Network Working Group
Request for Comments: 4761
Category: Standards Track

K. Kompella, Ed.
Y. Rekhter, Ed.
Juniper Networks

January 2007

Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling

VPLS с использованием BGP для автоматического обнаружения и сигнализации

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 можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться без ограничений.

Авторские права

Замечание IESG

Рабочая группа L2VPN создала два отдельных документа - RFC 4762 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.

Тезисы

Услуги VPLS[1], называемые также TLS[2] и VPSN[3], являются полезными предложениями сервис-провайдеров (SP[4]). Этот сервис предоставляет виртуальную частную сеть (VPN[5]) L2, однако в случае VPLS пользователи VPN соединяются через «многоточечную» (multipoint) ЛВС Ethernet в отличие от обычных L2 VPN с соединениями «точка-точка».

В этом документе описаны функции, требуемые для организации VPLS, сигнальный механизм VPLS и правила пересылки кадров VPLS через сеть с коммутацией пакетов.

[1]Virtual Private LAN Service - услуги виртуальной частной ЛВС.
[2]Transparent LAN Services - услуги «прозрачной ЛВС».
[3]Virtual Private Switched Network - виртуальная частная коммутируемая сеть.
[4]Service Provider.
[5]Virtual Private Network.

Оглавление

1. Введение

Услуги VPLS, называемые также TLS и VPSN, являются полезными предложениями сервис-провайдеров (SP). Виртуальные частные ЛВС (почти) во всех отношениях проявляются для абонентов SP как обычные Ethernet ЛВС. Однако в VPLS абоненты реально не подключены к одной ЛВС и могут быть соединены через городскую или распределенную сеть. По сути, VPLS «склеивает» отдельные ЛВС через сеть с коммутацией пакетов так, что они представляются и функционируют как единая ЛВС [9]. Это обеспечивается за счет встраивания функций обучения, лавинной рассылки и пересылки кадров в контекст псевдопроводов, соединяющих отдельные ЛВС через сеть с коммутацией пакетов.

В этом документе рассмотрены функции, требуемые для организации сервиса VPLS, и описан механизм автоматического обнаружения конечных точек и сигнализации VPLS. Описана также транспортировка кадров VPLS через туннели в сети пакетной коммутации. Механизм автоматического обнаружения и сигнализации использует BGP в качестве протокола уровня управления. В документе также кратко рассматриваются варианты развертывания, в частности, разделение функций между устройствами.

Другие варианты организации сервиса включают [14], где можно создавать L2 VPN с использованием Ethernet для соединения сетей и [13], где можно организовывать соединения Ethernet через сеть с коммутацией пакетов. Однако оба эти варианта предлагают услуги Ethernet «точка-точка». VPLS отличается от них предоставлением многоточечного обслуживания. Механизм организации псевдопроводов для VPLS с использованием протокола распространения меток LDP[1] определен в [10].

1.1. Область действия документа

Этот документ состоит из 4 основных частей, определяющих функциональную модель VPLS, уровень управления для организации VPLS, уровень данных для VPLS (инкапсуляция и пересылка данных) и варианты развертывания.

Функциональная модель базового сервиса VPLS очерчена в разделе 2. Здесь описаны предлагаемые услуги, компоненты, взаимодействующие для организации сервиса, и верхний уровень таких взаимодействий.

Описываемый в документе уровень управления использует расширение Multiprotocol BGP [4] для организации сервиса VPLS, т. е. автоматического обнаружения членов VPLS, а также организации и разрыва псевдопроводов, создающих данный экземпляр VPLS. Кроме того, в разделе 3 описана организация VPLS через границы автономных систем (AS[2]), а также обслуживание многодомных компонент. Использование BGP для уровня управления VPN не ново (см. [14], [6], [11]) и приведенное здесь описание базируется на механизмах, предложенных в работе [6].

Уровень пересылки и действия краевых маршрутизаторов провайдера (PE[3]), предлагающих услуги VPLS, описаны в разделе 4.

В разделе 5 определено понятие «отвязанной» операции, а также взаимодействия отвязанных и неотвязанных PE. Отвязывание повышает уровень гибкости при развертывании VPLS.

1.2. 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 интерпретируются в соответствии с RFC 2119 [1].

2. Функциональная модель

Описываемая модель графически представлена на рисунке 1.

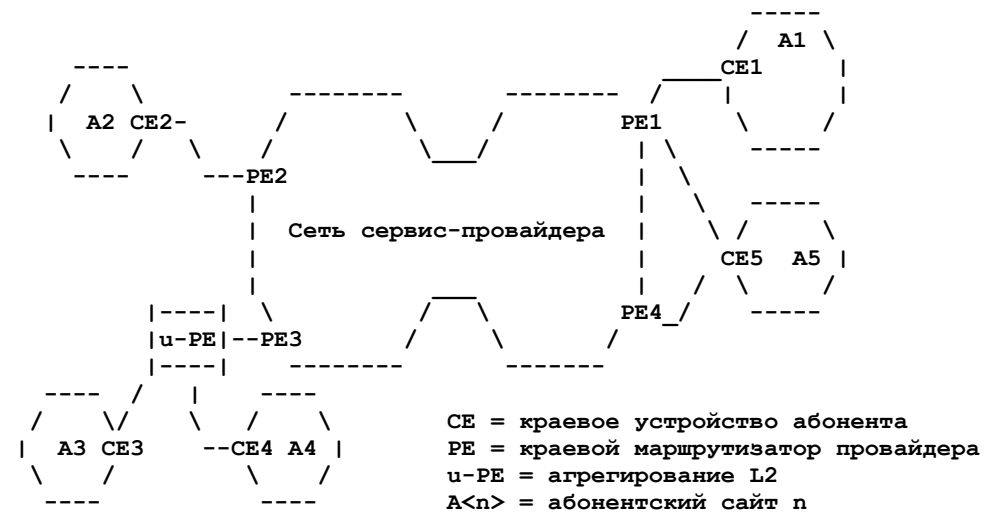

Рисунок 1. Пример VPLS.

[1]Label Distribution Protocol.
[2]Autonomous System.
[3]Provider Edge.

2.1. Терминология

Терминология похожа на используемую в [6] - сеть сервис-провайдера (SP) с внутренними (P[1]) и граничными (PE) маршрутизаторами, а также абонентскими краевыми устройствами (CE[2]). Однако здесь используется дополнительная концепция - u-PE - устройство L2 PE, используемое для агрегирования на канальном уровне (L2), которое описано в разделе 5. Устройства PE и u-PE знают о VPLS (VPLS-aware), т. е. им известно о предлагаемом сервисе VPLS. Термин VE обозначает краевое устройство VPLS, которым может служить PE или u-PE.

Устройства CE (которые могут принадлежать SP или абоненту и управляться им), напротив, ничего не знают о VPLS. CE соединяются с другими CE в рамках VPLS через коммутируемую сеть L2. Это означает, что CE не требуют внесения программных или аппаратных изменений для поддержки VPLS.

