Network Working Group
Request for Comments: 5251
Category: Standards Track

D. Fedyk, Ed.
Nortel
Y. Rekhter, Ed.
Juniper Networks
D. Papadimitriou
Alcatel-Lucent
R. Rabbat
Google
L. Berger
LabN

July 2008

Базовый режим VPN уровня 1

Layer 1 VPN Basic Mode

Статус документа

В этом документе описан проект стандартного протокола Internet, предложенного сообществу Internet, документ служит приглашением к дискуссии в целях развития предложенного протокола. Текущее состояние стандартизации протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться свободно.

Тезисы

В этом документе описан базовый режим VPN уровня 1 (L1VPN[1]). Базовый режим L1VPN (L1VPN BM[2]) представляет собой виртуальные частные сети (VPN) на основе портов. В L1VPN базовым элементом сервиса является путь с коммутацией по меткам (LSP[3]) между парой пользовательских портов с данной топологией портов VPN. В этом документе определена рабочая модель, использующая механизм предоставления или автоматического обнаружения VPN, а также сигнальные расширения для L1VPN BM.

Содержание

1. Введение

В этом документе описан базовый режим VPN уровня 1 (L1VPN BM), кратко очерченный в [RFC4847]. Вопросы применимости VPN уровня 1 рассмотрены в [RFC5253]. В этом документе рассматривается сеть сервис-провайдера уровня 1[4], которая состоит из устройств, поддерживающих GMPLS (например, устройств LSC[5], оптических кросс-

[1]Layer 1 VPN.
[2]L1VPN Basic Mode.
[3]Label Switched Path.
[4] Физический уровень модели OSI. *Прим. перев.*
[5] Lambda Switch Capable - коммутация длин волн (лямбда).

коннекторов, кросс-коннекторов SONET/SDH[1] и т. п.). Эти устройства будем делить на провайдерские (P) и краевые (PE[2]). В контексте этого документа будем просто обозначать устройства первого типа P, а второго - PE. Устройства P подключаются только к внутренним устройствам сети провайдера. Устройства PE подключаются к другим устройствам (P или PE) в сети провайдера, а также к внешним по отношению к этой сети устройствам. Будем называть такие устройства пользовательскими (CE[3]). Примером CE могут быть поддерживающие GMPLS устройства типа маршрутизаторов, кросс-коннекторов SDH или коммутаторов Ethernet.

[RFC4208] определяет сигнализацию от CE к PE. Используемый в [RFC4208] термин CN[4] соответствует узлам P и PE, а EN[5] - узлам CE. Здесь дополнительно определяется термин "edge Core Node[6]", соответствующий устройствам PE.

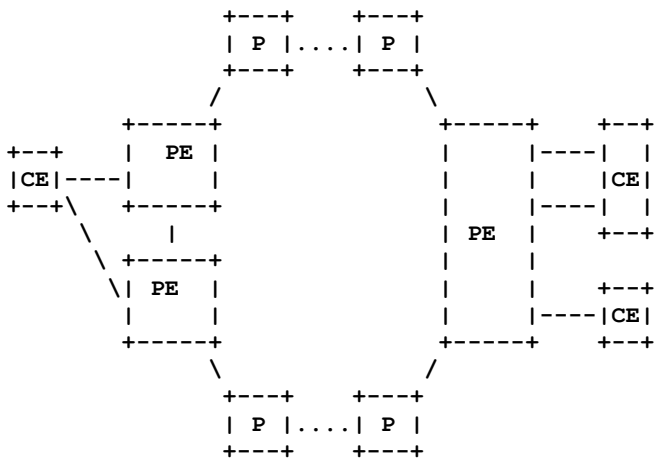

Рисунок 1. Централизованная модель L1VPN.

На рисунке 1 показаны компоненты сети L1VPN.

В этом документе описано как сервис L1VPN BM может быть реализован с использованием предоставления[7] или автоматического детектирования VPN, механизмов сигнализации [RFC3471, RFC3473], маршрутизации [RFC4202] и LMP[8] [RFC4204] протокола GMPLS[9].
Требования к автоматическому детектированию L1VPN [RFC4847] подобны требованиям к автоматическому детектированию L3VPN. Как и в L3VPN возможен выбор протокола, используемого для автоматического детектирования. В параграфе 4.1.1 рассматривается информация, которую нужно детектировать.
Маршрутизация и сигнализация GMPLS без расширений используются в сети провайдера для организации и поддержки соединений LSC или SONET/SDH TDM между узлами провайдера. Это соответствует модели [RFC4208].

В базовом режиме L1VPN LMP упрощает заполнение таблиц PIT[10] сервис-провайдера. Вместо этого LMP **может** использоваться как опция для автоматизации локального обнаружения каналов от CE к PE. LMP также **может** расширять возможности маршрутизации (в расширенном режиме), а также средства обработки отказов.

Организация L1VPN между разными провайдерами или автономными системами требует дополнительного анализа.

1.1. Используемые в документе соглашения

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

В документе предполагается, что читатель знаком с терминами, определенными и используемыми в [RFC3945], [RFC3471], [RFC3473], [RFC3477], [RFC4201], [RFC4202], [RFC4204], [RFC4208] и документах, на которые те ссылаются.

2. Сервис Layer 1 VPN

Услуги VPN уровня 1 на пользовательских и провайдерских портах **могут** предоставляться на любых интерфейсах уровня 1, поддерживаемых GMPLS. Поскольку предлагаемые в этом документе механизмы используют для сигнализации GMPLS, а GMPLS работает для интерфейсов SONET/SDH (TDM[11]) и LSC, услуги L1VPN предоставляются оборудованию, работающему на основе LSC или TDM (но не ограничиваются только этими типами оборудования). Отметим, что в этом документе описаны L1VPN базового типа, что обуславливает два требования:

(1) GMPLS RSVP-TE используется для сигнализации в сети провайдера (между PE), а также между оборудованием провайдера и пользовательским оборудованием (между CE и PE);

(2) маршрутизация GMPLS на канале от CE к PE выходит за пределы базового режима работы L1VPN (см. [RFC4847]).

