Network Working Group
Request for Comments: 4665
Category: Informational

W. Augustyn, Ed.
Y. Serbest, Ed.
AT&T

September 2006

Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks

Требования к предоставляемым провайдерами услугам L2VPN

Статус документа

В этом документе содержится информация для сообщества Internet. Документ не задаёт каких-либо стандартов Internet. Документ может распространяться без ограничений.

Аннотация

Этот документ описывает требования для предоставляемых провайдерами услуг виртуальных частных сетей канального уровня (L2VPN[1]). Здесь впервые определены терминология и систематика, а также заданы общие и базовые требования к сервису. Документ охватывает VPN типа «точка-точка», называемые VPWS[2], а также многоточечные VPN, называемые VPLS[3]. Требования детализированы и выражены с точки зрения абонентов и сервис-провайдеров.

Оглавление

1. Введение....2
1.1. Область действия....2
1.2. Структура документа....3
2. Уровни требований....3
3. Участники работы....3
4. Определения и систематика....3
4.1. Определения....3
4.2. Систематика типов L2VPN....3
4.3. VPWS....3
4.4. VPLS....3
5. Общие требования для абонента и сервис-провайдера....4
5.1. Область действия эмуляции....4
5.2. Типы трафика....4
5.3. Топология....4
5.4. Изолированный обмен данными и информацией о пересылке....5
5.5. Безопасность....5
5.5.1. Безопасность пользовательских данных....5
5.5.2. Контроль доступа....5
5.6. Адресация....5
5.7. Качество обслуживания....6
5.7.1. Стандарты QoS....6
5.7.2. Модели сервиса....6
5.8. Спецификация уровня сервиса....6
5.9. Защита и восстановление....6
5.10. Требования к каналам CE-PE и PE-PE....6
5.11. Управление....6
5.12. Совместимость....6
5.13. Взаимодействие....7
6. Абонентские требования....7
6.1. Независимость от SP....7
6.2. Поддержка L3....7
6.3. Качество обслуживания и параметры трафика....7
6.4. Спецификация уровня сервиса....7
6.5. Безопасность....7
6.5.1. Изоляция....7
6.5.2. Контроль доступа....7
6.5.3. Добавленные услуги защиты....7
6.6. Доступ в сеть....7
6.6.1. Технология физического и канального уровня....7
6.6.2. Подключения для доступа....8
6.7. Абонентский трафик....8
6.7.1. Пересылка индивидуального, группового и широковещательного трафика....8
6.7.2. Изменение порядка пакетов....8

[1]Layer 2 Provider-Provisioned Virtual Private Network.
[2]Virtual Private Wire Service - услуги виртуальных частных проводов.
[3]Virtual Private LAN Service - услуги виртуальных частных ЛВС.

6.7.3. Минимальное значение MTU....8
6.7.4. Сквозная трансляция тегов VLAN....9
6.7.5. «Прозрачность»....9
6.8. Поддержка протоколов управления L2....9
6.9. Предоставление CE....9
7. Требования сервис-провайдера....9
7.1. Расширяемость....9
7.1.1. Оценка пропускной способности сервиса....9
7.1.2. Параметры конкретных решений....9
7.2. Идентификаторы....9
7.3. Обнаружение относящейся к L2VPN информации....9
7.4. Качество обслуживания (QoS)....10
7.5. Изолированный обмен данными и информацией о пересылке....10
7.6. Безопасность....10
7.7. Межпровайдерские L2VPN....10
7.7.1. Управление....10
7.7.2. Запросы пропускной способности и QoS....11
7.8. «Оптовые» услуги L2VPN....11
7.9. Требования к туннелированию....11
7.10. Поддержка технологий доступа....11
7.11. Магистральные сети....11
7.12. Разделение и совместное использование ресурсов сети разными L2VPN....11
7.13. Совместимость....12
7.14. Тестирование....12
7.15. Поддержка имеющихся PE....12
8. Требования SP к управлению....12
9. Инженерные требования....12
9.1. Требования к уровню управления....12
9.2. Требования к уровню данных....12
9.2.1. Инкапсуляция....12
9.2.2. Отклики на перегрузку....12
9.2.3. Область широковещания....13
9.2.4. Экземпляры виртуальных коммутаторов....13
9.2.5. Изучение MAC-адресов....13
10. Вопросы безопасности....13
11. Благодарности....13
12. Литература....13
12.1. Нормативные документы....13
12.2. Дополнительная литература....13

1. Введение

В этом разделе описана структура и область действия документа.

1.1. Область действия

Этот документ описывает требования к предоставляемым провайдером услугам L2VPN. Документ определяет требования, которые **могут** применяться к одному или нескольким подходам, которые SP[1] может применять для предоставления услуг L2 VPN. В документе используется терминология, определённая в [RFC4026], и базовые компоненты развёртывания L2VPN, описанные в [RFC4664].

Технические спецификации для предоставления услуг L2VPN выходят за рамки этого документа. Эти вопросы рассматриваются в базовом документе [RFC4664] и нескольких других документах, описывающих технические аспекты предоставления услуг L2VPN, - [VPLS_LDP], [VPLS_BGP], [IPLS].

Документ описывает требования к двум типам L2VPN: (1) услуги виртуальных частных проводов (VPWS) и (2) услуги виртуальных частных ЛВС (VPLS). Подход, используемый в этом документе, различает типы L2VPN по способам организации соединений («точка-точка» или многоточечные), как описано в [RFC4664].

Этот документ предназначен на «контрольного списка» требований, которые обеспечат согласованный способ оценки и документирования соответствия каждого конкретного подхода конкретным требованиям. Результатом такой оценки должен быть документ о применимости каждого конкретного подхода.

В контексте предоставляемых провайдером VPN имеются два вовлечённых в работу сервиса участника - провайдер и абонент. Провайдер заключает с абонентом соглашение (договор) о поведении сервиса в нормальных условиях и исключительных ситуациях. Это называется спецификацией уровня обслуживания (SLS[2]) и является частью соглашения об уровне обслуживания (SLA[3]) между провайдером и абонентом.

Правильное устройство L2VPN помогает сформулировать SLS в части обеспечения способов подобающего разделения краевых устройств абонента (CE[4]) и провайдера (PE[5]), позволяющего выполнить SLS и обеспечить гибкий и обширный набор возможностей.

В документе приведены требования с точки зрения абонента и провайдера. Сначала рассматривается общая для провайдера и абонента точка зрения, затем рассматривается абонентский подход и потребности конкретного SP. Эти требования обеспечивают функции высокого уровня L2VPN, ожидаемые SP при предоставлении услуг L2VPN, включая требования SP к безопасности, конфиденциальности, управляемости, взаимодействию и расширяемости.

[1]Service Provider - сервис-провайдер.
[2]Service Level Specification.
[3]Service Level Agreement.
[4]Customer Edge.
[5]Provider Edge.