Устройство CE может быть соединено с PE или u-PE через коммутаторы L2, которые не знают о VPLS. С точки зрения VPLS такие коммутаторы L2 невидимы и поэтому далее не рассматриваются. Кроме того, u-PE могут подключаться к PE через устройства L2 и L3, как будет описано ниже.

Термин «демультиплексор» обозначает идентификатор в пакете данных, указывающий экземпляр VPLS, к которому относится пакет, а также входной маршрутизатор PE. В этом документе демультиплексором считается метка MPLS.

Термин VPLS обозначает сервис, а также конкретный экземпляр этого сервиса (т. е. эмулируемую ЛВС). Различия определяются контекстом.

2.2. Допущения

Сеть SP представляет собой сеть с коммутацией пакетов. Предполагается полная (логическая) связность между устройствами PE через туннели, в которые инкапсулируются и пересылаются относящиеся к сервису (например, VPLS) пакеты. Это могут быть туннели IP, такие как GRE[3] или туннели MPLS, организованные RSVP-TE[4] или LDP. Эти туннели организуются независимо от услуг, предлагаемых на их основе. Организация туннелей и сигнализация не рассматриваются в документе.

Лавинная рассылка (flooding) и изучение MAC-адресов (learning), рассмотренные в разделе 4, являются частью сервиса VPLS. Однако эти действия являются «частным делом» устройства SP, т. е. в описанном ниже сервисе VPLS ни одно устройство SP не запрашивает у других лавинной рассылки или изучения MAC-адресов от его имени.

Для всех PE, участвующих в сервисе VPLS, предполагается полная связность на уровне данных, т. е. наличие двухстороннего псевдопровода между каждой парой устройств PE, участвующих в сервисе VPLS, когда каждый (входной) маршрутизатор PE может напрямую передать пакет VPLS выходному (выходным) PE без использования промежуточных PE (см. параграф 4.2.5.). Это требует полной логической связности VPLS PE на уровне управления так, что PE может передать другому PE сообщение о необходимости организации между ними псевдопровода. Альтернативные варианты соединений рассмотрены в параграфе 3.6.

2.3. Взаимодействие

VPLS представляет собой «услуги ЛВС», где устройства CE, относящиеся к данному экземпляру VPLS V, могут взаимодействовать через сеть SP, как будто они подключены к единой локальной сети. VPLS является «частной» в том смысле, что устройства CE из разных VPLS не могут взаимодействовать. «Виртуальный» характер VPLS заключается в том, что в одной сети с коммутацией пакетов может одновременно существовать множество VPLS.

Устройства PE взаимодействуют для «обнаружения» всех других PE, участвующих в одном сервисе VPLS, и обмена демультиплексорами. Эти взаимодействия относятся к уровню управления, а не к уровню данных.

Устройства u-PE взаимодействуют с PE для организации соединений с удаленными PE или u-PE в том же сервисе VPLS. Это взаимодействие происходит на уровне управления.

Устройства PE могут одновременно участвовать в VPLS и IP VPN [6]. Это независимые услуги и данные для каждого типа сервиса хранятся раздельно в NLRI[5], имеющих разные идентификаторы семейства адресов (AFI[6]) и последующего семейства адресов (SAFI[7]). Следовательно, реализация **должна** поддерживать свои хранилища маршрутных данных для каждого сервиса. Однако множество экземпляров сервиса может пользоваться одними базовыми туннелями, а для демультиплексирования пакетов разных служб применяются метки VPLS или VPN.

3. Уровень управления

Двумя основными функциями уровня управления VPLS являются автоматическое обнаружение, а также организация и удаление псевдопроводов, составляющих VPLS, часто называемые сигнализацией. Эти функции описаны в параграфах 3.1 и 3.2. Обе эти функции реализуются с помощью одиночных анонсов BGP Update. В параграфе 3.3 более подробно описаны протокольные операции BGP для VPLS. В параграфе 3.4 описана организация псевдопроводов через несколько автономных систем (AS), а в параграфе 3.5 - работа многодомных узлов.

3.1. Автоматическое обнаружение

Обнаружением называют процесс поиска всех PE, участвующих в данном экземпляре VPLS. PE может быть настроен путем указания в конфигурации всех других PE данного экземпляра VPLS или может использовать тот или иной протокол обнаружения других PE. Второй вариант называется автоматическим обнаружением.

В первом варианте требуется большая работа по настройке конфигурации, поскольку для всех PE данного экземпляра VPLS нужна организация полносвязных (full mesh) соединений (т. е. каждый маршрутизатор PE в данном экземпляре

[1]Provider-only - только для провайдера.
[2]Customer Edge.
[3]Generic Routing Encapsulation - базовая инкапсуляция маршрутных данных.
[4]Reservation Protocol - Traffic Engineering - протокол резервирования ресурсов - организация трафика.
[5]Network Layer Reachability Information - информация о доступности на сетевом уровне.
[6]Address Family Identifier.
[7]Subsequent Address Family Identifier.

VPLS должен иметь псевдопровод к каждому другому PE в этом экземпляре). Кроме того, при изменении топологии VPLS (например, при добавлении или удалении PE) конфигурацию VPLS требуется менять на всех PE.

В случае автоматического обнаружения каждый маршрутизатор PE «открывает» для себя другие PE, участвующие в данном экземпляре VPLS с помощью того или иного протокола (в данном случае BGP). Это позволяет ограничиться в настройке каждого PE лишь указанием экземпляра VPLS, организованного на данном PE, без указания всех других PE этого экземпляра, которые будут определены автоматически. Кроме того, при изменении топологии VPLS меняется конфигурация лишь затронутых изменением PE, а остальные автоматически узнают о таком изменении.

3.1.1. Функции

Устройство PE, участвующее в данном экземпляре VPLS V, должно быть способно сказать всем другим PE в VPLS V о своем участии в V. PE должны также иметь способ оповещения остальных о своем выходе из VPLS. Для выполнения этих задач PE требуются способы идентификации VPLS и взаимодействия со всеми остальными PE.

Устройства u-PE также должны знать, из чего состоит данный экземпляр VPLS, однако некоторые детали им не нужны. Устройство (устройства) PE, к которому подключено устройство u-PE, предоставляет u-PE абстракцию VPLS, как описано в разделе 5.

3.1.2. Спецификация протокола

Описанный здесь механизм автоматического обнаружения основан на работах [14] и [6], он использует расширенные группы BGP [5] для идентификации участников VPLS. В частности, используется группа Route Target, формат которой описан в работе [5]. Семантика применения Route Target описана в [6] и используется для VPLS.

Поскольку предполагается полная связность в VPLS, одного Route Target RT достаточно для данной VPLS V и RT фактически служит идентификатором для VPLS V.

PE анонсирует (обычно с помощью I-BGP) свою принадлежность к VPLS V, указывая свои NLRI для V (см. следующий параграф) с Route Target RT и принимает NLRI от других PE, имеющих Route Target RT. PE анонсирует свой выход из V путем отзыва всех NLRI, анонсированных с Route Target RT.