[1] Synchronous Optical Network/Synchronous Digital Hierarchy.
[2] Provider edge.
[3] Customer Edge device - пользовательское краевое устройство.
[4] Core Node - центральный узел.
[5] Edge Node - краевой узел.
[6] Краевой центральный узел.
[7] В оригинале «off-line provisioning». *Прим. перев.*
[8] Link Management Protocol - протокол управления каналом.
[9] Generalized Multi-Protocol Label Switching - обобщенная многопротокольная коммутация меток.
[10] Port Information Table - таблица информации порта.
[11] Time Division Multiplexing - мультиплексирование с разделением по времени. *Прим. перев.*

Устройства CE соединяются с PE через один или множество каналов. В контексте этого документа канал представляет собой конструкцию GMPLS TE[1], определенную в [RFC4202]. В контексте этого документа канал TE представляет собой логическую конструкцию, являющуюся частью VPN, и обеспечивает возможность представления множества устройств CE, образующих VPN. Интерфейсы на конце каждого канала относятся к типам TDM или LSC, поддерживаемым GMPLS. Говоря точнее, канал <CE, PE> **должен** относиться к типу <X, LSC> или <Y, TDM>, где X представляет собой PSC[2], L2SC[3] или TDM, Y представляет собой PSC или L2SC. В случаях, когда LSP не завершается устройством CE, X **может** также представлять собой устройство LSC, а Y - устройство TDM. Одним из применений L1VPN является предоставления услуг virtual private lambda[4] или подобных им. В таких случаях CE является истинно конечной точкой в терминах GMPLS, и возможности коммутации на канале TE не имеют отношения к делу (хотя его идентификатор GPID[5] **должен** использоваться для сигнализации и совпадать на обоих CE[6]).

Подобно этому, PE могут представлять собой любые устройства уровня 1, поддерживаемые GMPLS (например, оптические кросс-коннекторы, кросс-коннекторы SDH), тогда как CE **могут** быть устройствами уровня 1, 2 или 3 (например, кросс-коннекторами SDH, коммутаторами Ethernet или маршрутизаторами, соответственно).

Каждое соединение TE **может** состоять из одного или множества каналов или субканалов (например, длина волны или длина волны и временной интервал[7], соответственно). В рамках нашего обсуждения все каналы в данном соединении **должны** иметь похожие разделяемые параметры (например, возможности коммутации[8], кодирование, тип и т. п.) и **могут** выбираться независимо с точки зрения CE. Для каналов на разных соединениях CE одинаковые характеристики не требуются.

Для данной пары CE-PE **может** существовать более одного соединения TE. Устройство CE **может** быть подключено к нескольким PE (по крайней мере через один порт на каждом PE). И, наоборот, PE **может** иметь более одного подключенного CE из различных VPN.

Если CE соединен с PE множеством каналов TE, относящихся к одной VPN, эти каналы (их называют компонетами) **можно** рассматривать как один канал TE, используя конструкции связок (bundling) [RFC4201].

Для выполнения требований базового режима L1VPN **требуется**, чтобы для данной пары CE-PE хотя бы один канал между ними имел по крайней мере один опорный (bearing) канал и по крайней мере один управляющий опорный канал или присутствовала IP-связность между CE и PE, которую можно использовать для обмена управляющей информацией.

Канал point-to-point имеет две конечных точки - CE и PE. В этом документе первая называется портом CE, вторая - портом PE. Из сказанного выше следует, что CE соединен с PE через один или множество портов и каждый порт **может** состоять из одного или множества каналов или субканалов (например, длина волны или длина волны и временной интервал), все каналы данного порта имеют похожие характеристики и могут быть поменяны местами с точки зрения CE. По аналогии с определением канала TE,порты в контексте этого документа являются логическими конструкциями, которые служат для представления групп физических ресурсов, используемых для подключения CE к PE на основе L1VPN.

В любой заданный момент данный порт PE связан не более, чем с одной L1VPN, точнее не более, чем с одной таблицей информации порта (Port Information Table), поддерживаемой PE (хотя разные порты в данном PE могут быть связаны с разными L1VPN или, точнее, с разными таблицами информации портов). Связь порта с VPN **может** определяться путем организации взаимосвязей на устройствах сервис-провайдера. Иными словами, контекст принадлежности к VPN в базовом режиме находится под управлением сервис-провайдера.

Требуется, чтобы интерфейс (между CE и PE, используемый для сигнализации) был способен инициировать/обрабатывать протокольные сообщения GMPLS [RFC3473] и следовал процедурам, описанным в [RFC4208].

Важной задачей сервиса L1VPN является возможность поддержки «одной точки обслуживания» (single-ended provisioning), когда добавление нового порта в данную L1VPN включает изменение конфигурации только в PE, содержащем этот порт. Расширение этой модели на CE выходит за рамки L1VPN BM.

Другой важной задачей сервиса L1VPN является организация/завершение LSP между парой (существующих) портов внутри L1VPN от устройств CE без изменения конфигурации в каких-либо устройствах сервис-провайдера. Иными словами, топология VPN находится под управлением CE (предполагается, что нижележащая связность PE-PE обеспечивается и разрешена сетью).

