и фильтровать кадры Ethernet. На рисунке 1 показана топологическая модель VPLS. Множество устройств PE, соединённых между собой псевдопроводами PW, представляется одной эмулируемой ЛВС для абонента X. Каждое устройство PE будет формировать MAC для своего PW и связывать подключённые напрямую MAC-адреса с локальными портами в сторону абонента. Это моделирует стандартное обучение IEEE 802.1 MAC.

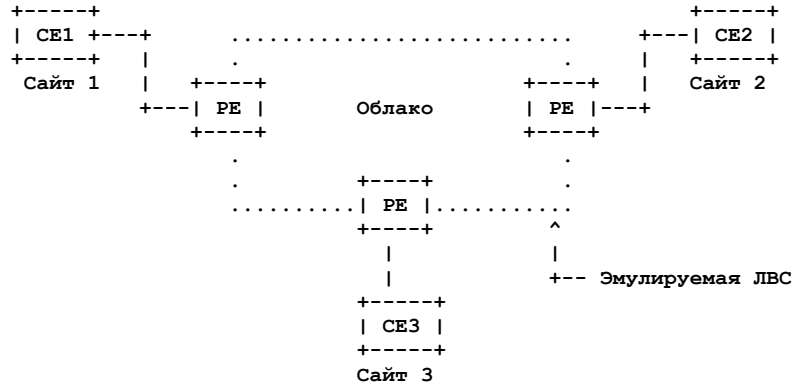


Рисунок 1. Топологическая модель VPLS для абонента с 3 сайтами.

Отметим ещё раз, что в документе приводятся конкретные примеры использования транспортных туннелей MPLS, но PW могут применять и другие туннели (как указано в [RFC4447]), например, GRE, L2TP, IPsec, если они позволяют идентифицировать исходное устройство PE, поскольку это нужно для процесса обучения MAC.

Областью применения VPLS являются устройства PE в сети сервис-провайдера и это подчёркивает тот факт, что кроме разграничения абонентского сервиса, форма доступа к сайту абонента никак не связана с VPLS [L2VPN-REQ]. Иными словами, устройство присоединения (AC), подключённое к абоненту, может быть физическим портом Ethernet, логическим (тег) портом Ethernet, ATM PVC, передающим кадры Ethernet и т. п., включая даже Ethernet PW.

PE обычно является граничным маршрутизатором, способным работать с сигнальным протоколом LDP и/или протоколами маршрутизации для организации PW. Кроме того, он способен организовывать транспортные туннели к другим PE и доставлять трафик через PW.

4.1. Пересылка и лавинная рассылка

Одним из свойств сервиса Ethernet является передача кадров по широковещательным адресам и лавинная рассылка во все порты кадров с неизвестным MAC-адресом получателя. Для лавинной рассылки в сети сервис-провайдера все кадры с неизвестным индивидуальным адресом, а также широковещательные и групповые кадры рассылаются в лавинном режиме через все соответствующие PW всем узлам PE, участвующим в VPLS, а также всем устройствам AC.

Отметим, что групповые кадры являются особым случаем и не обязательно требуют рассылки всем членам VPN. Для простоты по умолчанию используется широковещательная рассылка групповых кадров.

Для пересылки кадра устройство PE **должно** быть способно связать MAC-адрес получателя с PW. Неразумно, а порой и невозможно требовать настройки на всех PE статической привязки всех возможных MAC-адресов к PW. Поэтому поддерживающим VPLS устройствам PE **следует** иметь возможность динамического изучения MAC на AC и PW, а также пересылки и репликации пакетов через AC и PW.

4.2. Изучение адресов

В отличие от BGP VPN [RFC4364], информация о доступности не анонсируется и не распространяется на уровне управления. Доступность определяется стандартными функциями обучения моста на уровне данных.

Если для пришедшего в PW пакета MAC-адрес отправителя не известен, его нужно связать с PW, чтобы исходящие пакеты на этот MAC-адрес могли доставляться через соответствующий PW. Аналогично, при поступлении в AC пакета с неизвестным MAC-адресом отправителя адрес нужно связать с AC, чтобы исходящие пакеты на этот MAC-адрес могли доставляться через соответствующее устройство AC.

При смене состояния PW или AC требуется выполнять стандартные операции обучения, фильтрации и рассылки, определённые в [802.1D-ORIG], [802.1D-REV] и [802.1Q].

4.3. Топология туннелей

Предполагается, что маршрутизаторы PE способны организовывать транспортные туннели между собой для агрегирования трафика. Сигнализация PW служит для демультиплексирования инкапсулированных кадров Ethernet разных экземпляров VPLS, которые передаются через транспортные туннели.

В Ethernet L2VPN на сервис-провайдера ложится ответственность за создание топологии без петель. Для простоты определим топологию VPLS как полносвязный (full mesh) набор PW.

4.4. VPLS без петель

Если топология VPLS не является полносвязной, может оказаться, что пара PE не связана напрямую через PW и будет использовать промежуточные PE для трансляции пакетов. Такая топология будет требовать применения того или иного протокола устранения петель, подобного STP.

Вместо этого между PE организуется полносвязная сеть PW. Поскольку в этом случае каждое устройство PE напрямую соединяется со всеми другими PE в составе VPLS через псевдопровод PW, трансляция пакетов уже не требуется и можно использовать для устранения петель простое правило «расщепления горизонта» (split horizon), в соответствии с которым PE **недопустимо** пересылать трафик из одного PW в другой из состава той же сети соединений VPLS.

Отметим, что абоненты могут применять протокол STP (скажем, в соответствии с [802.1D-REV]), например, при наличии у абонента дополнительных соединений (back door) для резервирования на случай отказа в VPLS. В таких случаях STP BPDU[1] просто туннелируются через облако провайдера.

5. Обнаружение

Требуется возможность настройки адресов удалённых PE вручную. Однако ручная настройка перестаёт быть необходимой при использовании процедур автоматического обнаружения. Данный документ совместим со множеством процедур автоматического обнаружения ([RADIUS-DISC], [BGP-DISC]).

6. Уровень управления

Этот документ описывает функции уровня управления для сигнализации меток PW. Выполнены некоторые базовые работы в части поддержки многодомности (multi-homing). Расширениям, обеспечивающим многодомность, следует работать независимо от базовых операций VPLS и здесь они не рассматриваются.

6.1. Сигнализация демультиплексоров на базе LDP

Полная связность сессий LDP служит для организации сети PW. Требование полносвязной сети PW может приводить к большому числу сессий LDP. В разделе 10 рассмотрен вариант организации иерархической топологии для снижения числа связей в VPLS.

Поскольку сессии LDP организуются между двумя PE, все PW между этими двумя PE сигнализируются в одной сессии.