1.2. Структура документа

В разделе 4 приведены определения и систематика типов сервиса. В разделе 5 описаны общие требования, применимые к абоненты и SP, раздел 6 представляет требования с точки зрения абонента, а раздел 7 - с точки зрения SP. В разделе 8 рассматриваются требования к управлению SP, в разделе 9 описаны инженерные требования, в частности, для уровней данных и управления. Раздел 10 посвящён вопросам безопасности, в разделе 11 приведены благодарности, а в разделе 12 - список литературы.

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].

3. Участники работы

Этот документ является результатом работы группы людей. Ниже перечислены участники работы.

Waldemar Augustyn
Marco Carugi
Giles Heron
Vach Kompella
Marc Lasserre
Pascal Menezes
Hamid Ould-Brahim
Tissa Senevirathne
Yetik Serbest

4. Определения и систематика

4.1. Определения

Используемая в документе терминология определена в [RFC4026]. Базовый документ L2VPN [RFC4664] содержит описание концепций в контексте эталонной модели, определяющей многоуровневые соотношения между устройствами и одним или несколькими уровнями туннелирования.

4.2. Систематика типов L2VPN

Требования различают две основных модели L2VPN - виртуальные провода VPWS и виртуальные сети VPLS.

На рисунке 1 представлена эталонная модель сервиса L2VPN.

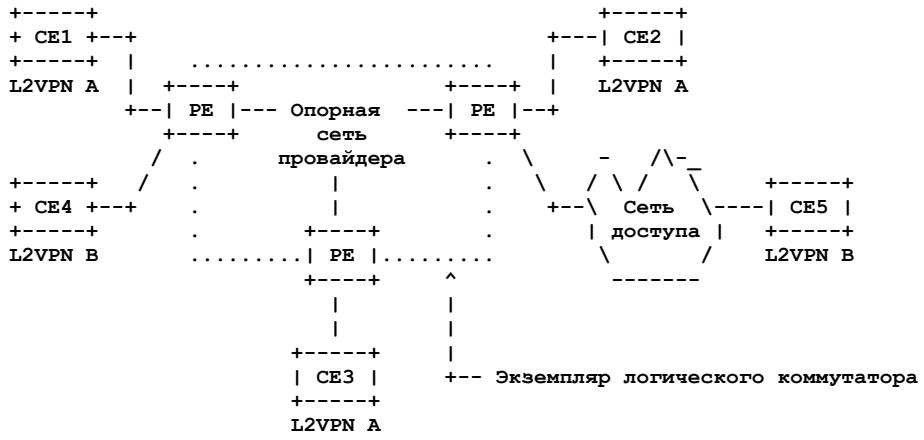

Рисунок 1. Эталонная модель L2VPN.

4.3. VPWS

Устройства PE обеспечивают логическое соединение между парой устройств CE, как будто они соединены одним логическим устройством L2. Устройства PE действуют как коммутаторы устройств (каналов) L2. Затем устройства L2 отображаются на туннели в сети SP. Эти туннели могут использоваться для конкретного экземпляра VPWS или быть общими для нескольких услуг. Сервис VPWS применим для Ethernet, ATM, Frame Relay и т. п. На рисунке 1 сеть L2VPN B представляет собой VPWS.

Каждое устройство PE отвечает за направление абонентских кадров L2 подходящему экземпляру VPWS и корректную пересылку заданному получателю.

4.4. VPLS

В случае VPLS устройства PE обеспечивают логические соединения так, что устройства CE, относящиеся к одной сети VPLS, представляются подключёнными к одной ЛВС. Сквозной сервис VPLS включает модуль моста и модуль эмуляции ЛВС ([RFC4664]). VPLS может включать одну или множество сетей VLAN([IEEE_802.1Q]). Вариантом этого сервиса является IPLS ([RFC4664]), где поддерживается лишь абонентский трафик IP.

В VPLS абонентский сайт получает обслуживание L2 от SP. Устройство PE подключается через каналы доступа к одному или множеству CE. PE выполняет пересылку пользовательских пакетов данных на основе информации в заголовках L2, такой как MAC-адрес получателя. На рисунке 1 сеть представляет L2VPN A сервис VPLS.

Детали рассматриваемой здесь эталонной модели описаны в [RFC4664]. В VPLS устройство PE можно рассматривать как содержащее экземпляр виртуального коммутатора (VSI[1]) для каждого поддерживаемого устройством сервиса L2VPN. Устройства CE подключаются (возможно, через сеть доступа) к модулю моста в PE. Внутри PE модуль моста соединяется через интерфейс эмулируемой ЛВС (Emulated LAN Interface) с эмулируемой ЛВС. Для каждого сервиса VPLS имеется экземпляр эмулируемой ЛВС. Emulated LAN состоит из модуля пересылки - VPLS Forwarder (один экземпляр на PE на сервис VPLS), подключённого псевдопроводом (PW[2]), который может проходить через туннели в сети пакетной коммутации (PSN[3]) по маршрутизируемой магистрали. VSI - это логический объект, содержащий модуль пересылки VPLS и часть модуля моста, относящуюся к экземпляру сервиса VPLS [RFC4664]. Следовательно VSI завершает PW для соединения с другими VSI, а также завершает устройства (каналы) присоединения - AC[4] (см. определение в [RFC3985]) для подключения устройств CE. VSI включает базы данных пересылки для L2VPN [RFC4664], которая представляет собой набор данных, определяющих пересылку кадров L2, принятых через AC от CE для VSI в других PE, поддерживающих тот же сервис L2VPN (и/или для других AC), а также данные для пересылки кадров L2, принятых из PW для устройств AC. Базы данных пересылки могут заполняться динамически (например, путём изучения MAC-адресов) или статически (например, в конфигурации). Каждое устройство PE отвечает за корректную пересылку абонентского трафика заданным получателям на основе базы данных пересылки соответствующего VSI.

5. Общие требования для абонента и сервис-провайдера

В этом разделе описаны общие требования для абонентов и провайдеров или те, что имеют общую природу.

5.1. Область действия эмуляции

Протоколам L2VPN **не следует** мешать работе имеющихся протоколов L2 и стандартов сетей L2, которыми управляет абонент. Если они влияют на абонентские протоколы L2, передаваемые через VPLS, это влияние **должно** быть документировано.

Некоторые различия между VPLS и реальными ЛВС, которые могут быть существенны, перечислены ниже.

- Надёжность может снижаться, т. е. вероятность того, что широковещательное сообщение через VPLS не будет замечено одним из модулей моста в PE выше, чем в реальной сети Ethernet.
- Кадры VPLS могут дублироваться, если в PW не включена опция упорядочения. Кадры данных передаются через PW в виде дейтаграмм IP и при некоторых отказах сети IP могут дублировать пакеты. Если протокол передачи данных в PW не гарантирует порядка пакетов, кадры могут дублироваться ил приниматься в нарушением порядка. Если абонентские кадры BPDU[5] передаются как пакеты данных, они могут дублироваться и последовательность BPDU может нарушаться, хотя это может и не создавать проблем для протокола RSTP[6].
- Отложенная (например, на полсекунды и более) доставка пакетов вместо их отбрасывания, может неблагоприятно влиять на производительность сервиса.
- Кадры 802.3x Pause не будут передаваться через VPLS, поскольку модули мостов ([RFC4664]) будут останавливать их.
- Поскольку решение IPLS нацелено на транспортировку инкапсулированного трафика (а не самих кадров L2), оно **не требует** сохранения заголовков L2 на пути от CE к CE. Например, адреса Source MAC могут не сохраняться в IPLS.