Описанные в этом документе механизмы направлены на решение этих задач. В частности, как компоненты сервиса L1VPN, эти механизмы (1) позволяют сервис-провайдеру ограничить набор портов, к которым может подключиться данный порт, (2) позволяют CE организовать LSP для подмножества портов. И, наконец, механизмы позволяют поддерживать любые топологии L1VPN, от hub-and-spoke (подключение к концентратору) до full mesh point-to-point (полносвязная сеть соединений «точка-точка». Поддерживаются только каналы point-to-point.

Обмен маршрутной и топологической информацией CE с поставщиком услуг выходит за рамки L1VPN BM.

3. Адресация, порты, каналы и каналы управления

Соглашения GMPLS для адресации и нумерации каналов рассмотрены в [RFC3945]. В этом разделе приводятся определения для случая L1VPN, где адресация пользователей и поставщиков услуг происходит в контексте уровня 1.

[1] Traffic Engineering - организация (построение) трафика.
[2] Packet Switch Capable - коммутация пакетов.
[3] Layer 2 Switch Capable - коммутация на канальном уровне.
[4] Виртуальная частная полоса (лямбда) в оптическом кабеле.
[5] Generalized Protocol Identifier - обобщенный идентификатор протокола.
[6] Head-end CE и tail-end CE.
[7] Timeslot.
[8] Switching capability.

3.1. Область адресов сервис-провайдера

Для провайдера или группы сервис-провайдеров, обеспечивающих услуги L1VPN, **требуется** наличие области адресации, покрывающей все устройства PE, вовлеченные в предоставление услуг L1VPN. Требуются механизмы GMPLS для организации и поддержки путей. Мы будем называть эту область адресной областью сервис-провайдера. Кроме того, для каждого абонента L1VPN **требуется** своя область адресации с полной свободой применения публичных или приватных адресов. Эти области мы будем называть областями адресации абонентов. Абонентские области адресации **могут** перекрываться (т. е., адреса в них не уникальны) между собой и **могут** также пересекаться с областью адресов провайдера.

3.2. Порты и индексы на уровне 1

В данной L1VPN каждый порт CE, соединяющий CE с PE, имеет идентификатор, который уникален в рамках этой L1VPN (не требуется уникальность в нескольких L1VPN). Одним из способов создания такого идентификатора является назначение каждому порту уникального в рамках L1VPN адреса и применение этого адреса в качестве идентификатора. Другим вариантом является назначение каждому порту CE уникального в масштабе CE индекса и назначение каждому CE уникального в рамках L1VPN адреса с использованием в качестве идентификатора порта пары <индекс порта, адрес CE>. Отметим, что адреса порта и CE **могут** указываться в нескольких форматах, включая IPv4 и IPv6. Этот идентификатор является частью абонентской области адресов и служит устройству CE для идентификации порта CE и удаленного порта CE для сигнализации. CE не знают и не понимают адресов из области сервис-провайдера.

В сети сервис-провайдера каждый порт PE, соединяющий данное устройство PE с устройством CE имеет уникальный в рамках этой сети идентификатор. Одним из способов создания таких идентификаторов является задание для каждого порта PE уникального в рамках данного PE индекса, назначение для PE уникального в масштабе области адресов провайдера адреса IP и использование пары <индекс порта, адрес PE IPv4> или <индекс порта, адрес PE IPv6> в качестве идентификатора порта в сети сервис-провайдера. Другим вариантом является назначение для каждого порта адреса IPv4 или IPv6, уникального в рамках области адресации сервис-провайдера. В любом случае адрес IPv4 или IPv6 является внутренним для сети сервис-провайдера и применяется для сигнализации GMPLS внутри этой сети.

В результате каждый канал, подключающий CE к PE, имеет порт CE с уникальным в рамках данной L1VPN идентификатором и порт PE с уникальным для сети сервис-провайдера идентификатором. Будем называть первый идентификатор CPI[1], а второй - PPI[2].

3.3. Отображение между портами и индексами

Этот документ требует для каждого порта PE, имеющего PPI, наличие также уникального в рамках связанной с этим портом L1VPN идентификатора из пользовательской области адресов. Одним из способов создания такого идентификатора является назначение каждому порту адреса, который уникален в пользовательской области адресов данной L1VPN, и использование этого адреса в качестве идентификатора порта. Другим вариантом является назначение каждому порту индекса, который уникален в рамках данного PE, назначение каждому PE уникального адреса IP из пользовательской области адресов данной L1VPN (этот адрес может не быть уникальным в сети сервис-провайдера) и использование пары <индекс порта, IP-адрес PE> в качестве идентификатора порта. Будет обозначать эти идентификаторы VPN-PPI (см. рисунок 2).

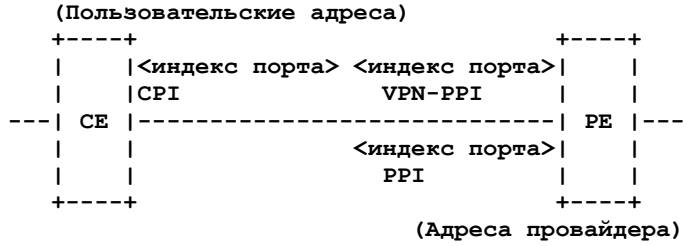

Рисунок 2. Отображение Customer/Provider Port/Index.

Для L1VPN требуется, чтобы операции сервис-провайдера были не зависимы от области адресации VPN абонента, а область адресации сервис-провайдера была скрыта от пользователей. Для решения этой задачи определим на PE два идентификатора - один для пользователя, другой для сервис-провайдера. IP-адрес PE, используемый для VPN-PPI, не зависит от IP-адреса PE, используемого для PPI (они берутся из разных областей адресации - первый из пользовательской, второй из области адресов VPN сервис-провайдера). Если для данного порта PE интерфейсы PPI и VPN-PPI являются безадресными (unnumbered), оба интерфейса могут использовать одинаковый индекс порта. Это достаточно удобно, поскольку PPI и VPN_PPI могут использовать любую комбинацию приемлемых форматов.