В [RFC4447] описано два типа FEC - PWid FEC Element (FEC типа 128) и Generalized PWid FEC Element (FEC типа 129). Исходные элементы FEC, применяемые для VPLS, совместимы с PWid FEC Element. Описание сигнализации с использованием элементов PWid FEC перенесено в Приложение A. Ниже вместо этого описано применение более обобщённого дескриптора L2VPN - Generalized PWid FEC Element.

6.1.1. Использование обобщённого элемента PWid FEC

В [RFC4447] описана обобщённая структура FEC, которая будет применяться для сигнализации VPLS, описанной ниже. Рассматривается назначение полей Generalized PWid FEC Element в контексте сигнализации VPLS.

Control bit (C) - слово управления
Этот бит указывает использование слова управления, описанного в [RFC4447].

PW type - тип псевдопровода
Разрешёнными типами PW являются Ethernet (0x0005) и Ethernet tagged (0x004), как указано в [RFC4446].

PW info length – размер информации псевдопровода
В соответствии с [RFC4447].

Attachment Group Identifier (AGI), Length, Value – идентификатор группы подключения, размер, значение
Уникальное имя данной VPLS. AGI указывает тип имени, а Length - размер поля Value, в котором задано имя VPLS. Термин AGI используется наравне с термином «идентификатор VPLS».

Target Attachment Individual Identifier (TAII), Source Attachment Individual Identifier (SAII)
Это пустые (null) значения, поскольку сеть PW в VPLS завершается таблицами обучения MAC, а не отдельными устройствами подключения. Использование непустых TAII и SAII зарезервировано на будущее.

Interface Parameters – параметры интерфейса

MTU
Максимальный размер передаваемого блока (MTU[2]) в VPLS **должен** совпадать для всех PW в сети (mesh).

Optional Description String – необязательная строка описания
В соответствии с [RFC4447].

Requested VLAN ID – запрошенный идентификатор VLAN
Если PW работает в режиме Ethernet с тегами, этот параметр может служить для сигнализации вставки подходящего VLAN ID, как определено в [RFC4448].

6.2. Отзыв MAC-адресов

Может оказаться желательным удаление или отмена обучения (unlearn) для определённых динамически MAC-адресов с целью ускорить схождение. Это достигается передачей сообщения LDP Address Withdraw со списком MAC-адресов для удаления всем другим PE через соответствующие сессии LDP.

[1] Bridge PDU - блок данных протокола мостов.
[2] Maximum Transmission Unit.

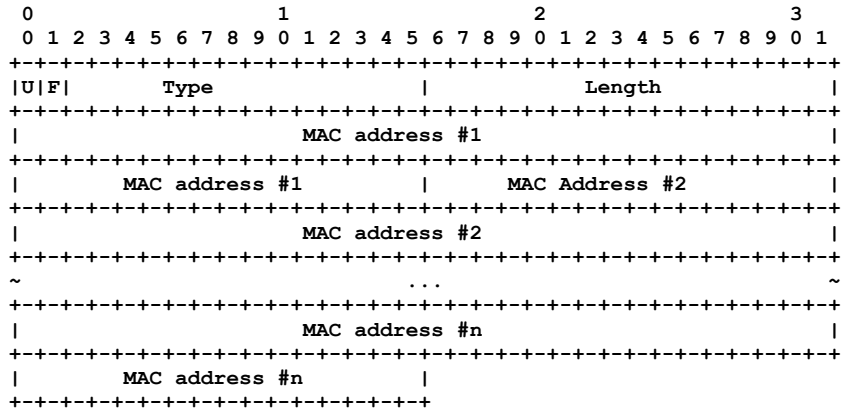
Здесь определяется необязательный элемент MAC List TLV в LDP для задания списка MAC-адресов, которые будут удалены (или для них будет отменено обучение) с помощью сообщений LDP Address Withdraw.

Сообщения Address Withdraw с MAC List TLV **могут** поддерживаться для ускоренного удаления MAC-адресов в результате изменения топологии (например, отказ основного канала для двудомного коммутатора с поддержкой VPLS).

Для минимизации влияния на схождение LDP при наличии в MAC List TLV большого числа MAC-адресов, может оказаться предпочтительной отправка отзывающего сообщения с пустым списком MAC-адресов.

6.2.1. TLV со списком MAC

Отмена обучения (unlearn) для MAC-адреса может быть указана передачей сообщения LDP Address Withdraw с новым MAC List TLV, формат которого описан ниже. Представление адреса MAC List TLV в 6-октетном формате MAC определено документами IEEE 802 [802.1D-ORIG] [802.1D-REV].



U bit

Флаг неизвестности, который **должен** иметь значение 1. Если формат MAC-адреса не распознан, элемент TLV также не будет понят и **должен** игнорироваться.

F bit

Флаг пересылки, который **должен** иметь значение 0. Поскольку применяется адресный (targeted) механизм LDP, пересылка TLV **недопустима**.

Type

Поле типа, которое **должно** иметь значение 0x0404 (MAC List TLV).

Length

Поле, указывающее общий размер (в октетах) MAC-адресов в TLV. Размер **должен** быть кратным 6.

MAC Address

MAC-адрес(а) для удаления.

Сообщение MAC Address Withdraw содержит FEC TLV (для указания VPLS), MAC Address TLV и необязательные параметры. Для сигнализации MAC Address Withdraw необязательных параметров не определено. Отметим, что при получении устройством PE непонятного сообщения MAC Address Withdraw, сообщение **должно** игнорироваться. В этом случае вместо очистки таблицы MAC-адресов будет продолжаться использование несвежей информации, пока не возникнет одно указанных ниже условий.

- Принят пакет с известной привязкой MAC-адреса из другого PW, которая заменит прежнюю привязку.
- Привязка устарела.

Сообщения MAC Address Withdraw лишь помогают ускорить схождение, поэтому PE, не понимающие сообщения, продолжат участвовать в VPLS.

6.2.2. Сообщение об отзыве с TLV со списком MAC-адресов

Обработка MAC List TLV из полученного сообщения Address Withdraw включает перечисленные ниже операции.

- Для каждого MAC-адреса в TLV удаляется привязка к AC или PW, откуда было принято сообщение.
- Для каждого сообщения MAC Address Withdraw с пустым списком адресов удаляются все MAC-адреса, связанные с экземпляром VPLS (задаётся FEC TLV), за исключением MAC-адресов, узнанных (learned) через PW, связанный с сигнальной сессией, в которой получено сообщение.

Областью действия MAC List TLV является VPLS, указанная полем FEC TLV в сообщении MAC Address Withdraw. Число MAC-адресов можно определить из поля размера TLV.