3.2. Сигнализация

После обнаружения каждая пара устройств PE в составе VPLS должна быть способна организовать (и разорвать) между собой псевдопровод, т. е. анонсировать (и отозвать) демультиплексоры. Этот процесс называется сигнализацией. Сигнализация также служит для передачи некоторых характеристик псевдопроводов, которые PE организует для данного экземпляра VPLS.

Напомним, что демультиплексор служит для того, чтобы различать потоки трафика в туннеле, где каждый поток может представлять свой сервис. В случае VPLS демультиплексор не только указывает принадлежность пакета к VPLS, но и задает входное устройство PE. Принадлежность к сервису используется для пересылки пакета, а информация о входном устройстве - для изучения MAC-адресов. Описываемые здесь демультиплексоры являются метками MPLS. Однако следует отметить, что туннели PE-PE могут быть не только туннелями MPLS.

Использование отдельного сообщения BGP Update для отправки демультиплексора каждому удаленному PE потребует от PE передачи N таких сообщений для N удаленных PE. Описанное здесь решение позволяет PE передать одно (общее) сообщение Update, содержащее демультиплексоры для всех удаленных PE, вместо N отдельных сообщений. Это снижает загрузку уровня управления на исходном PE и узлах BGP Route Reflector, которые могут быть вовлечены в распространение сообщения Update другим PE.

3.2.1. Блоки меток

Для решения задачи вводится понятие блока меток, который определяется базой LB[1] и размером VBS VE-блока, представляющего собой множество меток {LB, LB+1, ..., LB+VBS-1}. Рассмотрим работу такого блока. Всем PE в данном экземпляре VPLS в процессе настройки присваиваются уникальные идентификаторы VE ID. Устройство PE X, желающее передать обновление VPLS, отправляет один и тот же блок меток всем остальным PE. Каждое принимающее устройство PE выводит метку, предназначенную для PE X, путем добавления своего (уникального) VE ID к базе меток. Таким способом каждое устройство PE получает уникальный демультиплексор для PE X в данном экземпляре VPLS.

Это простое понятие дополняется концепцией смещения VE-блока VBO. Блок меток, определяемый <LB, VBO, VBS>, представляет собой множество {LB+VBO, LB+VBO+1, ..., LB+VBO+VBS-1}. Т. е. взамен одного большого блока меток, охватывающего все VE ID в VPLS, можно задать несколько блоков, имеющих разные базы. Это упрощает управление блоками и позволяет PE X аккуратно обрабатывать добавление в VPLS устройства PE, идентификатор VE ID которого не охватывается набором блоков меток, уже анонсированных устройством PE X.

При загрузке PE или настройке нового экземпляра VPLS процесс BGP может захотеть дождаться приема нескольких анонсов для данного экземпляра VPLS от других PE для повышения эффективности выделения блоков меток.

3.2.2. VPLS BGP NLRI

Описанные ниже VPLS BGP NLRI с новыми семействами адресов AFI и SAFI (см. [4]) служат для обмена информацией о принадлежности к VPLS и демультиплексорами.

VPLS BGP NLRI включает информационные элементы VE ID, VE Block Offset, VE Block Size и базу меток (LB). Формат VPLS NLRI показан на рисунке 2. AFI представляет собой L2VPN AFI (25), а SAFI - VPLS SAFI (65). Поле Length указывает размер в октетах.

Устройство PE, участвующее в VPLS, должно иметь хотя бы один идентификатор VE ID. Если устройство PE является VE, оно обычно имеет один идентификатор VE ID. Если устройство PE подключено к нескольким u-PE, оно будет иметь свой VE ID для каждого u-PE. Оно может иметь дополнительный идентификатор VE ID для себя при работе в качестве

[1]Label base.

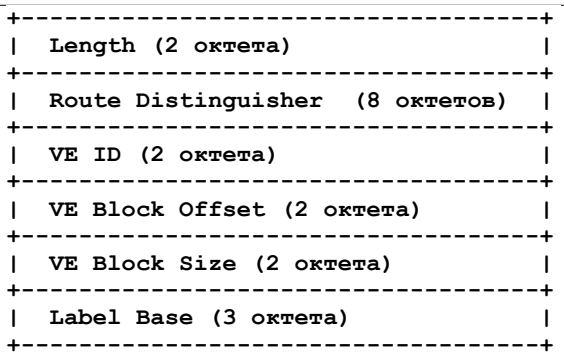

Рисунок 2. BGP NLRI для информации VPLS.

VE в данном экземпляре VPLS. Далее мы будем обозначать устройство PE, анонсирующее VPLS NLRI, как PE-a и считать, что оно владеет VE ID V (относящимся к самому PE-a или к устройству u-PE, подключенному к PE-a).

Идентификаторы VE ID обычно назначаются администратором сети. Их область действия ограничивается экземпляром VPLS. Данный идентификатор VE ID следует относить лишь к одному PE, если устройство CE не является многодомным (см. параграф 3.5).

Блок меток представляет собой набор меток демультиплексирования, используемых для связи с данным VE ID. VPLS BGP NLRI с VE ID V, VE Block Offset VBO, VE Block Size VBS, и базой меток LB сообщает партнерам:

блок меток для V - метки от LB до (LB + VBS - 1);

набор удаленного VE для V - от VBO до (VBO + VBS - 1).

Имеется взаимно-однозначное соответствие между набором удаленного VE и блоком меток - VE ID (VBO + n) соответствует метке (LB + n).

3.2.3. Организация и разрыв PW

Пусть PE-a является частью VPLS foo и делает анонсы с VE ID V, VE Block Offset VBO, VE Block Size VBS и базой меток LB. Если PE-b тоже является частью VPLS и имеет VE ID W, PE-b выполняет перечисленные ниже операции.

1. Проверяется принадлежность W к «набору удаленного VE» устройства PE-a — если VBO <= W < VBO + VBS, W is является частью набора удаленного VE для PE-a. В противном случае PE-b игнорирует это сообщение и пропускает остальную часть этой процедуры.
2. Организуется PW к устройству PE-a. Метка демультиплексора для передачи трафика от PE-b к PE-a рассчитывается как (LB + W - VBO).
3. Проверяется принадлежность V к «набору удаленного VE», анонсируемому PE-b, т. е. PE-b проверяет, относится ли V к тому или иному набору удаленного VE, который анонсирован PE-b (например, VE Block Offset VBO', VE Block Size VBS' и база меток LB'). Если это не так, устройство PE-b **должно** выполнить новый анонс, как описано в параграфе 3.3.
4. Организуется PW от PE-a. Метка демультиплексора с которой PE-b следует ожидать трафик от PE-a, рассчитывается как (LB' + V - VBO').

Если Y отзывает NLRI для V, используемый X, узел X **должен** удалить свое окончание псевдопровода между X и Y.