5.2. Типы трафика

Сеть VPLS **должна** поддерживать индивидуальный, групповой и широковещательный трафик. Весьма желательна поддержка эффективной репликации для группового и широковещательного трафика.

5.3. Топология

Сеть SP может быть реализована с применением одной или множества туннельных топологий для соединения устройств PE, начиная от простых соединений «точка-точка» и заканчивая распределенными иерархическими структурами. Типовые варианты топологии включают:

- «точка-точка» (Point-to-point);
- «один со многими» (Point-to-multipoint) или «звезда» (hub and spoke - концентратор и лучи);
- «каждый с каждым» (Any-to-any) или полносвязная (full mesh);
- смешанная или частично полносвязная (partial mesh);
- иерархическая.

Независимо от развёрнутой SP топологии сервис для абонентов **должен** сохранять тип соединений, предполагаемый решением L2VPN. Например, в VPLS **должны** поддерживаться многоточечные (multipoint-to-multipoint) соединения даже при реализации на каналах «точка-точка». Это требование не предполагает, что все характеристики трафика (такие как пропускная способность, QoS, задержки и т. п.) обязательно одинаковы между любой парой конечных точек L2VPN. Важно подчеркнуть, что требования SLS для сервиса связаны с типом топологии, которая может применяться.

Насколько это возможно, сервису L2VPN **следует** поддерживать работу через административные границы.

[1]Virtual Switching Instance.
[2]Pseudo wire.
[3]Packet Switched Network.
[4]Attachment Circuit.
[5]Bridge Protocol Data Unit - блок данных протокола мостов.
[6]Real-Time Streaming Protocol - протокол потоков в реальном масштабе времени.

Насколько это возможно, сервису L2VPN **следует** быть независимым от технологии сети доступа.

5.4. Изолированный обмен данными и информацией о пересылке

Решениям L2VPN **нужно** определять средства, которые предотвратят взаимодействие устройств CE в L2VPN с не имеющими полномочий элементами.

Решениям L2VPN **нужно** избегать внесения нежелательных данных, которые могут повредить базу данных пересылки L2VPN.

Должны предоставляться способы ограничения или изоляции для распространения имеющих конкретного адресата данных лишь тем сайтам VPLS, которые определены путём изучения MAC и/или параметрами конфигурации.

Внутреннюю структуру L2VPN не **следует** анонсировать за пределы L2VPN.

5.5. Безопасность

Набор решений L2VPN **должен** поддерживать широкий диапазон функций защиты. Каждое решение L2VPN **должно** заявлять поддерживаемые функции безопасности и указывать способы их настройки для каждого абонента.

Множество вопросов безопасности связано с организацией и работой L2VPN, начиная от ошибок конфигурации и заканчивая атаками, которые могут быть организованы на L2VPN и отнимать сетевые ресурсы, такие как память, пространство таблиц пересылки, пропускную способность и обработку в CPU.

В этом разделе рассмотрены потенциальные угрозы безопасности, которые могут возникать в результате конфигурационных ошибок и/или целенаправленных атак. **Должны** обеспечиваться меры защиты в перечисленных ниже ситуациях.

- Протокольные атаки:
  - организация/удаление избыточных отношений смежности;
  - избыточная сигнализация/отзыв.
- Расход ресурсов:
  - репликация на уровне пересылки (VPLS);
  - петли (в основном VPLS);
  - размер таблицы MAC (VPLS).
- Несанкционированный доступ:
  - неразрешенные участники VPN;
  - некорректный абонентский интерфейс;
  - некорректный тег VLAN для обозначения сервиса;
  - несанкционированный доступ к PE.
- Вмешательство в сигнализацию:
  - некорректная сигнализация FEC;
  - некорректное назначение метки PW;
  - передача некорректных параметров VPN (например, QoS, MTU и пр.).
- Вмешательство в пересылку данных:
  - некорректные записи изучения MAC;
  - некорректные метки PW;
  - некорректные идентификаторы AC;
  - некорректная инкапсуляция в сторону абонента;
  - некорректная инкапсуляция PW
  - перехват PW путём использования ложных туннелей;
  - некорректная туннельная инкапсуляция.

5.5.1. Безопасность пользовательских данных

Решение L2VPN **должно** обеспечивать разделение трафика разных L2VPN.

В случае VPLS для указания сервиса могут применяться идентификаторы VLAN. В таких случаях **должно** обеспечиваться аккуратное выделение тегов и разделение трафика.

5.5.2. Контроль доступа

Решение L2VPN **может** позволять использование подходящих средств фильтрации по запросу абонента.

5.6. Адресация

Решение L2VPN **должно** поддерживать использование перекрывающихся блоков адресов а разных L2VPN. Например, **недопустимо** препятствовать использованию абонентом одних MAC-адресов в разных L2VPN. Если сервис-провайдер

использует теги VLAN для обозначения сервиса, решение L2VPN **должно** гарантировать отсутствие совпадений тегов VLAN. Если теги VLAN не применяются для обозначения сервиса, решения L2VPN **могут** разрешать совпадение тегов.

5.7. Качество обслуживания

По возможности, для L2VPN QoS следует обеспечивать независимость от технологии сетей доступа.

5.7.1. Стандарты QoS

Как указано в [RFC3809], L2VPN **нужно** поддерживать QoS[1] в одном или нескольких стандартизованных режимах:

- Best Effort (поддержка обязательна для всех типов предоставляемых провайдером VPN);
- Aggregate CE Interface Level QoS (уровень «шланга»);
- Site-to-site QoS (уровень «трубы»).

Отметим, что во всех случаях использования QoS **может** потребоваться выполнение функций «формовки» и политики от устройств CE и/или PE.

Отображение и трансляция параметров L2 QoS на PSN QoS (например, DSCP или поле MPLS EXP), а также отображение QoS на основе VC (например, FR/ATM или VLAN) **может** выполняться для обеспечения «прозрачности» QoS. Реальные механизмы такого отображения или трансляции выходят за рамки этого документа. В дополнение к этому **может** применяться поддержка Diffserv базовыми технологиями туннелирования (например, [RFC3270] или [RFC3308]) и модель Intserv ([RFC2205]). Поэтому требования L2VPN SLS **следует** поддерживать подходящими механизмами в ядре сети.

5.7.2. Модели сервиса

Сервис-провайдер может предложить абонентам по меньшей мере базовые услуги QoS - управляемый доступ к услугам VPN или сквозной сервис QoS. Детали моделей сервиса приведены в [RFC3809] и [RFC4031].

В L2VPN для этих целей могут применяться поля DSCP ([RFC2474]) и 802.1p ([IEEE_802.1D]).