7. Пересылка данных в Ethernet PW

В этом разделе описано поведение уровня данных Ethernet PW, используемых в VPLS. Хотя инкапсуляция похожа на описанную в [RFC4448], функции вырезания указывающего сервис тега и использование «нормализованных» кадров Ethernet дополнительно описаны здесь.

7.1. Инкапсуляция VPLS

В VPLS абонентские кадры Ethernet без преамбулы инкапсулируются с заголовком, определенным в [RFC4448]. Определение типов абонентских кадров Ethernet приведено ниже.

- Если полученный PE кадр имеет инкапсуляцию, используемую данным PE в качестве обозначения сервиса (т. е. для идентификации конкретного абонента и/или конкретного сервиса для данного абонента), инкапсуляцию можно вырезать до отправки кадра в VPLS. На выходе кадра из VPLS сервисный тег может быть возвращён.

- Если пришедший в PE кадр имеет инкапсуляцию, не используемую данным PE в качестве обозначения сервиса, инкапсуляцию кадра не следует менять в VPLS. К таким кадрам относятся, например, кадры с заданными клиентом тегами VLAN, о которых сервис-провайдер не знает и которые не хочет менять.

Пользовательский кадр может прийти на обращённый в сторону абонента порт с тегом VLAN, указывающим экземпляр абонентского сервиса VPLS. Такой тег будет вырезаться до инкапсуляции в VPLS. На выходе тег может быть вставлен снова, если используется обозначение сервиса тегами.

Аналогично при поступлении кадра на обращённый в сторону абонента порт через ATM или Frame Relay VC, указывающий экземпляр абонентской VPLS, инкапсуляция ATM или FR будет удалена перед отправкой кадра в VPLS.

И напротив, при получении на обращённом в сторону абонента порту кадра с тегом VLAN, указывающим домен VLAN в абонентской сети L2, этот тег будет сохранен, поскольку он связан с остальной частью кадра.

В соответствии с этими правилами проходящие через VPLS кадры Ethernet всегда являются абонентскими. Отметим, что действия на входе и выходе с указывающими сервис тегами являются локальными и ни одно из устройств PE не сигнализирует другим о таких действиях. Это позволяет, например, смешивать и сопоставлять службы с тегами VLAN и без таковых на любой стороне и не передавать через VPLS теги VLAN с локальной значимостью. Указателем сервиса может служить и метка MPLS, поэтому Ethernet PW, определённый в [RFC4448], может применяться соединением для доступа к PE. Инкапсуляция RFC 1483 Bridged PVC также может указывать сервис. На основе ограничения области локальной значимости инкапсуляции краевыми устройствами, можно создать иерархическую модель VPLS для обеспечения возможности создания расширяемых систем VPLS, как описано ниже.

7.2. Обучение VPLS

Обучение выполняется на основе абонентских кадров Ethernet, как определено выше. База пересылки FIB отслеживает отображение адреса абонентского кадра Ethernet на подходящий PW. Определим два режима обучения - квалифицированный и неквалифицированный. Квалифицированное обучение применяется по умолчанию и **должно** поддерживаться, неквалифицированное обучение является **необязательным**.

При неквалифицированном обучении все VLAN одного абонента обслуживаются одной VPLS, что означает использование одного широковещательного домена и адресного пространства MAC. Поэтому MAC-адреса должны быть уникальными и не перекрываться в разных VLAN абонента, поскольку в противном случае их не удастся различить в VPLS и это может приводить к потере абонентских кадров. Применение неквалифицированного обучения представляет собой сервис VPLS на основе портов (т. е. абонентские AC не мультиплексируются и весь трафик на физическом порту, который может включать множество абонентских VLAN, отображается на один экземпляр VPLS).

При квалифицированном обучении каждой абонентской VLAN назначается свой экземпляр VPLS, что означает для каждой VLAN абонента отдельный домен широковещания и адресное пространство MAC. Поэтому при квалифицированном обучении MAC-адреса в разных VLAN абонента могут перекрываться, но корректность их обработки будет обеспечиваться использованием в каждой VLAN отдельной FIB, т. е. каждая VLAN абонента будет иметь своё пространство MAC-адресов. Поскольку VPLS по умолчанию передаёт групповые кадры в широковещательном режиме, квалифицированное обучение сужает область широковещания до одной абонентской VLAN. Квалифицированное обучение может приводить к росту размеров FIB, поскольку в таблицах будут храниться MAC-адреса вместе с тегами VLAN.

Для использования STP с квалифицированным обучением устройства VPLS PE должны быть способны пересылать STP BPDU нужным экземплярам VPLS. В иерархическом варианте VPLS (см. раздел 10) могут добавляться теги обозначения сервиса (Q-in-Q или [RFC4448]), чтобы PE могли однозначно идентифицировать весь абонентский трафик, включая STP BPDU. В базовом варианте VPLS восходящие коммутаторы должны вставлять такие теги обозначения сервиса. Когда порт доступа используется для множества абонентов, должны применяться зарезервированные теги VLAN для абонентских доменов, чтобы передавать трафик STP. Кадры STP инкапсулируются с уникальными для каждого абонента провайдерскими тегами (как и обычный трафик абонентов), а PE просматривают эти теги для передачи таких кадров через соответствующий экземпляр VPLS.

8. Пересылка данных в Ethernet VLAN PW

В этом разделе описано поведение уровня данных для Ethernet VLAN PW в VPLS. Хотя инкапсуляция похожа на описанную в [RFC4448], ниже рассмотрены функции наложения тегов и использования «нормализованных» кадров Ethernet. Обучение выполняется так же, как для Ethernet PW.

8.1. Инкапсуляция VPLS

В VPLS абонентские кадры Ethernet без преамбулы инкапсулируются с заголовком, определенным в [RFC4448]. Определение типов абонентских кадров Ethernet приведено ниже.

- Если принятый PE кадр имеет инкапсуляцию, которая является частью пользовательского кадра и служит данному PE в качестве обозначения сервиса (т. е. для идентификации конкретного абонента и/или конкретного сервиса для данного абонента), инкапсуляция сохраняется при передаче кадра в VPLS, если не указан необязательный параметр Requested VLAN ID (в этом случае тег VLAN заменяется до отправки кадра в PW).

- При поступлении в PE кадра с инкапсуляцией без требуемого тега VLAN, в него добавляется пустой (null) тег, если не задан необязательный параметр Requested VLAN ID.

Пользовательский кадр может прийти на обращённый в сторону абонента порт с тегом VLAN, указывающим экземпляр абонентского сервиса VPLS, а также VLAN абонента. Такой тег будет сохранен при инкапсуляции в VPLS.