3.2.4. Сигнальные возможности PE

Описанный ниже расширенный атрибут «Layer2 Info Extended Community» используется для передачи сигнальной информации о псевдопроводах, которые будут организованы для данного экземпляра VPLS. Значения для этого атрибута выделяются IANA (в настоящее время используется значение 0x800A). Эта информация включает Encaps Type (тип инкапсуляции в псевдопроводах), Control Flags (данные управления для псевдопроводов) и MTU[1] для псевдопроводов.

Encaps Type для VPLS имеет значение 19.

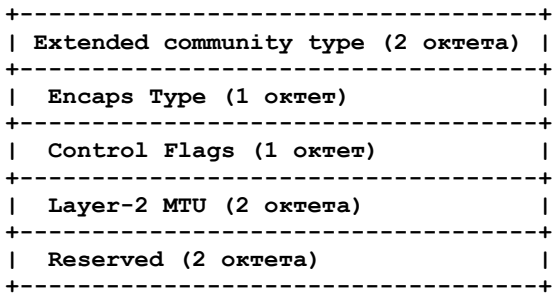

Рисунок 3. Расширенная группа Layer2 Info.

Флаги управления показаны на рисунке 4. Биты поля MBZ **должны** устанавливаться в 0 при передаче, а приемная сторона **должна** игнорировать эти биты.

[1]Maximum Transmission Unit - максимальный передаваемый блок.

```
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|    MBZ      |C|S|       (MBZ = ДОЛЖНО быть 0)
+-+-+-+-+-+-+-+-+
```

Рисунок 4. Вектор флагов управления.

C

При установленном (1) флаге слово управления [7] **должно** присутствовать при передаче пакетов VPLS этому устройству PE, при сброшенном (0) флаге наличие слова управления **недопустимо**.

S

При установленном (1) флаге передача пакетов VPLS этому устройству PE **должна** упорядочиваться, при сброшенном (0) флаге упорядочивание **недопустимо**.

3.3. Работа BGP VPLS

Для создания нового экземпляра VPLS (скажем, VPLS foo) администратор сети должен указать для него RT (например, RT-foo). Это будет использоваться всеми PE для обслуживания VPLS foo. Для настройки данного PE (скажем, PE-a) как участника VPLS foo сетевому администратору нужно лишь выбрать VE ID V для PE-a (если устройство PE-a подключено к u-PE, PE-a может иметь несколько VE ID и указанные ниже действия выполняются для каждого VE ID). Для PE может также указываться обозначение маршрута (RD[1]), если этого не делать, будет автоматически создано уникальное значение RD для VPLS foo. Предположим, что RD имеет значение RD-foo-a. После этого PE-a создает начальный блок меток и набор удаленного VE для V, определяемый VE Block Offset VBO, VE Block Size VBS и базой меток LB. Этот набор может быть пустым.

Затем PE-a создает VPLS BGP NLRI с RD-foo-a, VE ID V, VE Block Offset VBO, VE Block Size VBS и базой меток LB. К нему устройство присоединяет Layer2 Info Extended Community и RT со значением RT-foo. В качестве BGP Next Hop для этого NLRI устройство указывает себя и анонсирует NLRI своим партнерам. Протоколом сетевого уровня, связанным с сетевым адресом Next Hop для комбинации <AFI=L2VPN AFI, SAFI=VPLS SAFI> является IP, эта привязка требуется разделом 5 в [4]. Если поле Length в Next Hop имеет значение 4, Next Hop содержит адрес IPv4, при Length = 16 - адрес IPv6.

Если PE-a получает от другого PE (скажем, PE-b) анонс VPLS BGP с RT-foo и VE ID W, это говорит PE-a, что PE-b участвует с том же экземпляре VPLS (автоматическое обнаружение). Тогда PE-a организует свою часть псевдопровода VPLS между PE-a и PE-b, используя механизм, описанный в параграфе 3.2. Устройство PE-b аналогичным путем определит участие PE-a в том же экземпляре VPLS и должно организовать свою часть псевдопровода VPLS. Таким образом, сигнализация и организация псевдопровода обеспечиваются с помощью одного сообщения Update.

Если W нет ни в одном наборе удаленного VE, анонсированном PE-a для VE ID V в VPLS foo, PE-b не сможет быть частью псевдопровода к PE-a. Для решения этой проблемы PE-a может отозвать прежний анонс(ы) для VPLS foo и передать новое сообщение Update с большим набором удаленного VE и блоком меток, включающим все VE ID для VPLS foo. Однако это может вызвать прерывание обслуживания. Другим вариантом является создание устройством PE-a нового набора удаленного VE с соответствующим блоком меток и его анонс в новом сообщении Update без отзыва прежних анонсов.

Если конфигурация PE-a меняется с удалением VE ID V из VPLS foo, устройство PE-a **должно** отозвать все свои анонсы для VPLS foo, содержащие VE ID V. Если все соединения между PE-a и его устройствами CE в VPLS foo отключены (down), PE-a **следует** отозвать все свои NLRI для VPLS foo или как-то информировать другие PE в VPLS foo о том, что устройство PE-a больше не подключено к своим CE.

3.4. VPLS через множество AS

Как в [14] и [6], описанные выше функции автоматического обнаружения и сигнализации обычно анонсируются через I-BGP. Это предполагает, что все сайты в VPLS подключены к устройствам PE одной автономной системы (AS).

Однако сайты VPLS могут подключаться к PE из разных AS. Это ведет к возникновению двух проблем - (1) между этими PE не будет соединений I-BGP и потребуются другие методы сигнализации через AS, (2) между AS может не быть туннелей PE-PE.

Аналогичная проблема решается в разделе 10 документа [6]. Для решения проблемы (1) предложены 3 метода, каждый из которых имеет аналоги в VPLS через множество AS.

Схема такого сервиса VPLS приведена на рисунке 5.

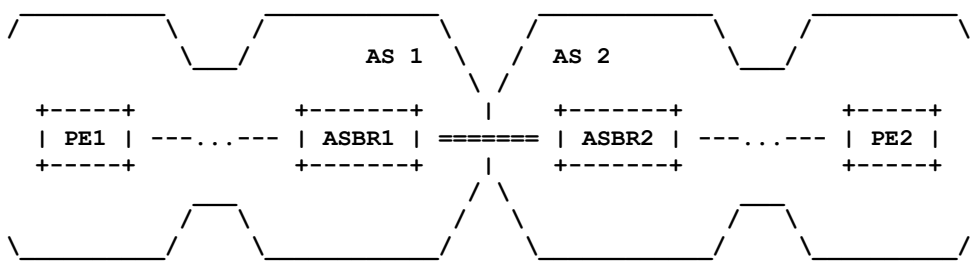

Рисунок 5. VPLS через множество AS.