Как было отмечено выше, адрес IP, используемый для CPI, PPI и VPN-PPI, может быть адресом IPv4 или IPv6.
Для данного канала, соединяющего CE с устройством PE выполняются приведенные ниже условия.

- Если CPI является адресом IPv4, значение VPN-PPI также **должно** быть адресом IPv4, поскольку для VPN-PPI используются адреса из пространства абонента. Если CPI представлен парой <port index, CPI IPv4 address>, значение VPN-PPI **должно** быть парой <port index, PE IPv4 address> по той же причине.

- Если CPI является адресом IPv6, значение VPN-PPI также **должно** быть адресом IPv6, поскольку для VPN-PPI используются адреса из пространства абонента. Если CPI представлен парой <port index, CPI IPv6 address>, значение VPN-PPI **должно** быть парой <port index, PE IPv4 address> по той же причине.

Примечание. Для конкретного порта PE использование в качестве VPN-PPI адреса IP или пары <port index, PE IP address> не зависит от формата PPI данного порта.

[1]Customer Port Identifier - идентификатор порта абонента.
[2]Provider Port Identifier - идентификатор порта провайдера.

В этом документе предполагается, что назначение PPI находится под исключительным контролем сервис-провайдера (без какой-либо координации с абонентами L1VPN), тогда как назначение адресов, используемых CPI и VPN-PPI, контролируется исключительно администраторами L1VPN. Это обеспечивает максимальную гибкость. Администратор L1VPN полностью управляет услугами L1VPN, относящимися к конкретным абонентам L1VPN. Эта функция может принадлежать сервис-провайдеру, но может также выполняться сторонней компанией, имеющей договор с сервис-провайдером. Естественно, каждый абонент L1VPN может назначать такие адреса самостоятельно, без какой-либо координации с другими L1VPN.

Этот документ также требуется связности на уровне IP между устройствами CE и PE, как было отмечено выше. Эта связь служит для организации канала управления между CE и PE. Связь может представлять собой один интервал (hop) IP, реализованный через выделенный канал, в форме L2 VPN или частной сети IP (например, L3VPN). Единственным требованием к такой связности является является однозначное сопоставление конкретного канада управления от CE к PE с конкретной сетью L1VPN. При реализации связи по выделенному каналу этот канал должен быть связан с конкретной сетью L1VPN. При реализации соединения на основе L2VPN, следует выделять отдельную L2VPN для сопоставления с L1VPN. При реализации соединения на основе L3VPN, следует выделять отдельную L3VPN для сопоставления с L1VPN.

Будем обозначать адрес CE этого канала CE-CC-Addr[1], а адрес PE - PE-CC-Addr[2]. Оба адреса CE-CC-Addr и PE-CC-Addr **должны** быть уникальными а рамках L1VPN, к которой они относятся, но не **требуется** обеспечивать их уникальность в разных L1VPN. Адреса канала управления не используются совместно в разных VPN. Назначение адресов CE-CC-Addr и PE-CC-Addr контролируется администраторами L1VPN.

Множество портов устройства CE могут использовать общий канал управления только в том случае, когда все эти порты относятся к одной L1VPN. Аналогично, множество портов устройства PE могут использовать общий канал управления только в том случае, когда все эти порты относятся к одной L1VPN.

4. Базовый режим L1VPN на основе портов

L1VPN представляет собой базовый сервис VPN на основе портов, где пара CE может быть соединена через сеть сервис-провайдера с помощью LSP на основе GMPLS в данной топологии порта VPN. Именно этот LSP является базовым элементом услуг L1VPN, которые предоставляет сервис-провайдер. Если порт, служащий для подключения CE к устройству PE, включает множество каналов (например, разные длины волн), CE может организовать LSP с несколькими другими устройствами CE в одной VPN через один порт.

В L1VPN сервис-провайдер не инициирует создания LSP между парой портов CE. Создание LSP инициируется устройством CE. Однако SP с помощью описанного здесь механизма и средств ограничивает набор портов CE, которые могут быть удаленными точками LSP с данным портом в качестве локальной конечной точки. С учетом этих ограничений связность между CE находится под управлением самих устройств CE. Иными словаи, SP позволяет иметь в L1VPN некий набор топологий, выражаемый как матрица соединений между портами. Для выбора определенной топологии из этого набора служит инициируемая CE сигнализация.

Для каждого экземпляра L1VPN, имеющего хотя бы один порт на данном PE, устройство PE поддерживает таблицу PIT, связанную с L1VPN. Эта таблица содержит список пар <CPI, PPI> для всех портов в L1VPN. Кроме того, для портов локального PE данного экземпляра L1VPN включаются также значения VPN-PPI.

Рисунок 3. Базовый режим L1VPN.

4.1. Таблицы информации портов L1VPN

На рисунке 3 показаны 3 сети VPN - VPN-A, VPN-B и VPN-C со связанными таблицами PIT. Таблица PIT включает локальные и удаленные данные. Отсюда следует, что PIT на данном PE заполняется из двух источников.

1. Информация, относящаяся к портам CE, которые подключены к портам локального PE.
2. Информация о CE, подключенных к удаленным PE.

PIT **может** заполняться путем предоставления или автоматического обнаружения. В случае предоставления вся таблица **может** быть заполнена по команде предоставления с консоли или из системы управления, которая может включать средства автоматизации. По мере роста сети автоматизация становится потребностью.