Ethernet VLAN PW обеспечивает простой способ сохранить абонентские биты 802.1p.

VPLS **может** включать оба типа псевдопроводов - Ethernet и Ethernet VLAN. Однако при невозможности поддержки в PE одновременно обоих типов PW **следует** передавать в неподдерживаемые PW сообщение Label Release с кодом «Unknown FEC», как указано в [RFC3036].

9. Работа VPLS

На рисунке 2 показан пример, где услуги VPLS обеспечиваются между PE1, PE2 и PE3. VPLS объединяет 4 сайта абонента (A1, A2, A3, A4), подключённые через устройства CE1, CE2, CE3 и CE4, соответственно.

Изначально VPLS организуется так, что PE1, PE2 и PE3 имеют полносвязный набор Ethernet PW. Экземпляр VPLS указывается идентификатором AGI. В этом примере PE1 сообщает метку PW 102 устройству PE2 и 103 - устройству PE3, а PE2 сообщает метку 201 устройству PE1 и 203 - устройству PE3.

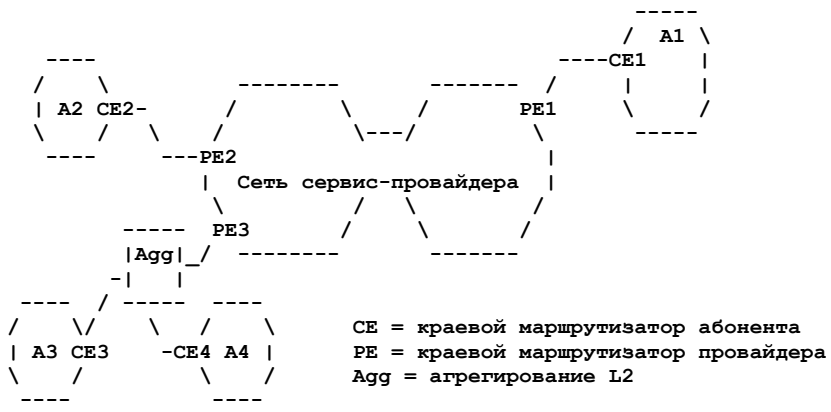


Рисунок 2. Пример VPLS.

Предположим, что пакет из A1 предназначен для A2. Он приходит на CE1 с MAC-адресом отправителя M1 и MAC-адресом получателя M2. Если PE1 не знает, где находится M2, он использует лавинную рассылку пакета, т. е. передаст его PE2 и PE3. PE2 получит этот пакет с меткой PW 201 и может сделать вывод, что MAC-адрес M1 расположен за PE1, поскольку метка 201 была передана PE1. Поэтому можно связать MAC-адрес M1 с меткой PW 102.

9.1. Старение MAC-адресов

Устройствам PE, изучающим удалённые MAC-адреса, **следует** иметь механизм старения, позволяющий удалять неиспользуемые записи, связанные с меткой PW. Это важно как для экономии памяти, так и для администрирования. Например, если абонентский сайт A[1] отключён, другие PE должны в конце концов «забыть» MAC-адреса этого сайта.

Таймер старения для MAC-адреса M **следует** сбрасывать при получении пакета с MAC-адресом отправителя M.

10. Иерархическая модель VPLS

Описанное выше решение требует полносвязного набора туннелей LSP между маршрутизаторами PE, участвующими в сервисе VPLS. Для каждой услуги VPLS должно быть организовано n*(n-1)/2 PW между маршрутизаторами PE. Хотя это ведёт к издержкам на сигнализацию, реальной проблемой для крупномасштабных систем являются требования репликации пакетов для каждого псевдопровода PW на маршрутизаторе PE. Описанные в этом документе иерархические соединения снижают издержки на сигнализацию и репликацию, позволяя создавать большие системы.

Зачастую сервис-провайдеры размещают небольшое число устройств в зданиях со множеством арендаторов и затем агрегируют их в PE центрального офиса (CO[2]). В некоторых случаях могут применяться стандартные теги IEEE 802.1q для более простого отображения интерфейсов CE на каналы доступа в VPLS на маршрутизаторах PE.

Часто выгодно распространить методы туннелирования услуг VPLS на домен коммутируемого доступа. Это можно сделать путём реализации устройств доступа как PE и организации PW между ними и другими краевыми устройствами как базового сервиса VPLS. Другим способом является применение [RFC4448] PW или логических интерфейсов Q-in-Q между устройством доступа и выбранными маршрутизаторами PE с поддержкой VPLS. Инкапсуляция Q-in-Q является другой формой туннелирования L2, которая может применяться с сигнализацией MPLS, как описано ниже. В двух приведённых ниже сценариях рассматривается альтернативный подход. PW ядра VPLS (концентратор) дополняются PW доступа (лучи) для формирования 2-уровневой иерархической VPLS (H-VPLS).

Лучевые PW могут быть реализованы с помощью любого туннельного механизма L2 и за счёт расширения первого уровня путём включения маршрутизаторов VPLS PE без функций моста. Такие PE будут расширять лучевые PW от коммутатора L2, подключённого к ним через ядро сети оператора, к маршрутизатору VPLS PE с функциями моста, служащему концентратором PW. Мы опишем также участие требуемых для VPLS узлов и простых CE без поддержки MPLS в работе иерархической VPLS.

В оставшейся части документа устройства с поддержкой функций моста обозначаются MTU-s, а PE без функций моста - PE-r. Устройства с поддержкой функций моста и маршрутизатора обозначаются PE-rs.

10.1. Иерархическая связность

В этом параграфе описана модель соединений в виде концентратора с лучами (hub and spoke - звезда) и требования к мостам и устройствам MTU-s для поддержки лучевых соединений.

10.1.1. Лучевая связность для устройств с функциями моста

На рисунке 3 к устройству MTU-s подключены три абонентских сайта через устройства CE-1, CE-2, CE-3. MTU-s имеет одно соединение (PW-1) с PE1-rs, а это устройство подключено к полносвязному базовому сервису VPLS. Для каждого сервиса VPLS организуется один лучевой PW между MTU-s и PE-rs на базе [RFC4447]. В отличие от традиционных PW, завершающихся на физическом (или логическом с тегом VLAN) порту, лучевой PW завершается на экземпляре виртуального коммутатора (Virtual switch instance или VSI, см [L2FRAME]) на устройствах MTU-s и PE-rs.

[1]Предложено исключить в этом предложении указание конкретного сайта A. См. https://www.rfc-editor.org/errata/eid4834. *Прим. перев.*
[2]Central Office.