5.8. Спецификация уровня сервиса

Для сервиса L2VPN **следует** поддерживать возможности мониторинга и уведомлений для SLS [RFC3809].

5.9. Защита и восстановление

Для инфраструктуры сервиса L2VPN **следует** поддерживать резервные пути, обеспечивающие высокий уровень доступности. При возникновении отказа **следует** предпринимать попытки восстановить сервис по резервному пути.

Задача состоит в обеспечении времени восстановления, которое **должно** быть меньше времени, нужного устройствам CE или абонентским протоколам управления L2 и протоколам маршрутизации L3 для обнаружения отказа L2VPN.

5.10. Требования к каналам CE-PE и PE-PE

В качестве каналов между CE и PE **могут** применяться:

- прямые физические соединения (например, 100BaseTX, T1/E1 TDM);
- логические каналы (например, ATM PVC, каналы с инкапсуляцией RFC2427);
- транспортные сети Ethernet;
- туннели L2 через сети L3 (например, сессии L2TP).

Кадры L2 **могут** туннелироваться через магистрали L3 от PE к PE с использованием подходящего протокола (например, IP-in-IP, GRE, MPLS, L2TP и т. п.).

5.11. Управление

Должны обеспечиваться стандартные интерфейсы для управления услугами L2VPN (например, модули SNMP MIB). Этим интерфейсам **следует** предоставлять доступ к протоколам настройки, верификации и мониторинга работы.

Управление сервисом **может** включать функциональность TMN FCAPS[2], описанную в [ITU_Y.1311.1].

5.12. Совместимость

Следует гарантировать совместимость решений разных производителей, соответствующие близким сетевым и сервисным уровням в элементах сети. Это явно будет зависеть от полноты соответствия стандартам.

Технические решения **должны** совместимыми не только в инфраструктуре сети SP, но и с абонентским сетевым оборудованием и службами, использующими сервис L2VPN.

Решениям L2VPN **недопустимо** препятствовать использованию разных технологий доступа.

Например, абонентские подключения для доступа к сервису L2VPN **могут** быть разными на различных устройствах CE (например, Frame Relay, ATM, 802.1D, MPLS).

[1]Quality of service - качество обслуживания.
[2]Fault, Configuration, Accounting, Performance, and Security - отказы, настройка, учет, производительность и защита.

5.13. Взаимодействие

Весьма желательно взаимодействие между разными решениями, обеспечивающими сервис L2VPN. Возможны случаи, когда потребуется взаимодействие или соединение между сайтами через сети с разными решениями L2VPN или разными реализациями одного подхода. Для взаимодействия **следует** поддерживать расширяемость.

При взаимодействии **должны** обеспечиваться по меньшей мере изоляция, безопасность, QoS, контроль доступа и управление. Это требование важно для случаев перемещения сети, чтобы обеспечить непрерывность обслуживания между сайтами в разных частях сети.

6. Абонентские требования

В этом разделе рассматриваются требования с точки зрения абонентов.

6.1. Независимость от SP

Абонентам **может** требоваться сервис L2VPN, организуемый через множество административных доменов или сетей SP. Поэтому сервис L2VPN **должен** быть способен работать через множество автономных систем (AS) и сетей SP, оставаясь единой и однородной сетью L2VPN с точки зрения абонента.

Абонент может начать с сервиса L2VPN в одной AS с той или иной спецификацией SLS, а затем запросить расширение сервиса на множество AS и/или SP. В этом случае, а также в других вариантов межпровайдерских и многодоменных (AS) услуг L2VPN, сервису L2VPN **следует** поддерживать возможность обеспечения одной спецификации SLS для всех сайтов VPN независимо от AS/SP, к которым они подключены.

6.2. Поддержка L3

За исключением IPLS, услугам L2VPN **следует** независимыми от типа абонентского трафика L3 (например, IP, IPX, Appletalk), инкапсулированного в кадры L2.

В IPLS **должна** обеспечиваться поддержка абонентского трафика IPv4 и IPv6, инкапсулированного в кадры L2. В IPLS **следует** также обеспечивать «прозрачную» передачу трафика ISIS и MPLS между CE, когда он используется с IP.

6.3. Качество обслуживания и параметры трафика

Предполагается QoS является важным параметром сервиса L2VPN для некоторых абонентов.

Абонентам нужно, чтобы служба L2VPN обеспечивала параметры QoS, подходящие для приложений, которые могут занимать диапазон от PW (например, эмуляция SONET) до голоса, интерактивного видео и multimedia-приложений. Поэтому сервис L2VPN **должен** поддерживать режим best-effort, а также чувствительный к задержкам и потерям трафик. Абонентским приложениям **следует** обеспечивать согласованные параметры QoS независимо от технологии сетей доступа на разных сайтах одной сети L2VPN.

6.4. Спецификация уровня сервиса

Большинство абонентов просто хотят нормальной работы своих приложений. SLS является средством, позволяющим абоненту оценить (измерить) качество обслуживания, предоставляемого SP. Поэтому при покупке услуг абоненту требуются от SP меры поддержки согласованных параметров SLS.

Следует предоставлять стандартные интерфейсы для мониторинга L2VPN (например, модули SNMP MIB).

6.5. Безопасность

6.5.1. Изоляция

Решение L2VPN **должно** обеспечивать изоляцию трафика а также данных пересылки для абонентов, как это делается на частных каналах, а также в сетях FR и ATM.

Сервис L2VPN **может** использовать идентификаторы абонентских VLAN в качестве указателей сервиса. В таких случаях **должна** обеспечиваться подобающая обработка идентификаторов и изоляция трафика VLAN.

6.5.2. Контроль доступа

Решение L2VPN **может** включать механизмы фильтрации по запросу абонента. Например, **может** применяться фильтрация по MAC-адресам и/или тегам VLAN между устройствами CE и PE в VPLS.

6.5.3. Добавленные услуги защиты

Решение L2VPN **может** предоставлять дополнительные услуги защиты, такие как шифрование и/или аутентификацию абонентских пакетов, управление сертификатами и т. п.

Службам L2VPN **недопустимо** конфликтовать с механизмами защиты, развёрнутыми абонентами на уровне L3 и выше. Механизмы защиты L2, такие как 802.10b ([IEEE_802.10]) и 802.1AE ([IEEE_802.1AE]) **могут** мешать службам L2VPN, когда указывающие сервис теги VLAN оказываются зашифрованными.

6.6. Доступ в сеть

Каждый пакет, передаваемый между абонентом и SP через канал доступа, **должен** выглядеть, как будто он получен из частной сети, предоставляющей услуги, эквивалентные сервису L2VPN.

6.6.1. Технология физического и канального уровня

Решениям L2VPN **следует** поддерживать широкий диапазон технологий доступа на физическом и канальном уровне, таких как PSTN, ISDN, xDSL, кабельные модемы, арендованные линии, Ethernet, Ethernet VLAN, ATM, Frame Relay,

беспроводные сети, сети сотовой связи и т. п. Пропускная способность и QoS **могут** зависеть от применяемой технологии.