[1]CE Control Channel Address - адрес CE канала управления.
[2]PE Control Channel Address - адрес PE канала управления.

Для локальной информации между CE и PE элемент PE **может** усилить LMP для заполнения канальной информации <CPI, VPN-PPI>. Эта локальная информация должна также распространяться другим PE в той же VPN. Механизмы этого выходят за рамки документа, но информация, которой нужно обмениваться, указана в параграфе 4.1.1.

PIT по своей природе относится к VPN. Элементу PE **требуется** поддерживать PIT для каждой L1VPN, куда она имеет локально подключенные CE. PE не требуется поддерживать PIT для других L1VPN. Однако полный набор PIT со всеми записями L1VPN для множества VPNs **может** быть доступен всем PE.

Удаленная информация в контексте идентификатора VPN (т. е. удаленные CE этой VPN) также **может** передаваться локальным CE, относящимся к той же VPN. Обмен этой информацией выходит за рамки документа.

4.1.1. Локальные данные автоматического обнаружения

Данными, которые требуется обнаруживать на локальном порту PE, являются локальный CPI и VPN-PPI.

Эта информация **может** быть настраиваемой или **может** быть полученной при обмене с LMP, если тот применяется между CE и PE.

Когда CPI обнаружен, соответствующий VPN-PPI отображается в локальном контексте на идентификатор VPN и соответствующий PPI. Одним из способов обеспечения контролируемого провайдером контекста VPN является предварительное обеспечение VPN-PPI идентификатором VPN. Другие механизмы политики для решения этой задачи выходят за рамки документа. Таким образом, связь CPI и VPN и PPI порта может быть установлена когда порт предоставлен как относящийся к VPN.

4.1.2. Информация автоматического обнаружения в PE

В этом параграфе представлена информация, которая передается любым механизмом автоматического обнаружения и служит для динамического заполнения PIT. Информация обеспечивает одно отображение <CPI, PPI>. Каждый механизм автоматического детектирования будет определять метод(ы) для обмена и аннулирования множества отображений <CPI, PPI>.

Эту информацию следует рассматривать независимо от используемого для ее распространения механизма [RFC5195], [RFC5252].

Формат кодирования <PPI, CPI> представлен на рисунке.

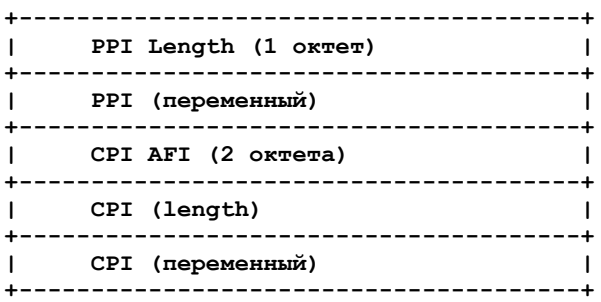

Рисунок 4. Информация автоматического обнаружения.

Значение полей описано ниже.

PPI Length

Однооктетное поле, указывающее размер поля PPI.

PPI

Поле переменного размера, содержащее значение PPI (адрес или <port index, address>). Отметим, что PPI всегда согласованно кодируются в домене провайдера, поэтому формат поля PPI неявно присутствует в сети данного провайдера.

CPI AFI

Двухоктетное поле, указывающее семейство адресов CPI. Значения берутся из [RFC1700].

CPI Length

Однооктетное поле, указывающее размер поля CPI.

CPI

Поле переменного размера, содержащее значение CPI (адрес или <port index, address>).

Кортежи <PPI, CPI> также **должны** быть связаны с одним или несколькими уникальными в глобальном масштабе идентификаторами, связанным с конкретной VPN. Такими идентификаторами могут служить VPN-ID, цель маршрута или иной идентификатор, уникальный в глобальном масштабе. Для базового режима достаточно уникальности идентификатора в административном домене сервис-провайдера. При использовании множества провайдеров (это выходит за рамки документа) достаточно уникальности и согласованности идентификатора среди этих провайдеров. В этом документе задан базовый формат кодирования для уникального в глобальном масштабе идентификатора, подходящий для всех механизмов автоматического обнаружения. Однако каждый такой механизм будет определять конкретный метод(ы) распространения кодирования и привязки к кортежу <PPI, CPI>. Кодирование уникального в глобальном масштабе идентификатора, связанное с VPN показано на рисунке.

```
+-----------------------------------------------+
|Глобально уникальн. идентифик. L1VPN(8 октетов) |
+-----------------------------------------------+
```

Рисунок 5. Auto-Discovery Globally Unique Identifier Format.

4.2. Организация LSP между CE

Для организации LSP элементу CE нужно идентифицировать все другие CE в его L1VPN, с которыми он хочет соединиться. CE может уже иметь эту информацию, полученную через представление или иную схему (такие схемы выходят за рамки документа).

Порты, связанные с данным каналом от CE к PE, **могут** также иметь другую связанную с ними информацию в дополнение к их CPI и PPI, которая описывает характеристики и ограничения каналов в этих портах, такие как поддерживаемое каналами кодирование, пропускная способность, общая незарезервированная полоса порта и т. п. Эта информация может быть дополнена данными о некоторых возможностях сети провайдера (например, поддержка служебной информации секции регенерации - RSOH[1], прозрачность DCC[2], произвольная конкатенация и пр.). Такая информация служит для обеспечения наличия у портов на каждой стороне LSP совместимых характеристик и достаточно объема нераспределенных ресурсов для организации LSP между этими портами.

Может случиться, что для данной пары портов в L1VPN каждый из CE, подключенных к этим портам, будет одновременно пытаться организовать LSP с другим CE. Если наличие пары LSP между двумя портами нежелательно, можно потребовать от CE с меньшим значением CPI прервать LSP, созданный этим CE. Эта опция может управляться настройкой CE.