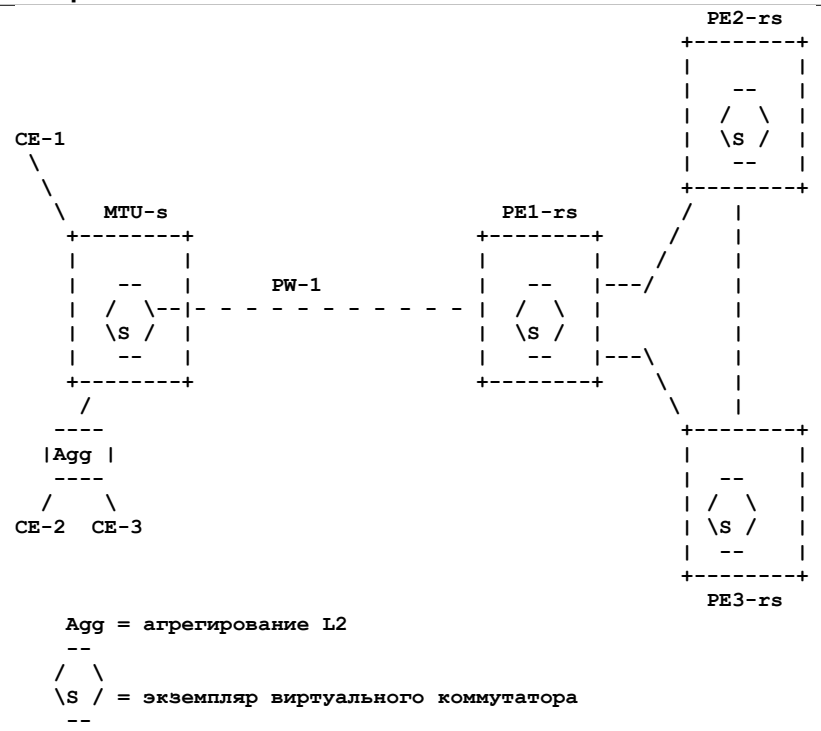


Рисунок 3. Пример иерархической модели VPLS.

MTU-s и PE-rs рассматривают каждое лучевое соединение подобно AC в сервисе VPLS. Метка PW служит для привязки трафика луча к экземпляру VPLS.

10.1.1.1. Работа MTU-s

MTU-s определяется как устройство, поддерживающее функциональность коммутатора L2 и все обычные функции обучения и репликации кадров во все порты, включая луч, рассматриваемый как виртуальный порт. Пакеты для неизвестных получателей реплицируются во все обслуживаемые порты, включая порт луча. После изучения MAC-адресов трафик между CE1 и CE2 будет локально коммутироваться MTU-s, снижая загрузку луча в направлении PE-rs. Аналогично, трафик между CE1 или CE2 и любым удаленным адресатом коммутируется напрямую в луч и передаётся PE-rs через PW «точка-точка».

Поскольку MTU-s поддерживает функции моста, требуется лишь один псевдопровод PW на экземпляр VPLS при любом числе соединений доступа в одном сервисе VPLS. Это также снижает издержки на сигнализацию между MTU-s и PE-rs.

Если устройство MTU-s напрямую подключено к PE-rs, в луче могут применяться другие методы инкапсуляции (например, Q-in-Q).

10.1.1.2. Работа PE-rs

PE-rs представляет собой устройство, поддерживающее все функции моста для сервиса VPLS, а также маршрутизацию и инкапсуляцию MPLS, т. е. все описанные выше функции для базового сервиса VPLS.

Работа PE-rs не зависит от типа устройства на другой стороне луча. Таким образом, луч от MTU-s рассматривается как виртуальный порт и PE-rs будет коммутировать трафик между лучевым PW, псевдопроводами концентратора PW и устройствами AC после изучения MAC-адресов.

10.1.2. Преимущества лучевых соединений

Лучевые соединения обеспечивают несколько преимуществ в плане расширения и эксплуатации при создании крупномасштабных систем VPLS, сохраняя возможность предлагать полную функциональность VPLS.

- Снимается необходимость организации полносвязной сети туннелей и PW для всех устройств, участвующих в сервисе VPLS.
- Снижаются издержки на сигнализацию за счёт снижения числа PW, требуемых для сервиса VPLS.
- Узловое обнаружение сегментов VPLS. MTU-s нужно знать лишь узел PE-rs, хотя устройство участвует в сервисе VPLS, охватывающем множество устройств. С другой стороны, каждое устройство VPLS PE-rs должно знать о всех других VPLS PE-rs, а также о всех локально подключённых устройствах MTU-s и PE-r.
- Добавление других сайтов требует настройки новых MTU-s, но не требует какого-либо обеспечения для имеющихся в данном сервисе устройств MTU-s.
- Иерархические соединения могут служить для организации сервиса VPLS через множество доменов сервис-провайдеров, как описано ниже.

Отметим, что по мере роста числа устройств, участвующих в VPLS, растёт и число устройств, в которых требуется поддержка обучения и репликации.

10.1.3. Лучевые соединения для устройств, не являющихся мостами

В некоторых случаях поддерживающие функции мостов устройства PE-rs могут отсутствовать в сети или устройства PE-r могут быть уже установлены. В этом параграфе описано, как устройства PE-r, не поддерживающие функций мостов VPLS, могут применяться для сервиса VPLS.

На рисунке 4 три абонентских сайта (CE-1, CE-2, CE-3) подключены к VPLS через устройство PE-r. Для каждого устройства подключения, участвующего в сервисе VPLS, маршрутизатор PE-r создаёт PW «точка-точка», завершающиеся на VSI маршрутизатора PE1-rs.

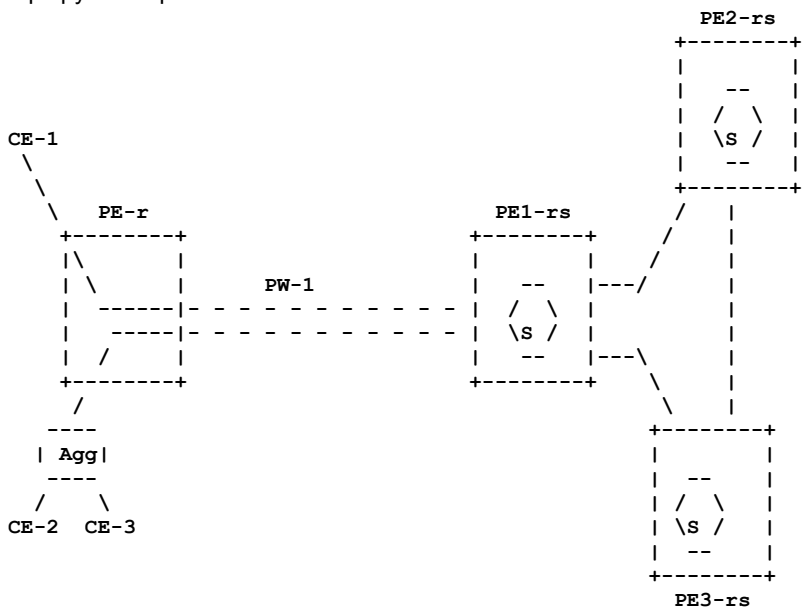


Рисунок 4. Пример иерархической VPLS с лучами без мостов.