6.6.2. Подключения для доступа

Должны поддерживаться разные варианты физического подключения, такие как многодомные сайты, «закулисные» (backdoor) соединения между сайтами, устройства подключённые к нескольким сетям SP. В случае VPLS **следует** поддерживать агрегирование каналов IEEE 802.3ad-2000. Решениям L2VPN **следует** поддерживать по меньшей мере подключения физического и канального уровня, показанные на рисунках 2 - 4 (в дополнение к рисунку 1). Как показано на рисунке 2, CE может иметь два подключения к одному или разным SP через разные сети доступа.

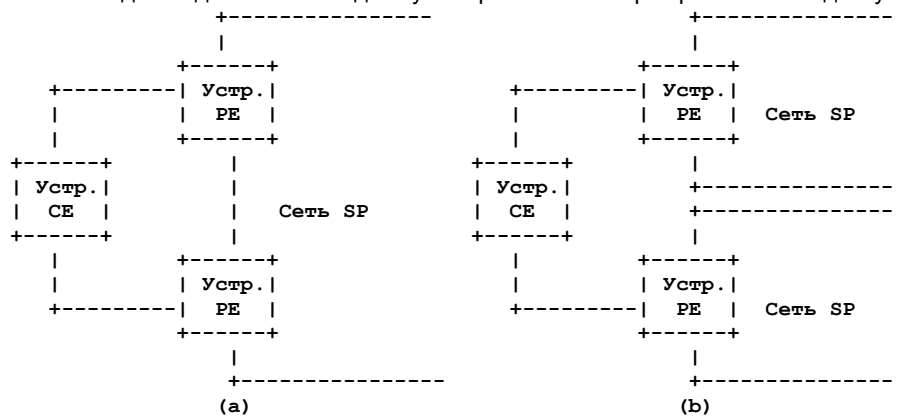

Рисунок 2. Двудомный доступ устройств CE.

Отказоустойчивость сервиса L2VPN может быть повышена дополнительно, как показано на рисунке 3, где устройства CE имеют «закулисное» соединение через одного или разных SP.

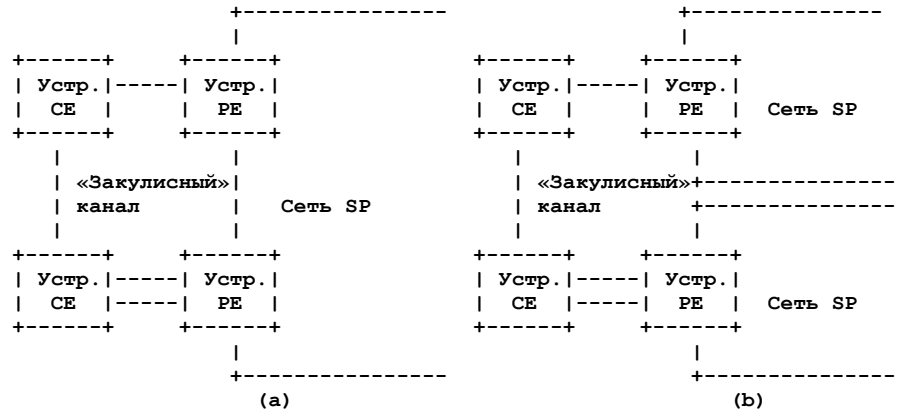

Рисунок 3. «Закулисные» соединения между CE.

Произвольные комбинации описанных методов (см. рисунок 4) **следует** поддерживать любым решениям L2VPN.

6.7. Абонентский трафик

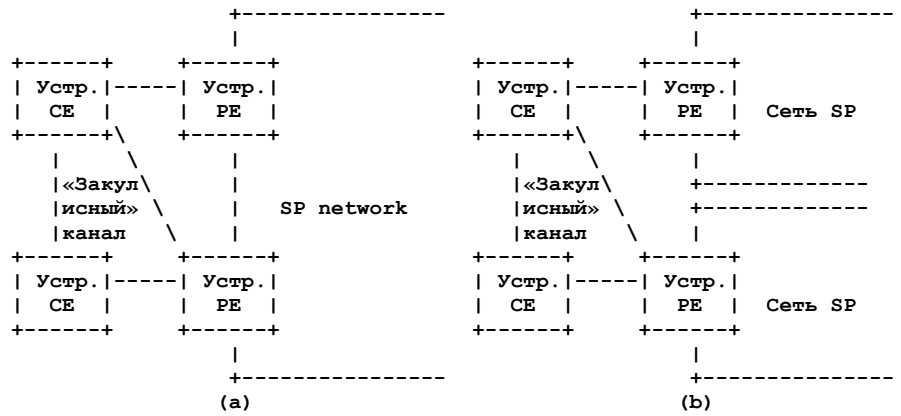

Рисунок 4. Комбинация двудомных подключений и "закулисных" каналов для CE.

6.7.1. Пересылка индивидуального, группового и широковещательного трафика

Сеть VPLS **должна** доставлять каждый пакет по меньшей мере указанным получателям в сфере действия VPLS с учётом входной политики и правил безопасности.

6.7.2. Изменение порядка пакетов

При нормальной работе механизмам постановки в очередь и правилам пересылки **следует** сохранять порядок пакетов с одинаковыми параметрами QoS.

6.7.3. Минимальное значение MTU

В VPLS **должно** поддерживаться теоретическое значение MTU предлагаемого сервиса.

Принятое минимальное значение MTU **должно** быть одинаковым в рамках экземпляра VPLS. Разные службы L2VPN **могут** иметь разные значения MTU. При использовании абонентских VLAN в качестве обозначения сервиса все VLAN в данном экземпляре VPLS **должны** наследовать общее значение MTU.

VPLS **может** применять фрагментацию IP, если на абонентских краевых устройствах VPLS будут представляться собранные пакеты.

6.7.4. Сквозная трансляция тегов VLAN

Сервис L2VPN **может** поддерживать трансляцию идентификаторов абонентских AC (например, тегов VLAN при их применении для обозначения сервиса). Такие услуги упрощают соединения между сайтами, которые хотят сохранить назначения своих AC, или сайтов, относящихся к разным административным доменам. В последнем случае соединения иногда называют L2 extranet. С другой стороны следует отметить, что трансляция тегов VLAN влияет на поддержку множества связующих деревьев (802.1s [IEEE_802.1s]) и может нарушать работу.

6.7.5. «Прозрачность»

Сервис L2VPN должен быть незаметным (прозрачным) для абонентских сетей L2. Решениям L2VPN **не следует** требовать какой-либо специальной обработки пакетов конечными пользователями перед их отправкой в сеть SP.

Если идентификаторы VLAN назначает SP, «прозрачность» VLAN не обеспечивается. Поэтому «прозрачность» в данном случае не применима, как и в модели сервиса FR/ATM.