Как и в упомянутых выше документах, предлагается три метода сигнализации для VPLS через сети нескольких провайдеров. Метод (a) наиболее прост концептуально и в реализации, он требует соединения Ethernet между AS, а также состояний для уровней данных и управления VPLS на граничных маршрутизаторах AS (ASBR[2]). Метод (b) требует состояния уровня управления VPLS на ASBR и MPLS для соединений между AS (это не обязательно Ethernet). Для метода (c) требуется MPLS на соединениях AS-AS, но не нужны состояния VPLS на маршрутизаторах ASBR.

[1]Route Distinguisher.
[2]AS border router.

3.4.1. Метод (a) - соединения VPLS-VPLS на ASBR

В этом методе граничный маршрутизатор ASBR1 служит в качестве PE для всех VPLS в AS1 и AS, к которым ASBR1 подключен (в данном случае AS2). ASBR в соседней AS (ASBR2) представляется ASBR1 устройством CE для VPLS, которые проходят через AS1 и AS2. Маршрутизатор ASBR2 служит PE для этого экземпляра VPLS с точки зрения AS2 и видит ASBR1 как устройство CE.

Этот метод не требует поддержки MPLS на канале ASBR1-ASBR2, но требует передачи через этот канал трафика Ethernet и наличия отдельного субинтерфейса VLAN для каждого сервиса VPLS, проходящего через канал. Кроме того, от ASBR1 требуется выполнение функций PE (обнаружение, сигнализация, изучение MAC-адресов, лавинная рассылка, инкапсуляция и т. п.) для всех VPLS, проходящих через ASBR1. Это создает значительную нагрузку на уровнях управления и данных в ASBR1, что ограничивает число multi-AS VPLS.

Отметим, что в общем случае между парой AS организуется множество соединений для резервирования. В таких случаях должен применяться протокол STP[1] [15] или иные способы обнаружения и предотвращения петель для каждого экземпляра VPLS, проходящего через эти AS, чтобы для каждого экземпляра VPLS могла быть построена топология без петель. Это создает добавочную нагрузку на ASBR и PE, участвующие в таких VPLS, поскольку на устройствах требуется поддерживать алгоритм обнаружения петель для каждого экземпляра VPLS. Решение этого вопроса выходит за рамки документа.

3.4.2. Метод (b) - распространение данных VPLS между ASBR с помощью EBGP

Для этого метода нужно партнерство I-BGP между устройствами PE в AS1 и ASBR1 в AS1 (возможно через рефлектор маршрутов), партнерство E-BGP между ASBR1 и ASBR2 в AS2, а также партнерство I-BGP между ASBR2 и устройствами PE в AS2. В приведенном выше примере PE1 передает маршрутизатору ASBR1 анонс VPLS NLRI с блоком меток, указывая себя в качестве BGP nexthop. ASBR1 передает NLRI маршрутизатору ASBR2 с новым блоком меток и собой в качестве BGP nexthop, а ASBR2 передает NLRI устройству PE2 с новым блоком и собой в качестве nexthop. В результате возникают три туннеля - T1 от PE1 до ASBR1, T2 от ASBR1 до ASBR2 и T3 от ASBR2 до PE2. В каждом туннеле метка VPLS будет использоваться для определения принимающего устройства. Например, меткой VPLS в T1 будет метка из блока, переданного ASBR1 устройству PE1. Маршрутизаторы ASBR отвечают за прием пакетов VPLS, инкапсулированных в туннель и выполнение соответствующих операций замены меток (см. ниже), позволяющих следующему устройству корректно идентифицировать и переслать пакет.

Блок VPLS NLRI, переданный ASBR1 маршрутизатору ASBR2 (и NLRI от ASBR2 к PE2), идентичен VPLS NLRI от PE1 к ASBR1, за исключением блока меток. Точнее, поля Length, Route Distinguisher, VE ID, VE Block Offset и VE Block Size **должны** совпадать, а Label Base могут различаться. Кроме того, маршрутизатор ASBR1 должен также обновить свой путь пересылки, как описано ниже.

Если LB от PE1 имеет значение L1, Label-block Size - N, LB от ASBR1 - L2, а метка туннеля от ASBR1 к PE1 - T, маршрутизатор ASBR1 должен выполнить для своего пути пересылки следующие операции:

поменять L2 на L1 и втолкнуть T;

поменять L2+1 на L1+1 и втолкнуть T;

…;

поменять L2+N-1 на L1+N-1 и втолкнуть T.

Маршрутизатор ASBR2 должен действовать аналогично, но ему может не потребоваться метка туннеля, если он напрямую соединен с ASBR1.

Когда устройство PE2 хочет передать пакет VPLS устройству PE1, оно использует VE ID для получения нужной метки VPLS из блока ASBR2 для PE1 и применяет метку туннеля для доступа к ASBR2. Маршрутизатор ASBR2 меняет метку туннеля VPLS на метку от ASBR1, затем ASBR1 меняет метку туннеля VPLS на метку от PE1 и выталкивает метку туннеля для доступа к PE1.

Для этого метода требуется поддержка MPLS на интерфейсе ASBR1-ASBR2, но не требуется Ethernet на канальном уровне. Кроме того, маршрутизаторы ASBR принимают участие в распространении информации VPLS. Однако требования к уровню данных ASBR значительно проще, чем для метода (a) и ограничиваются операциями с метками. Наконец, формирование беспетлевой топологии VPLS осуществляется на уровне маршрутизации путем выбора BGP path и nexthop, поэтому не нужно поддерживать STP для каждого экземпляра VPLS. В результате этот метод обеспечивает более эффективную расширяемость по сравнению с методом (a).

3.4.3. Метод (c) - распространение данных VPLS с помощью Multi-Hop EBGP

В этом методе используется партнерство multi-hop E-BGP между устройствами PE (или, предпочтительно, Route Reflector) в AS1 устройствами PE (или Route Reflector) в AS2. PE1 передает VPLS NLRI с метками и собой в качестве nexthop устройству PE2. При использовании рефлектора маршрутов BGP nexthop не меняется. Это требует наличия туннеля LSP от PE1 до PE2. Такой туннель можно создать как в разделе 10 (c) документа [6] (например, используя E-BGP для обмена маршрутами с метками для loopback-интерфейсов PE).

Когда PE1 хочет передать пакет VPLS устройству PE2, он вталкивает метку VPLS, соответствующую его VE ID в пакет. Затем он выталкивает метку (метки) туннеля для доступа к PE2.

Этот метод не требует информации VPLS (на уровне данных или управления) на ASBR. Маршрутизаторам ASBR нужно лишь организовать туннели LSP между устройствами PE на уровне управления и выполнять операции с метками на уровне данных. Как и в методе (b), формирование беспетлевой топологии VPLS осуществляется на уровне маршрутизации путем выбора пути BGP и nexthop, поэтому не нужно поддерживать STP для каждого экземпляра VPLS. Этот вариант явно обеспечивает лучшую расширяемость среди всех трех методов, представленных здесь.

[1] Spanning Tree Protocol - протокол связующего дерева.