PE-r является устройством, поддерживающим маршрутизацию, но не поддерживающим функции моста. Однако оно может создавать PW между собой и PE-rs. Для каждого порта, поддерживаемого в сервисе VPLS, организуется PW от PE-r к PE-rs. После организации PW функции обучения и репликации на PE-r не нужны. Весь трафик, полученный на любом из AC, передаётся в PW. Аналогично, весь трафик, полученный на PW, передаётся в AC, где завершается PW. Таким образом, трафик от CE1, адресованный CE2, коммутируется на PE1-rs, а не на PE-r.

Отметим, что в случае использования устройствами PE-r провайдерских VLAN (P-VLAN[1]) в качестве демультиплексора вместо PW, маршрутизатор PE1-rs может работать с ними и отображать эти «каналы» в домен VPLS для организации функций моста между ними.

Эта модель отличается большими издержками по сравнению с моделью на основе лучей MTU-s, поскольку требуется PW для каждого устройства AC, участвующего в сервисе, в отличие от одного PW на сервис (независимо от числа AC) при использовании MTU-s. Однако этот подход обладает преимуществом за счёт предоставления услуг VPLS вместе с маршрутизируемым сервисом Internet без добавления нового MTU-s.

10.2. Избыточные лучевые соединения

Очевидной слабостью описанной модели «hub and spoke» является то, что MTU-s имеют одно соединение с PE-rs. В случае отказа соединения или PE-rs устройство MTU-s полностью теряет связь с сетью.

В этом параграфе описан способ организации резервных соединений для предотвращения потери связности с MTU-s. Описанный механизм подходит как для MTU-s, так и для PE-r.

10.2.1. Двудомный MTU-s

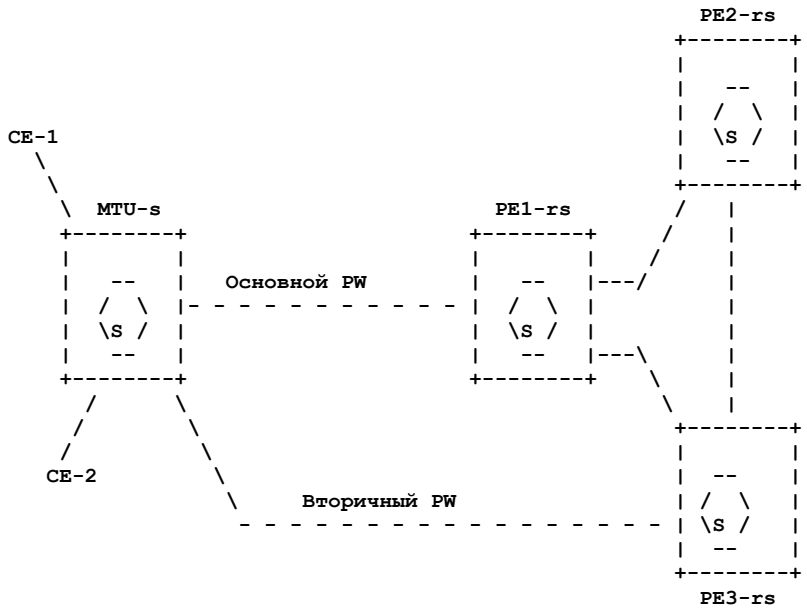


Рисунок 5. Пример двудомного MTU-s.

Для защиты от отказа соединений PW или устройств PE-rs применяются двудомные MTU-s или PE-r с подключением к двум устройствам PE-rs, которые должны относиться к одному экземпляру сервиса VPLS.

[1]Provider VLAN.

На рисунке 5 два абонентских сайта подключены через CE-1 и CE-2 к устройству MTU-s, которое организует до двух PW (один для PE1-rs, другой для PE3-rs) для каждого экземпляра VPLS. Один из двух PW назначается основным и работает в обычных условиях, а другой служит резервным и поддерживается в режиме ожидания (standby). MTU-s согласует метки PW для основного и резервного псевдопровода, но не использует резервный PW до возникновения отказа на основном PW. Выбор первичного и вторичного луча выходит за рамки этой спецификации. Например, одним из вариантов может быть экземпляр STP, работающий между MTU-s и двумя узлами PE-rs. Другие методы требуют настройки.

10.2.2. Обнаружение отказов и восстановление

MTU-s следует контролировать использование лучей к устройствам PE-rs. Если узлами служат PW, для согласования меток PW применяется протокол LDP и сообщения hello, используемые в сессиях LDP, можно применять для детектирования отказа основного PW. Использование других механизмов, способных детектировать отказы быстрее, выходит за рамки этой спецификации.

При отказе основного PW устройство MTU-s незамедлительно переключается на резервный PW. В этот момент PE3-rs, завершающий резервный PW, начинает изучение MAC адресов на лучевом PW. Все другие узлы PE-rs в сети считают, что CE-1 и CE-2 расположены за PE1-rs и могут продолжать передачу трафика PE1-rs, пока не узнают, что эти устройства находятся за PE3-rs. Процесс отмены обучения (unlearning) может занять много времени, что может оказать негативное влияние на связность протоколов верхних уровней с CE1 и CE2. Для более быстрого схождения устройство PE3-rs, где активируется вторичный PW, может передать сообщение для сброса адресов (как описано в параграфе 6.2), используя MAC List TLV (см. раздел 6), всем узлам PE-rs. При получении этого сообщения узлы PE-rs будут сбрасывать MAC-адреса, связанные с этим экземпляром VPLS.

10.3. Многодоменный сервис VPLS

Иерархия может также применяться для организации крупномасштабного сервиса VPLS в одном домене или сервиса, охватывающего множество доменов, без необходимости организации полносвязных соединений между всеми поддерживающими VPLS устройствами. Две полносвязных сети VPLS можно соединить вместе через один туннель LSP между «граничными» устройствами VPLS. Для объединения двух доменов организуется один лучевой PW на сервис VPLS.

Если нужно соединить более двух доменов, между граничными PE организуется полносвязная сеть междоменных лучей. Правила пересылки через эту сеть идентичны правилам, определенным в разделе 4.