Поскольку решение IPLS предназначено для транспортировки инкапсулированного трафика (а не кадров L2), ему **недопустимо** менять пакеты, инкапсулированные в кадры L2, которые транспортируются IPLS. Однако от решения IPLS **не требуется** сохранять заголовок L2 при передаче между устройствами CE. Например, адрес Source MAC может не сохраняться. Решение IPLS **может** удалять заголовки L2 при транспортировке через магистральную сеть и затем восстанавливать их на выходе без ущерба для транспортировки инкапсулированного трафика.

6.8. Поддержка протоколов управления L2

Решению L2VPN **следует** обеспечивать прозрачность для протоколов управления L2, используемых абонентом.

В случае VPLS сервис L2VPN **должен** гарантировать предотвращение петель. Это может обеспечиваться беспетлевой топологией или соответствующими правилами пересылки. Может также применяться протокол связующего дерева (STP[1]) или похожие протоколы. Решение L2VPN **может** использовать индикацию абонентских протоколов управления L2 (например, STP BPDU snooping) для повышения эффективности работы VPLS.

6.9. Предоставление CE

Решение L2VPN **должно** ограничиваться минимальными требованиями к настройке CE (в зависимости от типа устройства), вплоть до полного отсутствия требований к настройке CE.

7. Требования сервис-провайдера

В этом разделе рассматриваются требования с точки зрения SP.

7.1. Расширяемость

В этом параграфе рассматриваются требования к размеру и расширяемости L2VPN, а также связанные с расширяемостью показатели для отдельных решений.

7.1.1. Оценка пропускной способности сервиса

В [RFC3809] приведены требования и показатели для размера и расширяемости L2VPN, а также примеры.

7.1.2. Параметры конкретных решений

Для каждого решения L2VPN **нужен** документ с количественными характеристиками расширяемости.

7.2. Идентификаторы

Домен SP **должен** однозначно определяться по крайней мере сред всех соединённых между собой сетей SP при поддержке L2VPN через множество SP. В идеальном случае **следует** использовать уникальный в глобальном масштабе идентификатор (например, номер AS).

Для каждого экземпляра L2VPN **следует** применять уникальный по крайней мере в каждой сети SP идентификатор, поскольку он **может** применяться для автоматического обнаружения, управления (например, сопоставления сигналов и сервиса, поиск неисправностей, сбор статистики) и сигнализации. В идеальном случае **следует** использовать уникальный в глобальном масштабе идентификатор L2VPN при организации сервиса через множество SP (например, [RFC2685]). Такие идентификаторы упрощают развёртывание межпровайдерских услуг L2VPN.

7.3. Обнаружение относящейся к L2VPN информации

Настройка устройств PE (U-PE и N-PE [RFC4664]) является важной задачей SP. Решениям **следует** обеспечивать методы динамического обнаружения информации L2VPN устройствами PE для минимизации работ по настройке.

Каждому устройству в L2VPN **следует** поддерживать возможность определения других устройств, присутствующих в L2VPN. Такая схема динамического обнаружения принадлежности к сервису **должна** предотвращать несанкционированный доступ и аутентификации источников.

Распространение информации L2VPN **следует** ограничивать кругом устройств, вовлечённых в L2VPN. Решениям L2VPN **следует** поддерживать механизмы обнаружения для минимизации объёма рабочей информации,

[1]Spanning Tree Protocol - протокол связующего дерева.

поддерживаемой SP. Например, если SP добавляет или удаляет абонентский порт на устройстве PE, остальным PE **следует** самостоятельно определять требуемые в ответ действия без необходимости явной настройки этих PE.

Решениям L2VPN **следует** поддерживать для подключённых устройств CE возможность аутентифицировать друг друга и проверить корректность соединений SP L2VPN.

Механизмам **следует** своевременно реагировать на изменение членства в L2VPN. «Своевременно» в данном случае говорит о времени реакции, не превышающем время предоставления, которое обычно составляет несколько минут. Время реакции **может** быть порядка времени на перемаршрутизацию, которое обычно измеряется секундами.

Динамическое создание, изменение и поддержка множества экземпляров L2VPN и соответствующих абонентских сайтов является другим аспектом членства, которые решение L2VPN **должно** поддерживать.

7.4. Качество обслуживания (QoS)

Важным аспектом предоставляемых провайдерами VPN является поддержка QoS. SP управляет выделением ресурсов и конфигурацией параметров по меньшей мере в устройствах PE и P, а в некоторых случаях и в CE. Поэтому SP предоставляет управляемый уровень QoS при доступе или сквозной сервис QoS, как определено в [RFC4031].

7.5. Изолированный обмен данными и информацией о пересылке

С высокоуровневой точки зрения SP сервис L2VPN **должен** изолировать обмен трафиком и данными пересылки, ограничивая доступ лишь кругом сайтов, являющихся подлинными и уполномоченными участниками L2VPN.

Решениям L2VPN **следует** предоставлять средства для выполнения требований QoS SLS к предоставляемым провайдером VPN, которые изолируют трафик L2VPN от воздействия трафика не относящихся к VPN абонентов. решению L2VPN **следует** также обеспечивать средства, предотвращающие влияние перегрузки в одном экземпляре L2VPN на другие L2VPN.

7.6. Безопасность

Требования безопасности описаны в параграфе 6.5. **Следует** соблюдать требования безопасности, указанные в [RFC3809]. **Следует** соблюдать требования безопасности, указанные в [RFC4031], исключая требования к L3 и выше.

В дополнение к этому сеть SP **должна** быть защищена от атак с некорректно сформированным и вредоносным трафиком из сетей абонентов. Это включает дубликаты или некорректные адреса L2, петли на сайтах абонентов, слишком короткие или длинные пакеты, обманные пакеты управления, обманные теги VLAN, избыточный трафик и т. п.

Недопустим доступ к устройствам сети SP из любых L2VPN без специального разрешения. Устройствам в сети SP **следует** поддерживать те или иные методы информирования о попытках вторжения в сет SP при обнаружении таких вторжений.

Когда решение L2VPN работает частично через Internet, следует обеспечивать конфигурационные опции для поддержки одного или нескольких перечисленных ниже методов IPsec для защиты абонентского трафика VPN:

- защита конфиденциальности, позволяющая расшифровать трафик лишь уполномоченным устройствам;
- защита целостности для сохранения данных неизменными;
- проверка подлинности отправителей;
- защита от атак с повторным использованием пакетов.

Перечисленным выше функциям **следует** быть применимыми к трафику данных абонента, включающему обмен данными между сайтами. **Следует** также иметь возможность применения этих функций к трафику управления, такому как протоколы маршрутизации и сигнализации, который не обязательно воспринимается непосредственно клиентами, но нужен для поддержки VPN.

Эти такие защиты **должны** настраиваемыми между парами конечных точек, такими как PE-PE и PE-MTU при передаче трафика данных L2VPN по протоколу IP [RFC4023]. Методы защиты потоков данных на естественном уровне сервиса (L2) в парах CE-CE, CE-MTU и CE-PE выходят за рамки этого документа. Желательно также обеспечивать настройку защиты на уровне VPN.

Решение VPN **может** поддерживать одну или несколько схем шифрования, включая AES и 3DES. Шифрование, дешифрование и распространение ключей **следует** включать в профили как часть системы управления безопасностью.