3.4.4. Назначение VE ID во множестве AS

Чтобы упростить выделение VE ID для VPLS через множество AS, можно задать диапазоны значений для каждой AS. Например, AS1использует VE ID от 1 до 100, AS2 - от 101 до 200 и т. д. При наличии 10 сайтов, подключенных к AS1 и 20 - к AS2, выделенными значениями VE ID могут быть 1-10 и 101 - 120. Это минимизирует число передаваемых VPLS NLRI при обеспечении уникальности VE ID.

Если в приведенном выше примере AS1 требуется больше 100 сайтов, выделенный AS1 диапазон значений будет другим. Единственным предостережением является отсутствие перекрытий между диапазонами VE ID разных AS. Исключением из этого правила являются многодомные подключения, рассматриваемые ниже.

3.5. Многодомные подключения и выбор пути

Зачастую желательно иметь многодомный сайт VPLS, т. е. подключить его ко множеству PE, возможно даже из разных AS. В таких случаях для PE, подключенных к одному сайту, можно задать одно или разные значения VE ID. В последнем случае обязательно использовать протокол STP на устройстве CE, а возможно и на устройствах PE для создания топологии VPLS без петель. Способы реализации этого выходят за рамки документа, однако в остальной части этого параграфа более подробно рассматривается первый вариант. Отметим, что многодомное подключение к SP и протокол STP на устройствах CE могут применяться совместно. Пользователям VPLS рекомендуется применять STP, если устройства CE поддерживают протокол.

Если устройствам PE, подключенным к одному сайту, назначается одинаковый идентификатор VE ID, беспетлевая топология формируется механизмами маршрутизации, в частности, выбором пути BGP. Когда узел BGP получает два эквивалентных NLRI (см. ниже), он применяет стандартные критерии выбора пути (такие, как Local Preference и AS Path Length) для определения нужного NLRI (узел **должен** выбрать один). Если выбранный блок NLRI позднее отзывается, узел BGP применяет механизм выбора пути к оставшимся эквивалентным VPLS NLRI для выбора другого. Если таких NLRI больше нет, связанная с ними информация о пересылке удаляется.

Два VPLS NLRI считаются эквивалентными с точки зрения выбора пути, если значения Route Distinguisher, VE ID и VE Block Offset у них совпадают. Если двум PE выделено одно значение VE ID в данном экземпляре VPLS, они **должны** использовать одинаковое значение Route Distinguisher, а также им **следует** анонсировать один VE Block Size для данного VE Offset.

3.6. Иерархические BGP VPLS

В этом параграфе описано, как можно расширить уровень управления VPLS при использовании BGP. Имеется по меньшей мере три аспекта расширяемости уровня управления.

1. Уход от требования полносвязных (full mesh) соединений между всеми узлами VPLS BGP.
2. Ограничение числа сообщений BGP VPLS за счет их передачи лишь заинтересованным узлам BGP.
3. Упрощение процедур добавления и удаления узлов BGP для VPLS или других приложений.

К счастью, применение BGP для маршрутизации Internet и IP VPN дало несколько хороших решений для этих проблем. Основным вариантом является использование иерархии на основе рефлекторов маршрутов BGP RR[1] [8]. Идея заключается в назначении небольшого набора рефлекторов маршрутов, а затем организации сессий BGP между каждым узлом BGP и одним или множеством RR. В этом случае не требуется организации полносвязных соединений между всеми узлами BGP. Если для конкретного провайдера требуется большое число RR, этот метод можно использовать рекурсивно, заменяя полносвязные соединения между всеми RR их соединениями с RR другого уровня. Применение RR решает проблемы 1 и 3.

Важно подчеркнуть, что применение RR для VPLS и VPN полностью относится к уровню управления. RR не создает состояний и требований к пересылке на уровне данных, а также не меняет путей пересылки трафика VPLS. Это отличается от модели иерархического сервиса VPLS, определенной в [10].

Другим следствием такого подхода является отсутствие требования обработки одним набором RR всех сообщений BGP или обработки отдельным RR всех сообщений от данного PE. Можно определить несколько наборов RR, например, один для обработки VPLS, другой для IP VPN, а третий для маршрутизации Internet. Возможно другое разделение, когда то или иное подмножество VPLS и IP VPN обрабатывается одним набором RR, а второе подмножество - другим. Использование фильтрации целей маршрутов (RTF[2]), описанной в [12], позволяет сделать это более просто и эффективно.

Проблема 2 (передача сообщений BGP VPLS лишь заинтересованным узлам BGP) решается с помощью RTF. Этот метод «ортогонален» использованию RR, но они хорошо работают вместе. Фильтрация RTF также очень эффективна для VPLS через множество AS. Подробности и преимущества использования RTF описаны в [12]. Следует также упомянуть один аспект уровня управления, с которым часто возникает путаница. Обмен MAC-адресами не выполняется по протоколу BGP. Все операции изучения и старения MAC-адресов выполняются на уровне данных отдельно для каждого PE. Единственной задачей сообщений BGP VPLS является автоматическое обнаружение и обмен метками.

Таким образом, обработка BGP для VPLS возникает

1. при добавлении или удалении PE из VPLS;
2. при отказе в сети, отключающем (down) туннель PE-PE или канал PE-CE.

Такие события сравнительно редки и обычно вызывают генерацию сообщения BGP Update. В сочетании с эффективностью обмена сообщениями BGP для сигнализации VPLS это показывает, что применение BGP в качестве уровня управления для VPLS обеспечивает достаточно хорошую расширяемость в плане обработки и требований к памяти.

[1]Route Reflector.
[2]Route Target Filtering.

4. Уровень данных

В этом разделе описаны два аспекта уровня данных для устройств PE и u-PE, участвующих в VPLS, - инкапсуляция и пересылка.

4.1. Инкапсуляция

Кадры Ethernet, полученные от устройств CE, инкапсулируются для передачи через сеть с коммутацией пакетов, к которой подключены PE. Инкапсуляция выполняется в соответствии с [7].

4.2. Пересылка

Пакеты VPLS классифицируются как относящиеся к данному экземпляру сервиса и связанной с ним таблице пересылки в соответствии с принявшим пакет интерфейсом. Пакеты пересылаются в контексте экземпляра сервиса по MAC-адресу получателя. Первая операция определяется настройками, вторая рассматривается ниже.

4.2.1. Изучение MAC-адресов

Как было отмечено выше, ключевым отличием VPLS является поддержка многоточечного сервиса. Это означает, что всей сети сервис-провайдера следует быть одним логическим обучающимся мостом для каждого сервиса VPLS, поддерживаемого в сети SP. Логическими портами «моста» SP являются абонентские порты, а также псевдопровода на VE. Как обычный обучаемый мост изучает MAC-адреса на своих портах, так и мост SP должен изучать MAC-адреса на своих VE.