Это создаёт трехуровневую иерархическую модель, включающую лучевую (hub-and-spoke) топологию между устройствами MTU-s и PE-rs, полносвязную топологию между PE-rs и полносвязную сеть междоменных лучей между краевыми устройствами PE-rs.

Этот документ не задаёт способов поддержки избыточных граничных PE на уровне домена для каждого сервиса VPLS.

11. Иерархическая модель VPLS с сетями доступа Ethernet

В этом параграфе иерархическая модель расширена для включения сетей доступа Ethernet. Модель сохраняет иерархическую архитектуру, описанную выше, с использованием полносвязных соединений между устройствами PE-rs, однако не задаётся ограничений для сетей доступа Ethernet (например, топология между MTU-s и PE-rs не обязательно «звезда»).

Рассмотрение Ethernet в сетях доступа обусловлено тем, что технология Ethernet сейчас используется многими сервис-провайдерами для предоставления услуг VPLS своим абонентам. Поэтому важно обеспечить механизм, который позволит интегрировать такие сети с ядром IP или MPLS для организации расширяемых услуг VPLS.

Один из подходов к туннелированию абонентского трафика Ethernet через сеть доступа Ethernet заключается в добавлении тега VLAN к абонентским данным (они уже могут иметь свой тег). Дополнительный тег называют P-VLAN. Внутри сети оператора каждая сеть P-VLAN указывает абонента или, более точно, экземпляр VPLS для данного абонента. Поэтому имеется взаимно-однозначное соответствие между P-VLAN и экземпляром VPLS. В этой модели устройства MTU-s должны быть способны добавлять дополнительный тег P-VLAN к немультиплексируемым AC, где абонентские VLAN не служат указателем сервиса. Эта функциональность описана в [802.1ad].

Если абонентские VLAN должны служить указателями сервиса (например, AC является мультиплексируемым портом), устройства MTU-s должны обеспечивать трансляцию абонентских VLAN (C-VLAN[1]) в P-VLAN или вталкивание дополнительного тега P-VLAN для предотвращения проблем, связанных с использованием перекрывающихся VLAN разными абонентами. Поэтому MTU-s в этой модели могут рассматриваться как типичные мосты с поддержкой такой дополнительной возможности. Эта функциональность описана в [802.1ad].

Устройства PE-rs должны быть способны выполнять функции моста через стандартные порты Ethernet в направлении сети доступа, а также через PW в направлении ядра сети. В этой модели для PE-rs может потребоваться запуск протокола STP в направлении сети доступа в дополнение к «расщеплению горизонта» для ядра MPLS. PE-rs должны отображать P-VLAN на экземпляр VPLS и связанные с ним PW (и наоборот).

Детали, относящиеся к операциям моста для MTU-s и PE-rs (например, формат инкапсуляции для сообщений Q-in-Q, обработка протокола управления абонентских сетей Ethernet и т. п.), выходят за рамки этого документа и описаны в [802.1ad]. Тем не менее, важной частью является взаимодействие между модулем моста и псевдопроводами MPLS/IP PW в устройствах PE-rs, которое не отличается от обычного поведения VPLS.

11.1. Расширяемость

Поскольку каждая P-VLAN соответствует экземпляру VPLS, общее число поддерживаемых экземпляров VPLS ограничено значением 4K. P-VLAN служит локальным обозначением сервиса в сети оператора, которое вырезается при отображении на PW в экземпляре VPLS. Поэтому ограничение в 4K применимо лишь в сети доступа Ethernet (остров Ethernet), а не во всей сети. Сеть SP состоит из ядра MPLS/IP, соединяющего множество островов Ethernet.

[1]Customer VLAN.

Поэтому число экземпляров VPLS может расти с ростом числа островов Ethernet (сети доступа в городе могут быть представлены одним или множеством островов).

11.2. Двудомные устройства и восстановление при отказах

В этой модели MTU-s может быть двудомным для различных устройств (агрегаторы и устройства PE-rs). Защита от отказов для узлов доступа в сеть и каналов может быть обеспечена за счёт применения STP на каждом острове. STP каждого из островов не зависит от других островов и не взаимодействует с ними. Если остров имеет более одного PE-rs, между этими PE-rs используется полносвязная сеть PW для передачи пакетов SP BPDU с острова. На уровне P-VLAN протокол STP будет назначать одно устройство PE-rs для передачи трафика через ядро. Защита от петель через ядро выполняется с использованием «расщепления горизонта», а защита от отказов в ядре - с помощью стандартной перемаршрутизации IP/MPLS.

12. Участники работы

Loa Andersson, TLA
Ron Haberman, Alcatel-Lucent
Juha Heinanen, Independent
Giles Heron, Tellabs
Sunil Khandekar, Alcatel-Lucent
Luca Martini, Cisco
Pascal Menezes, Independent
Rob Nath, Alcatel-Lucent
Eric Puetz, AT&T
Vasile Radoaca, Independent
Ali Sajassi, Cisco
Yetik Serbest, AT&T
Nick Slabakov, Juniper
Andrew Smith, Consultant
Tom Soon, AT&T
Nick Tingle, Alcatel-Lucent

13. Благодарности

Спасибо Joe Regan, Kireeti Kompella, Anoop Ghanwani, Joel Halpern, Bill Hong, Rick Wilder, Jim Guichard, Steve Phillips, Norm Finn, Matt Squire, Muneyoshi Suzuki, Waldemar Augustyn, Eric Rosen, Yakov Rekhter, Sasha Vainshtein и Du Wenhua за их полезные замечания.

Спасибо также Rajiv Papneja (ISOCORE), Winston Liu (Ixia) и Charlie Hundall за указание проблем в черновых вариантах, связанных с тестированием взаимодействия.

Спасибо Ina Minei, Bob Thomas, Eric Gray и Dimitri Papadimitriou за техническое рецензирование документа.

14. Вопросы безопасности

Более полное рассмотрение вопросов безопасности, связанных с L2VPN, приведено в [RFC4111]. Незащищённые услуги VPLS имеют некоторые уязвимости, создающие риски для сетей абонентов и провайдеров. Большинства проблем безопасности можно избежать путём реализации соответствующих мер защиты. Некоторые из них можно предотвратить с помощью имеющихся протоколов.