7.7. Межпровайдерские L2VPN

Все применимые требования SP, такие как изоляцию трафика и данных пересылки, SLS, управление, безопасность, предоставления и т. п., **должны** сохраняться для смежных AS. Решение **должно** отписывать сетевой интерфейс между SP, методы инкапсуляции, протоколы маршрутизации и другие применимые параметры.

Решение L2VPN **должно** выполнять требования конкретных услуг L2VPN, организуемых через несколько AS и/или SP.

Решение L2VPN **должно** поддерживать распространение пригодных рабочих параметров всем элементам сервиса L2VPN при наличии множества AS и/или SP. Решение L2VPN **должно** реализовать механизмы совместного использования рабочих параметров в разных AS.

Решениям L2VPN **следует** поддерживать правила для подобающего выбора рабочих параметров, приходящих из разных AS. Аналогично, решениям L2VPN **следует** поддерживать правила для выбора информации, распространяемой в разные AS.

7.7.1. Управление

Общие требования для управления в одной AS применимы и для случая нескольких AS. Минимальный набор обеспечиваемых возможностей должен включать:

- средства диагностики;
- защищённый доступ к системе управления одной AS из других;
- средства запроса конфигурации и состояния;
- уведомления об отказах и средства поиска неисправностей.

7.7.2. Запросы пропускной способности и QoS

При организации L2VPN через несколько AS требуется механизм-посредник (брокер) для запроса некоторых параметров SLS (таких, как пропускная способность и QoS) в других доменах и сетях, вовлечённых в передачу трафика на разные сайты. Важно отметить, что решение **должно** быть способно определить, может ли множество вовлечённых AS организовать и гарантировать однородные параметры QoS для поддержки предоставляемой VPN.

7.8. «Оптовые» услуги L2VPN

Архитектура **должна** поддерживать возможность предоставления одним SP услуг L2VPN для других SP. Например, один SP продаёт сервис L2VPN «оптом» другому SP, которые может перепродать их своим абонентам.

7.9. Требования к туннелированию

Соединениям между CE на сайтах и PE в магистрали **следует** поддерживать возможность использования разных технологий туннелирования, таких как L2TP, GRE, IP-in-IP, MPLS и т. п.

Каждое устройство PE **должно** поддерживать протокол организации туннелей, если туннели применяются. PE **может** поддерживать статическую настройку туннелей. Если используется протокол организации туннелей, ему **следует** обеспечивать возможность переноса указанной ниже информации.

- Относящиеся к делу идентификаторы.
- Параметры QoS/SLS.
- Параметры восстановления.
- Идентификаторы мультиплексирования.
- Параметры безопасности.

Должны обеспечиваться средства мониторинга перечисленных ниже аспектов туннелей.

- Статистика (такая как время в активном и отключённом состоянии).
- Счётчик переходов из активного в неактивное состояние и обратно.
- События (такие как переходы между активным и неактивным состоянием).

Технология туннелирования, применяемая VPN SP и связанные с ней механизмы организации, мультиплексирования и поддержки туннелей **должны** удовлетворять требованиям к расширяемости, изоляции, безопасности, QoS, управляемости и т. п.

Независимо от выбранного способа туннелирования наличие туннелей и их работа **должны** быть незаметны для абонентов.

7.10. Поддержка технологий доступа

Соединения между устройствами PE и CE называются AC и **могут** проходить через сети других провайдеров и сети общего пользования.

Имеется несколько вариантов реализации AC, среди которых наиболее популярны Ethernet, ATM (DSL), Frame Relay, виртуальные каналы на базе MPLS и т. п.

В случае VPLS устройства AC **должны** использовать кадры Ethernet в качестве блоков данных сервиса (SPDU).

Подключение CE через AC **должно** быть двухсторонним.

Устройства PE **могут** поддерживать множество AC на одном физическом интерфейсе. В таких случаях устройствам PE **недопустимо** различать соединения на основе управляемых абонентом параметров. Например, если для этого применяются теги VLAN, провайдер должен контролировать назначение тегов и строго проверять их соответствие на устройствах CE.

Устройство AC (физическое или виртуальное) **должно** поддерживать все заявленные характеристики абонентского трафика, такие как QoS, приоритет и пр. Характеристики AC применимы лишь к данному соединению.

7.11. Магистральные сети

В идеале соединениям в сети SP между устройствами PE и P **следует** быть независимыми от технологии физического и канального уровня. В любом случае характеристики магистральной технологии **должны** приниматься во внимание при задании аспектов QoS в спецификациях SLS для предлагаемых услуг VPN.

7.12. Разделение и совместное использование ресурсов сети разными L2VPN

Если сетевые ресурсы - памяти, таблицы данных пересылки, пропускная способность, обработка в CPU совместно используются несколькими L2VPN, решению **следует** предотвращать захват ресурсов любым экземпляром L2VPN, препятствующий получению ресурсов другими экземплярами или вызывающий их отказы. Решению **следует** поддерживать возможность ограничения ресурсов, потребляемых экземпляром L2VPN, а также **следует** гарантировать доступность ресурсов, требуемых для выполнения согласованной спецификации SLS.

7.13. Совместимость

Сервис-провайдеры заинтересованы в обеспечении совместимости по меньшей мере для перечисленных вариантов:

- упрощение использования PE и управляемых CE в одной сети SP;
- реализация услуг L2VPN через несколько сетей SP;
- обеспечение совместной работы и связности между сайтами абонента, использующими разные решения L2VPN или разные реализации одной модели.

Каждая модель **должна** указывать, какие из перечисленных целей она может поддерживать. Если та или иная задача решается, модель **должна** описывать способы достижения совместимости.

7.14. Тестирование

Решениям L2VPN **следует** поддерживать возможность тестирования и проверки работы и управления на уровне экземпляра L2VPN, а в случае VPLS - на уровне VLAN, если абонентские VLAN служат обозначением сервиса.

Механизмам L2VPN **следует** поддерживать механизмы проверки связности, а также детектирования и поиска отказов.

Примерами механизмов тестирования являются:

- проверка связности между знающими о сервисе (service-aware) узлами сети;
- проверка целостности уровней данных и управления;
- проверка членства для сервиса.

Предоставляемые механизмы **должны** удовлетворять следующие требования: проверка связности для абонента **должна** позволять сквозное тестирование пути передачи абонентских пакетов и тестовые пакеты **должны** распространяться, не выходя за пределы сети SP.

7.15. Поддержка имеющихся PE

Насколько это возможно, решениям IPLS **следует** упрощать поддержку IPLS на имеющихся устройствах PE, которые уже могли быть развёрнуты SP, и **может** быть разработана прежде всего для услуг L3.

8. Требования SP к управлению

SP нужны средства для просмотра топологии, рабочего состояния и других параметров, связанных с экземплярами абонентских L2VPN. Кроме того, SP нужны средства для просмотра базовой физической и логической топологии, рабочего состояния, статуса предоставления и других параметров, связанных с оборудованием, обеспечивающим сервис L2VPN для абонентов. Поэтому устройствам **следует** по возможности поддерживать стандартные интерфейсы (например, модули L2VPN MIB).