4.3. Сигнализация

В L1VPN BM нужно настраивать CE с CPI других портов. После настройки CE с CPI других портов в той же L1VPN, которые называют целевыми портами, CE использует подмножество сигнализации GMPLS для запроса у сети провайдера организации LSP с целевым портом.

Для соединений между CE элемент CE создает запрос, содержащий CPI одного из портов, который он хочет применять для LSP, и CPI целевого порта. Когда PE, подключенный к инициировавшему запрос CE, получит этот запрос, он будет определять соответствующую PIT, а затем использовать информацию этой PIT для поиска PPI, связанного с CPI целевого порта, указанного в запросе. Для организации LSP элементу PE должно быть достаточно PPI. В конечном итоге запрос приходит в CE, связанный с целевым CPI (отметим, что в запросе сохраняется CPI инициировавшего запрос элемента). Если CE, связанный с целевым CPI, принимает запрос, организуется LSP.

Отметим, что CE не требуется создавать LSP с каждым целевым портом, известным ему, т. .е локальная политика заключается в выборе подмножества целевых портовЮ с которыми CE будет пытаться организовать LSP.

Процедуры организации отдельного соединения между двумя соответствующими CE совпадают с процедурой, заданной для перекрытия GMPLS [RFC4208].

4.3.1. Сигнальные процедуры

Когда входной CE передает сообщение RSVP Path входному PE, IP-адрес отправителя в пакете IP с сообщением указывает подходящий CE-CC-Addr, а целевой адрес IP в пакете - подходящий PE-CC-Addr. Когда входной PE шлет назад входному CE соответствующее сообщение Resv, для IP-адреса отправителя в пакете IP с сообщением указывается PE-CC-Addr, а для получателя - CE-CC-Addr.

Аналогично при передаче выходным PE сообщения RSVP Path выходному CE адрес отправителя в пакете IP с сообщением содержит подходящий PE-CC-Addr, а адрес получателя - подходящий CE-CC-Addr. Когда выходной CE возвращает выходному PE соответствующее сообщение Resv, IP-адресом отправителя в пакете с сообщением будет CE-CC-Addr, получателя - PE-CC-Addr.

Помимо использования IP-адресов в пакетах IP с сообщениями RSVP между CE и PE, адреса CE-CC-Addr и PE-CC-Addr применяются в поле Next/Previous Hop Address объектов IF_ID RSVP_Hop Object, передаваемых между CE и PE.

Когда канал между CE и PE имеет адреса и не является связкой, CPI и VPN-PPI этого канала используются для TLV типа 1 или 2 объекта IF_ID RSVP_Hop Object, который передается между CE и PE. Если канал между CE и PE является безадресным и не является связкой, CPI и VPN-PPI этого канала используются для поля IP Address в TLV типа 3. Если канал между CE и PE является связкой, CPI и VPN-PPI этого канала используются для поля IP Address в TLV типа 3.

Дополнительная обработка, связанная с безадресными каналами, описана в разделе 3 (Обработка объекта IF_ID RSVP_HOP) и параграфе 4.1 (Безадресаная смежность по пересылке) RFC 3477 [RFC3477].

Когда входной CE передает сообщение Path для организации LSP от удаленного порта к данному CE о определенный целевой порт, CE использует CPI своего порта в объекте Sender Template. Если CPI целевого порта является адресом IP, CE использует его в объекте Session. А если это кортеж <port index, IP address>, CE использует IP-адрес из кортежа в объекте Session, а весь кортеж - в качестве субобъекта Unnumbered Interface ID в явном объекте маршрутизации (ERO[3]).

Для сессий RSVP-TE имеется два варианта. В одном имеется сквозной сеанс RSVP-TE, где адреса клиента и провайдера меняются местами на PE (это называется перестановкой). В другом варианте используется сшивание или иерархия для создания двух сессий LSP - одна между провайдерскими PE, другая (сквозная) - между CE.

4.3.1.1. Сессии с перестановкой

Сессии перетасовки применяются, когда желательно иметь LSP, начинающийся на CE и завершающийся на удаленном CE. Адрес клиента заменяется провайдерским адресом на входном PE, а на выходном PE выполняется обратная перестановка с использованием отображения, предоставленного PIT.

[1]Regeneration section overhead.
[2]Data Communications Channel - канал передачи данных.
[3]Explicit Route Object.

Когда сообщение Path приходит на входной PE, тот выбирает PIT, связанную с L1VPN, а затем использует его для отображения CPI, передаваемых в объектах Session и Sender Template на подходящие PPI. После того как отображение выполнено, входной PE заменяет CPI этими PPI. В результате объекты Session и Sender Template, которые передаются сигнализацией GMPLS в сети провайдера, содержат PPI, а не CPI.

На выходном PE выполняется обратное отображение. PE извлекает значения входных и выходных PPI из объектов Sender Template и Session (соответственно). Выходной PE идентифицирует подходящую PIT для поиска нужного CPI, связанного с PPI выходного CE. Когда отображение найдено, выходной PE заменяет входное и выходное значения PPI соответствующими значениями CPI. В результате объекты Session и Sender Template (включенные в сообщение GMPLS RSVP-TE Path от выходного PE к выходному CE) содержат значения CPI, а не PPI.

Для сообщений GMPLS RSVP-TE Path, отправленных от выходного PE элементу CE здесь также устанавливается для IP-адреса отправителя (в пакете IP с сообщением) подходящее значение PE-CC-Addr, а для получателя - подходящее значение CE-CC-Addr.