Обучение заключается в связывании MAC-адресов отправителей пакетов с (логическими) портами, через которые пакеты приходят. Эта привязка создает таблицу FIB[1], используемую для пересылки пакетов. Предположим, например, что мост получает пакет с MAC-адресом отправителя S на (логическом) порту P. Если после этого мост получит пакет с MAC-адресом получателя S, он будет знать, что пакет нужно передать через порт P.

Если VE узнает MAC-адрес отправителя S на логическом порту P, а затем видит S на другом порту P', устройство VE **должно** обновить свою таблицу FIB, указав в ней новый порт P'. VE **может** реализовать механизм демпфирования смены (flapping) портов-источников для данного MAC-адреса.

4.2.2. Старение

Устройствам VPLS PE **следует** поддерживать механизм старения, чтобы удалять связанный с портом MAC-адрес, как это делают обучающиеся мосты. Это нужно для того, чтобы MAC-адрес был «переучен» (relearn), если он «переходит» с одного логического порта на другой в результате физического перемещения владеющей адресом станции на другой порт или в результате изменения топологии ЛВС, меняющего пути пакетов. Кроме того, старение снижает размер таблицы VPLS MAC, сохраняя в ней лишь активные, а не все MAC-адреса в данном экземпляре VPLS.

«Возрастом» MAC-адреса S на логическом порту P считается время с момента, когда он последний раз наблюдался в качестве MAC-адреса отправителя на порту P. Если возраст превышает время старения T, запись для S **должна** быть удалена из FIB. При каждом появлении S в качестве MAC-адреса отправителя на порту P возраст S сбрасывается (0).

Реализации **следует** предоставлять средство настройки времени старения T на уровне VPLS. В дополнение к этому реализация **может** ускорять старение всех MAC в VPLS для некоторых ситуаций (например, при изменении топологии STP в данном экземпляре VPLS).

4.2.3. Лавинная рассылка

Когда мост получает пакет, для которого адрес получателя отсутствует в FIB, такой пакет пересылается во все остальные порты. Аналогично, VE будет применять лавинную рассылку пакетов для неизвестных получателей всем другим VE в VPLS.

В примере на рисунке 1 устройство PE2 будет отвечать за лавинную рассылку кадра всем другим PE в том же экземпляре VPLS, если CE2 передаст PE2 кадр Ethernet с отсутствующим в таблице FIB устройства PE2 (для данного экземпляра VPLS) адресом получателя. При получении такого кадра PE1 будет отвечать за дальнейшую лавинную рассылку кадра устройствам CE1 и CE5 (если PE1 не знает, какое из устройств CE «владеет» этим MAC-адресом).

С другой стороны, если устройство PE3 получает кадр, оно будет поручать лавинную рассылку своему u-PE. Если устройство PE3 подключено к двум u-PE, оно будет анонсировать наличие двух u-PE. PE3 может анонсировать неспособность к лавинной рассылке и в этом случае будет получать 2 кадра (по одному для каждого u-PE) или указать возможность лавинной рассылки, получая при этом один экземпляр кадра, который будет пересылаться обоим u-PE.

4.2.4. Широковещательные и групповые кадры

Имеются общеизвестные широковещательные MAC-адреса. Кадр Ethernet с широковещательным MAC-адресом получателя должен передаваться всем станциям данного экземпляра VPLS. Это может быть реализовано так же, как выполняется лавинная рассылка.

Имеется также легко распознаваемое множество групповых (multicast) MAC-адресов. Кадры Ethernet с групповым MAC-адресом получателя **могут** передаваться широковещательно всем станциям. VE **может** также применять те или иные методы ограничения групповой пересылки меньшим множеством получателей, которые указали заинтересованность в соответствующей multicast-группе. Рассмотрение этого вопроса выходит за рамки документа.

4.2.5. Пересылка с «расщепленным горизонтом»

Когда поддерживающее лавинную рассылку устройство PE (скажем, PEx) получает широковещательный кадр Ethernet или кадр с неизвестным MAC-адресом получателя, оно должно применять лавинную рассылку для этого кадра. Если кадр принят от подключенного CE, устройство PEx должно передать копию кадра всем другим подключенным CE, а также устройствам PE, участвующим в VPLS. Если же кадр приходит от другого PE (например, PEy), устройство PEx

[1]Forwarding Information Base - база информации для пересылки кадров.

должно передать копию пакета лишь подключенным CE. PEx **недопустимо** передавать такой кадр другим PE, поскольку устройство PEy уже сделало это. Это называют пересылкой с «расщепленным горизонтом» и такая является следствием наличия полной связности между PE в рамках VPLS.

Правила пересылки с расщепленным горизонтом применяются для широковещательных и групповых пакетов, а также пакетов с неизвестным MAC-адресом получателя.

4.2.6. Квалифицированное и неквалифицированное обучение

Ключом для нормального обучения Ethernet MAC обычно служат (6-октетные) MAC-адреса. Это называется неквалифицированным обучением. Однако возможно включение в процесс имеющихся в кадрах тегов VLAN и тогда это называется квалифицированным обучением.

В случае VPLS обучение выполняется в контексте экземпляра VPLS, который обычно соответствует одному абоненту. Если абонент применяет теги VLAN, он может разделять квалифицированное и неквалифицированное обучение. Если ключом при обучении в VPLS является лишь MAC-адрес, VPLS будет работать в режиме неквалифицированного обучения. Если ключом служит абонентский тег VLAN и MAC-адрес, VPLS использует квалифицированное обучение.

Выбор типа обучения включает несколько факторов, из которых наиболее важным является наличие одного или множества (по VLAN) доменов широковещания. Во втором варианте эффективность лавинной рассылки и широковещания повышается, но растет и размер таблиц MAC. Это применимо как к обычной пересылке Ethernet, так и к VPLS.

4.2.7. Класс обслуживания

Для поддержки разных классов обслуживания в рамках VPLS реализация может сопоставлять биты 802.1p в абонентских кадрах Ethernet с тегами VLAN с битами EXP в псевдопроводе и/или метке туннеля, что позволяет по-разному обрабатывать кадры VPLS в сети с коммутацией пакетов.

Чтобы такое сопоставление было полезно, реализации **следует** разрешать свое отображение для каждого экземпляра VPLS, поскольку каждый абонент VPLS может иметь свое представление об установке поведения битов 802.1p.

5. Варианты развертывания

При развертывании сети с поддержкой VPLS оператор должен решить, какие функции будут обеспечивать устройства с поддержкой VPLS, расположенные близко к абонентам (VE). Используемый по умолчанию случай, описанный в этом документе, предполагает применение в качестве VE маршрутизаторов PE. Однако имеется много причин, по которым VE может быть устройством, выполняющим все функции L2 (такие как изучение MAC-адресов и лавинная рассылка), а также ограниченный набор функций L3 (такие, как взаимодействие со своим PE), но не поддерживающим, например, полноценного обнаружения и сигнализации PE-PE. Такие устройства называются u-PE.