- Уровень данных
  - Изоляция трафика между доменами VPLS гарантируется использованием на уровне VPLS своей таблицы L2 FIB и своих PW.
  - Абонентский трафик, состоящий из кадров Ethernet, передаётся через VPLS без изменений. Если нужна защита, абонентский трафик **следует** шифровать и/или аутентифицировать до отправки в сеть сервис-провайдера.
  - Предотвращение широковещательных штормов может обеспечиваться использованием маршрутизаторов в качестве устройств CPE или правилами для объёма широковещательного трафика от абонента.
- Уровень управления
  - **Следует** применять методы защиты LDP (аутентификация), как описано в [RFC3036]. Это будет предотвращать нарушения работы PE в VPLS с помощью подставных сообщений.
- Атаки на отказ в обслуживании
  - **Следует** реализовать те или иные меры по ограничению числа MAC-адресов (на сайт и VPLS), которым PE может обучиться.

15. Взаимодействие с IANA

Поле типа в MAC List TLV определено со значением 0x404 в параграфе 6.2.1.

16. Литература

16.1. Нормативные документы

[RFC4447] Martini, L., Rosen, E., El-Aawar, N., Smith, T., and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", RFC 4447, April 2006.

[RFC4448] Martini, L., Rosen, E., El-Aawar, N., and G. Heron, "Encapsulation Methods for Transport of Ethernet over MPLS Networks", RFC 4448, April 2006.

[802.1D-ORIG] Original 802.1D - ISO/IEC 10038, ANSI/IEEE Std 802.1D-1993 "MAC Bridges".

[802.1D-REV] 802.1D - "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3: Media Access Control (MAC) Bridges: Revision. This is a revision of ISO/IEC 10038: 1993, 802.1j-1992 and 802.6k-1992. It incorporates P802.11c, P802.1p and P802.12e." ISO/IEC 15802-3: 1998.

[802.1Q] 802.1Q - ANSI/IEEE Draft Standard P802.1Q/D11, "IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks", July 1998.

[RFC3036] Andersson, L., Doolan, P., Feldman, N., Fredette, A., and B. Thomas, "LDP Specification", RFC 3036, January 2001.

[RFC4446] Martini, L., "IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)", BCP 116, RFC 4446, April 2006.

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

16.2. Дополнительная литература

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.

[RADIUS-DISC] Heinanen, J., Weber, G., Ed., Townsley, W., Booth, S., and W. Luo, "Using Radius for PE-Based VPN Discovery", Work in Progress, October 2005.

[BGP-DISC] Ould-Brahim, H., Ed., Rosen, E., Ed., and Y. Rekhter, Ed., "Using BGP as an Auto-Discovery Mechanism for Network-based VPNs", Work in Progress[1], September 2006.

[L2FRAME] Andersson, L. and E. Rosen, "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664, September 2006.

[L2VPN-REQ] Augustyn, W. and Y. Serbest, "Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks", RFC 4665, September 2006.

[RFC4111] Fang, L., "Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)", RFC 4111, July 2005.

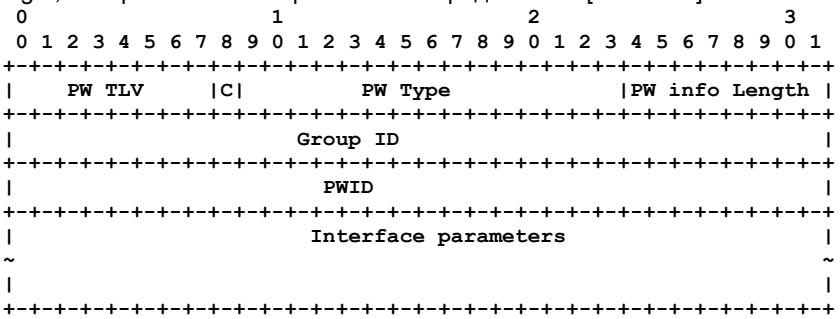
[802.1ad] "IEEE standard for Provider Bridges", Work in Progress[2], December 2002.

Приложение A. Сигнализация VPLS с использованием PWid FEC

Этот раздел был сохранен потому, что остаются реализации, применяющие эту версию сигнализации для VPLS.

Сигнальная информация VPLS передаётся в сообщениях Label Mapping, отправляемых без запроса в нисходящем направлении, и содержащих приведённую ниже структуру PWid FEC TLV.

Поля PW, C, PW Info Length, Group ID и Interface parameters определены в [RFC4447].



Мы используем тип Ethernet PW для указания PW, которые передают трафик при многоточечной связности.

В VPLS мы используем идентификатор PWID (который при использовании обобщённого PWid FEC будет заменяться более обобщённым идентификатором AGI, для расширения области действия VPLS), указывающий сегмент эмулируемой ЛВС. Отметим, что PWID в соответствии с [RFC4447] является идентификатором сервиса, указывающим службу, эмулирующую виртуальный канал «точка-точка». В VPLS идентификатор PWID является единственным указателем сервиса, поэтому он имеет глобальную значимость для всех PE, вовлечённых в экземпляр VPLS[3].

Адреса авторов

Marc Lasserre

Alcatel-Lucent

EMail: mlasserre@alcatel-lucent.com

Vach Kompella

Alcatel-Lucent

[1] Работа опубликована в RFC 5195. *Прим. перев.*
[2] Стандарт принят и включён в IEEE Std 802.1Q-2011.
[3] В оригинале этот абзац содержит ошибки. См. https://www.rfc-editor.org/errata/eid4144. *Прим. перев.*

EMail: vach.kompella@alcatel-lucent.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Copyright (C) The IETF Trust (2007).

К этому документу применимы права, лицензии и ограничения, указанные в BCP 78, и, за исключением указанного там, авторы сохраняют свои права.

Этот документ и содержащаяся в нем информация представлены "как есть" и автор, организация, которую он/она представляет или которая выступает спонсором (если таковой имеется), Internet Society и IETF отказываются от каких-либо гарантий (явных или подразумеваемых), включая (но не ограничиваясь) любые гарантии того, что использование представленной здесь информации не будет нарушать чьих-либо прав, и любые предполагаемые гарантии коммерческого использования или применимости для тех или иных задач.

Интеллектуальная собственность

IETF не принимает какой-либо позиции в отношении действительности или объема каких-либо прав интеллектуальной собственности (Intellectual Property Rights или IPR) или иных прав, которые, как может быть заявлено, относятся к реализации или использованию описанной в этом документе технологии, или степени, в которой любая лицензия, по которой права могут или не могут быть доступны, не заявляется также применение каких-либо усилий для определения таких прав. Сведения о процедурах IETF в отношении прав в документах RFC можно найти в BCP 78 и BCP 79.

Копии раскрытия IPR, предоставленные секретариату IETF, и любые гарантии доступности лицензий, а также результаты попыток получить общую лицензию или право на использование таких прав собственности разработчиками или пользователями этой спецификации, можно получить из сетевого репозитория IETF IPR по ссылке http://www.ietf.org/ipr.

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Информацию следует направлять в IETF по адресу ietf-ipr@ietf.org.

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.