На этом этапе CE видит один LSP «точка-точка» между двумя CE с виртуальным каналом между узрами PE - CE-PE(-)PE-CE. Узлы L1VPN PE видят сегмент PE-PE LSP со всеми детялями. Элементы PE **могут** фильтровать сигнализацию RSVP-TE, т. е. удалять информацию о топологии провайдера и заменять ее представлением виртуального канала.

Эта трансляция адресов и идентификаторов сессий называется перестановкой (shuffling) и управляется таблицами L1VPN Port Information Table (раздел 4). Перестановка **должна** выполняться для всех сообщений RSVP-TE на краевых устройствах PE. В этом случае имеется одна сессия CE-CE.

4.3.1.2. Сшитые или вложенные сессии

Варианты Stitching (сшивание) или Nesting (вложение) зависят от типа коммутации LSP. Если PE между CE (CE-CE) и между PE (PE-PE) идентичны по типу коммутации и пропускной способности, LSP **можно** сшить вместе и применить процедуры [RFC5150]. Если CE-CE LSP и PE-PE LSP имеют разный тип коммутации или имет разную, но совместимую пропускную способность, LSP **можно** вложить один в другой применить процедуры [RFC4206]. Поскольку сигнальные процедуры Stitched и Nested LSP включают организацию сессии между элементами PE, совместимой с параметрами сессии CE, они описываются вместе.

При получении сообщения Path Message входным PE этот PE выбирает PIT, связанную с L1VPN, а затем использует его для отображения значений CPI из объектов Session и Sender Template на подходящие PPI. После отображения организуется новая сессия между PE с параметрами, совместимыми с сессией CE. После организации этой сессии передается запрос сигнализации CE выходному элементу PE.

На входном PE при использовании сшивания или встраивания организуется сессия между PE. Это можно сделать одним из перечисленных ниже способов.

- Связывание имеющегося LSP между PE или Forwarding Adjacency LSP (FA-LSP) с получателем, соответствующим запрошенным параметрам.
- Организация подходящего сегмента PE-PE LSP.

В этот момент CE будет видеть один LSP «точка-точка» между двумя CE с виртуальгым каналом между узлами PE - CE-PE(-)PE-CE. Узлы L1VPN PE будет видеть сегмент PE-PE LSP со всеми детялями. Узлы PE не фильтруют сигнализацию RSVP-TE путем удаления данных о топологии провайдера, поскольку сигнализация PE-PE не видна CE.

4.3.1.3 Прочая сигнализация

Входной PE может получить и, возможно, отвергнуть сообщение Path с ERO, что может привести к отказу при организации коммутируемого соединения. Однако входной PE может воспринимать объекты ERO, которые включают последовательность {<входной PE (строго), CPI выходного CE (loose)>}.

- Сообщение Path без ERO. Когда входной PE получает от входного CE сообщение Path без ERO, он **должен** рассчитать маршрут к получателю для PE-PE LSP и включить этот маршрут в ERO до пересылки сообщения Path. Единственным исключениям является случай, когда выходной узеля ядра является смежным с данным узлом.
- Сообщение Path с ERO. Когда входной PE получает от входного CE сообщение Path ERO (в указанной выше форме), он рассчитывает путь до выходного PE. Затем этот добавляется в ERO до пересылки сообщения Path.

В случае перестановки правила налодения для уведомлений и обработки RRO идентичны UNI[1] или модели Overlay [RFC4208], в которых сказано, что Edge PE **может** удалять и редактировать Provider Notification и объекты RRO при передаче сообщений элементам CE.

4.4. Процедуры восстановления

Сигнализация

CE запрашивает защищенный сетью LSP (т. е. LSP, защищенный от PE до PE), используя описанный в [RFC4873] метод. Динамическая идентификация узлов слияния поддерживается с помощью флагов LSP Segment Recovery Flag, передаваемых в объекте Protection (см. параграф 6.2 в [RFC4873]).

Уведомления

Объект Notify Request **может** быть помещен в сообщение Path или Resv для указания адреса элемента CE, который следует уведомлять при отказе LSP. Уведомления **можно** запросить в восходящем и нисходящем направлении:

- восходящие уведомления указываются включением объекта Notify Request в соответствующее сообщение Path;

[1]User-Network Intercase - интерфейс между пользователем и сетью.

- нисходящие уведомления указываются включением объекта Notify Request в соответствующее сообщение Resv.

PE, получившему сообщение с объектом Notify Request, **следует** сохранить Notify Node Address в соответствующем блоке состояния RSVP. PE **следует** также включить объект Notify Request в исходящее сообщение Path или Resv. Исходящий адрес Notify Node Address **может** быть обновлен на основе локальной политики. Это означает, что PE при получении объекта от CE **может** обновить значение Notify Node Address.

Если входной CE включает объект Notify Request в сообщение Path, входной PE **может** заменить принятое значение Notify Node Address своим выбранным Notify Node Address (в частности, локальным TE Router_ID). Объект Notify Request **может** передаваться в сообщениях Path или Resv (раздел 7 в [RFC3473]). Формат объекта Notify Request определен в [RFC3473]. В соответствии с параграфом 4.2.1 [RFC3473] в качестве Notify Node Addresses **нужно** указывать адрес IPv4 или IPv6.

Включение объекта Notify Request служит для запроса генерации уведомлений, но не гарантирует создания сообщений Notify.

5. Вопросы безопасности

Безопасность L1VPN рассмотрена в [RFC4847] и [RFC5253]. В этом документе рассматриваются вопросы безопасности, связанные с уровнем управления.