Поскольку у обоих вариантов есть свои преимущества, хотелось бы иметь возможность их совместного применения. Представленные здесь механизмы сигнализации позволяют это. Например, в данной сети оператора одно устройство PE может напрямую подключаться к CE, другое - к устройствам u-PE, соединенным с устройствами CE, а третье может подключаться напрямую к абонентам через те или иные интерфейсы и к устройствам u-PE - через другие. Все эти PE будут одинаково выполнять обнаружение и сигнализацию. Функции обучения и пересылки зависят от того, является ли устройство u-PE, однако это локальный вопрос, не связанный с сигнализацией. Детали работы u-PE и их взаимодействия с устройствами PE и другими u-PE выходят за рамки этого документа.

6. Вопросы безопасности

Основное внимание в VPLS уделяется приватности данных, т. е. данные в VPLS распространяются только узлам данного экземпляра VPLS и недоступны каким-либо внешним агентам или другим VPLS. Отметим, что сервис VPLS не предоставляет защиты конфиденциальности, целостности и проверки подлинности. Пакеты VPLS передаются в сеть пакетной коммутации в открытом виде и злоумышленник на пути передачи[1] может перехватывать пакет, а в некоторых случаях имеет возможность помещать свои пакеты в поток данных. Если требуется защита, в качестве туннелей PE-PE могут служить туннели IPsec. Для дополнительной защиты оконечные системы на сайтах VPLS могут использовать подходящее шифрование пакетов до их отправки в сеть сервис-провайдера.

Имеется два аспекта, связанных с приватностью в VPLS - безопасность уровня управления и защита пути пересылки. Компрометация уровня управления может приводить к передаче устройством PE данных, относящихся к одному экземпляру VPLS, в другой, созданию «черной дыры» для данных VPLS или даже отправки их перехватывающему устройству. Ни одно из таких событий не приемлемо с точки зрения приватности. Поскольку весь обмен на уровне управления осуществляется по протоколу BGP, методы, описанные в [2], могут помочь при проверке подлинности сообщений BGP, осложняя подмену обновлений (которые могут использоваться для направления трафика VPLS другому экземпляру VPLS) или отзыв данных (атаки на отказ в обслуживании). В методах (b) и (c) для работы через множество AS, описанных в разделе 3, это обеспечивает защиту сеансов BGP между AS, а также между устройствами ASBR, PE и рефлекторами маршрутов. Можно также применять методы, описанные в разделе 10 (b) и (c) документа [6], как для уровня управления, так и для уровня данных. Отметим, что методы [2] не помогут сохранить приватность меток VPLS, а зная эти метки, можно перехватить трафик VPLS. Однако для этого нужен доступ к путям данных в сети SP.

Возможны ошибочные конфигурации, ведущие к непреднамеренным подключениям устройств CE не к тем VPLS. Это может быть вызвано, например, некорректным Route Target для экземпляра VPLS. Эта проблема, как отмечено в [6], требует дополнительного исследования.

Для защиты уровня данных нужно обеспечить корректное поведение туннелей PE-PE (это выходит за рамки документа) и восприятие меток VPLS только от разрешенных интерфейсов. Для PE такими интерфейсами будут каналы к маршрутизаторам P, для ASBR - канал от маршрутизатора ASBR в AS, являющуюся частью данного экземпляра VPLS. При организации VPLS через множество AS особенно важно восприятие пакетов VPLS VPLS лишь от разрешенных интерфейсов.

[1]Man-in-the-middle - человек посередине.

В документе [3] описано туннелирование MPLS-in-IP и MPLS-in-GRE. Если желательно применение таких туннелей для транспортировки пакетов VPLS, нужно разобраться с вопросами безопасности, отмеченными в разделе 8 упомянутого документа. Любая реализация VPLS, которая позволяет туннелировать пакеты VPLS в соответствии с указанным документом, **должна** включать поддержку IPsec, которую можно использовать, как описано здесь. Если туннель не защищен с помощью IPsec, описанная в параграфе 8.2 этого документа фильтрация по адресам IP на граничных маршрутизаторах, будет единственным способом обеспечить на выходе из туннеля в конкретное устройство PE присутствие пакетов только от разрешенных входных точек туннелей (т. е. отсечь пакеты с подставным адресом отправителя). Поскольку граничные маршрутизаторы зачастую фильтруют лишь по адресам отправителей, фильтрация пакетов может оказаться неэффективной, если выходной PE не может проверить IP-адрес отправителя во всех принимаемых пакетах и сравнить его со списком IP-адресов разрешенных начальных точек туннелей. Любая реализация, разрешающая применять инкапсуляцию MPLS-in-IP или MPLS-in-GRE без защиты IPsec, **должна** позволять выходному PE такую проверку по IP-адресам для всех полученных туннелированных пакетов.

7. Взаимодействие с IANA

Агентство IANA выделило значение AFI 25 для информации L2VPN. Это значение совпадает с AFI, запрошенным в [11].

Агентство IANA выделило значение 0x800a для Layer2 Info Extended Community.

8. Литература

8.1. Нормативные документы

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

[2] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.

[3] Worster, T., Rekhter, Y., and E. Rosen, "Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)", RFC 4023, March 2005.

[4] Bates, T., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, January 2007.

[5] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, February 2006.

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

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

8.2. Дополнительная литература

[8] Bates, T., Chen, E., and R. Chandra, "BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)", RFC 4456, April 2006.

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

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

[11] Ould-Brahim, H., "Using BGP as an Auto-Discovery Mechanism for VR-based Layer-3 VPNs", Work in Progress, April 2006.

[12] Marques, P., "Constrained VPN Route Distribution", Work in Progress, June 2005.

[13] 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.

[14] Kompella, K., "Layer 2 VPNs Over Tunnels", Work in Progress, January 2006.

[15] Institute of Electrical and Electronics Engineers, "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.", IEEE Standard 802.1D, July 1998.

Приложение A. Участники работы

Ниже перечислены участники работы над документом.

Javier Achirica, Telefonica
Loa Andersson, Acreo
Giles Heron, Tellabs
Sunil Khandekar, Alcatel-Lucent
Chaitanya Kodeboyina, Nuova Systems
Vach Kompella, Alcatel-Lucent
Marc Lasserre, Alcatel-Lucent
Pierre Lin
Pascal Menezes
Ashwin Moranganti, Appian
Hamid Ould-Brahim, Nortel
Seo Yeong-il, Korea Tel

Приложение B. Благодарности

Спасибо Joe Regan и Alfred Nothaft за их вклад в работу. Большое спасибо Eric Ji, Chaitanya Kodeboyina, Mike Loomis и Elwyn Davies за подробные рецензии.

Адреса редакторов

Kireeti Kompella

Juniper Networks

1194 N. Mathilda Ave.

Sunnyvale, CA 94089

US

EMail: kireeti@juniper.net

Yakov Rekhter

Juniper Networks

1194 N. Mathilda Ave.

Sunnyvale, CA 94089

US

EMail: yakov@juniper.net

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru

Полное заявление авторских прав

Интеллектуальная собственность

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.