Привязка определенного порта к конкретной L1VPN (точнее, к определенной PIT) является операцией настройки, обычно выполняемой сервис-провайдером вручную при настройке предоставления услуги. Таким образом, ее нельзя подменить через сигнализацию между CE и PE. Это означает, что сигнализацию невозможно использовать для доставки трафика L1VPN не тому клиенту. Оператору следует использовать подходящие механизмы защиты процессов администрирования и настройки, а также рассмотреть методы проверки уровня данных для предотвращения непреднамеренных ошибок при настройке. Клиент может также использовать сквозную (от CE до CE) проверку связности на уровне данных L1VPN для обнаружения некорректных соединений. Тестирование связности уровня данных можно выполнить с помощью протокола LMP[1] [RFC4204].

Отметим, что можно заполнить локальную часть PIT с помощью автоматического обнаружения LMP. Протокол LMP может быть защищен, как описано в [RFC4204]. Предполагается, что сигнализация между CE и PE передается по частному каналу (например, в основной полосе или по волокну) или частной сети. Использование частных каналов делает соединение CE с PE защищенным с тем же уровнем, что и описанный выше канал данных. Использование частной сети предполагает, что внешние элементы не могут подделать или изменить управляющее взаимодействие между CE и PE. Кроме того, все элементы частной сети считаются доверенными. Таким образом, для описанных в этом документе протокольных обменов не требуется механизмов защиты.

Однако оператор, озабоченный безопасностью своих частных линий, может применять функции аутентификации и защиты целостности, доступные в RSVP-TE [RFC3473], или использовать IPsec ([RFC4301], [RFC4302], [RFC4835], [RFC4306], и [RFC2411]) для сигнализации «точка-точка» между PE и CE. В [MPLS-SEC] рассмотрены варианты защиты, доступные для уровня управления GMPLS.

Отметим, что частая сеть (например, L2 VPN или L3 VPN) может применяться для организации управляющего соединения между PE и несколькими CE. В таком варианте **некомендуется** для каждого клиента L1 VPN иметь свою частную сеть. Механизмы защиты частной сети **следует** использовать для обеспечения безопасности управляющих взаимодействий между клиентом и сервис-провайдером.

6. Литература

6.1. Нормативные документы

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

[RFC3471] Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description", RFC 3471, January 2003.

[RFC3473] Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

[RFC3477] Kompella, K. and Y. Rekhter, "Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)", RFC 3477, January 2003.

[RFC4202] Kompella, K., Ed., and Y. Rekhter, Ed., "Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4202, October 2005.

[RFC4204] Lang, J., Ed., "Link Management Protocol (LMP)", RFC 4204, October 2005.

[RFC4206] Kompella, K. and Y. Rekhter, "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)", RFC 4206, October 2005.

[RFC4208] Swallow, G., Drake, J., Ishimatsu, H., and Y. Rekhter, "Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model", RFC 4208, October 2005.

[RFC4873] Berger, L., Bryskin, I., Papadimitriou, D., and A. Farrel, "GMPLS Segment Recovery", RFC 4873, May 2007.

[RFC5150] Ayyangar, A., Kompella, K., Vasseur, JP., and A. Farrel, "Label Switched Path Stitching with Generalized Multiprotocol Label Switching Traffic Engineering (GMPLS TE)", RFC 5150, February 2008.

[1]Link Management Protocol - протокол управления каналом.

6.2. Дополнительная литература

[RFC1700] Reynolds, J. and J. Postel, "Assigned Numbers", RFC 1700[1], October 1994.

[RFC3945] Mannie, E., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", RFC 3945, October 2004.

[RFC4201] Kompella, K., Rekhter, Y., and L. Berger, "Link Bundling in MPLS Traffic Engineering (TE)", RFC 4201, October 2005.

[RFC4847] Takeda, T., Ed., "Framework and Requirements for Layer 1 Virtual Private Networks", RFC 4847, April 2007.

[RFC2411] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4306] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.

[RFC5195] Ould-Brahim, H., Fedyk, D., and Y. Rekhter, "BGP-Based Auto-Discovery for Layer-1 VPNs", RFC 5195, June 2008.

[RFC5252] Bryskin, I. and L. Berger, "OSPF-Based Layer 1 VPN Auto-Discovery", RFC 5252, July 2008.

[RFC5253] Takeda, T., Ed., "Applicability Statement for Layer 1 Virtual Private Network (L1VPN) Basic Mode", RFC 5253, July 2008.

[MPLS-SEC] Fang, L., Ed., " Security Framework for MPLS and GMPLS Networks", Work in Progress, February 2008.

7. Благодарности

Авторы благодарят Adrian Farrel, Hamid Ould-Brahim и Tomonori Takeda за полезные комментарии.

Sandy Murphy, Charlie Kaufman, Pasi Eronen, Russ Housley, Tim Polk и Ron Bonica помогли в процессе IESG review.

Адреса авторов

Don Fedyk

Nortel Networks

600 Technology Park

Billerica, MA 01821

Phone: +1 (978) 288 3041

EMail: dwfedyk@nortel.com

Yakov Rekhter

Juniper Networks

1194 N. Mathilda Avenue

Sunnyvale, CA 94089

EMail: yakov@juniper.net

Dimitri Papadimitriou

Alcatel-Lucent

Fr. Wellesplein 1,

B-2018 Antwerpen, Belgium

Phone: +32 3 240-8491

EMail: Dimitri.Papadimitriou@alcatel-lucent.be

Richard Rabbat

Google Inc.

1600 Amphitheatre Pky

Mountain View, CA 95054

EMail: rabbat@alum.mit.edu

Lou Berger

[1]В соответствии с RFC 3232 этот документ заменен базой данных http://www.iana.org/numbers/. *Прим. перев.*

LabN Consulting, LLC

Phone: +1 301-468-9228

EMail: lberger@labn.net

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

Полное заявление авторских прав

Интеллектуальная собственность