Детали требований сервис-провайдеров к системам сетевого управления (NMS[1]) в традиционных категориях настройки, контроля отказов, учёта, производительности и безопасности (FCAPS[2]) приведены в [ITU_Y.1311.1].

9. Инженерные требования

Эти требования определяются характеристиками реализации, которые делают достижимыми требования сервиса и SP.

9.1. Требования к уровню управления

Сервису L2VPN **следует** требовать для предоставления небольшого числа шагов. Поэтому протоколам управления **следует** обеспечивать методы сигнализации между PE. Сигналам **следует** передавать информацию о членстве, туннелировании и других параметрах, относящихся к делу.

Инфраструктура **может** реализовать методы ручной настройки для предоставления этого типа информации.

Инфраструктуре **следует** применять правила для области действия членства и доступности анонсов конкретного сервиса L2VPN. **Должен** обеспечиваться механизм для изоляции распространения информации о доступности лишь кругом сайтов, связанных с L2VPN.

Трафик на уровне управления растёт по мере увеличения числа членов L2VPN, а также по мере роста числа экземпляров L2VPN. Загрузка ресурсов на уровне управления **может** увеличиваться при добавлении хостов в L2VPN.

Решению L2VPN **следует** минимизировать трафик и потребление ресурсов на уровне управления. **Можно** предлагать на уровне управления средства ограничения числа хостов, подключённых к сервису L2VPN.

9.2. Требования к уровню данных

9.2.1. Инкапсуляция

Решениям L2VPN **следует** применять методы инкапсуляции, определённые PWE3 ([RFC3985]), и не **следует** вносить новых требований к этим методам.

9.2.2. Отклики на перегрузку

Решениям L2VPN **следует** применять методы предотвращения перегрузок, определённые PWE3 ([RFC3985]).

[1]Network Management System.
[2]Fault, configuration, accounting, performance, and security.

9.2.3. Область широковещания

Должна поддерживаться отдельная область широковещания (Broadcast Domain) для каждой сети VPLS.

В дополнение к доменам широковещания VPLS решение L2VPN **может** поддерживать абонентские области широковещания VLAN, если абонентские VLAN служат обозначением сервиса. В этом случае решению L2VPN **следует** поддерживать отдельные домены широковещания для всех VLAN абонента.

9.2.4. Экземпляры виртуальных коммутаторов

В L2VPN устройства PE **должны** поддерживать отдельный коммутатор VSI[1] для каждой сети VPLS. Каждый VSI должен быть способен пересылать кадры на основе параметров абонентского трафика, таких как MAC-адреса, теги VLAN (при использовании) и т. п, в соответствии с локальными правилами с учётом локальных правил.

Устройства L2VPN PE **должны** иметь возможность распределять входящий абонентский трафик по VSI.

Каждый экземпляр VSI **должен** поддерживать лавинную рассылку в свой домен широковещания для упрощения подобающей пересылки абонентского трафика с широковещательными, групповыми и неизвестными индивидуальными адресами получателей.

9.2.5. Изучение MAC-адресов

VPLS **следует** получать данные о топологии и пересылке из пакетов с абонентских сайтов, для чего обычно служит изучение MAC-адресов. В IPLS может также применяться отслеживание определённых пакетов и сигнализация.

Динамическое заполнение таблиц пересылки (например, путём изучения MAC-адресов) **должно** выполняться на уровне VSI, т. е. в контексте VPLS и VLAN (при использовании последних).

10. Вопросы безопасности

Вопросы безопасности возникают на разных уровнях L2VPN, как указано в этом документе.

Требования, основанные на вопросах безопасности и возможных угрозах описаны в параграфе 6.5. Дополнительные требования для абонентов и сервис-провайдеров рассмотрены в параграфах 6.5 и 7.6, соответственно. Требования к изоляции трафика и маршрутной информации рассмотрены в параграфах 5.4 и 7.5. Меры защиты сетевых ресурсов, таких как память, CPU, пропускная способность, рассмотрены в параграфе 7.12.

Для обеспечения дополнительной защиты можно использовать IPsec после туннелирования трафика L2.

В случаях, когда сервис L2VPN работает на основе IP [RFC4023] через несколько сетей SP с передачей через незащищённые SP, POP, NAP или IX, **должны** обеспечиваться механизмы защиты, включая шифрование, проверку подлинности и защиту ресурсов, как описано в параграфе 5.5. Например, провайдеру следует рассмотреть использование шифрования и аутентификации для туннеля, служащего частью L2VPN и проходящего через сеть другого провайдера.

11. Благодарности

Авторы благодарны за комментарии и предложения Loa Andersson, Joel Halpern, Eric Rosen, Ali Sajassi, Muneyoshi Suzuki, Ananth Nagarajan, Dinesh Mohan, Yakov Rekhter, Matt Squire, Norm Finn, Scott Bradner и Francois Le Faucheur. Хотелось бы также выразить признательность своим работодателям и другим людям, которые ознакомились с этой работой и предоставили свои отзывы. В работе принимала участие вся команда L2 PPVPN. Значительная часть текста этого документа заимствована из документа с требованиями L3 VPN, разработанного одноимённой командой.

12. Литература

12.1. Нормативные документы

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

[RFC4026] Andersson, L. and T. Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology", RFC 4026, March 2005.

12.2. Дополнительная литература

[VPLS_LDP] Lasserre, M., Kompella, V. "Virtual Private LAN Services over MPLS", Work in Progress[2].

[VPLS_BGP] Kompella, K., Rekhter, Y. "Virtual Private LAN Service", Work in Progress[3].

[IPLS] Shah, H., et al. "IP-Only LAN Service (IPLS)", Work in Progress[4].

[IEEE_802.1Q] IEEE Std 802.1Q-1998, "Virtual Bridged Local Area Networks", 1998

[RFC2205] Braden, R., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification", RFC 2205, September 1997.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[RFC2685] Fox, B. and B. Gleeson, "Virtual Private Networks Identifier", RFC 2685, September 1999.

[RFC3270] Le Faucheur, F., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P., and J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services", RFC 3270, May 2002.

[1]Virtual Switching Instance - экземпляр виртуального коммутатора.
[2]Работа опубликована в RFC 4762. *Прим. перев.*
[3]Работа опубликована в RFC 4761. *Прим. перев.*
[4]Работа опубликована в RFC 7436. *Прим. перев.*

[RFC3308] Calhoun, P., Luo, W., McPherson, D., and K. Peirce, "Layer Two Tunneling Protocol (L2TP) Differentiated Services Extension", RFC 3308, November 2002.

[RFC3809] Nagarajan, A., "Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN)", RFC 3809, June 2004.

[RFC3985] Bryant, S. and P. Pate, "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", RFC 3985, March 2005.

[RFC4023] Worster, T., Rekhter, Y., and E. Rosen, "Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)", RFC 4023, March 2005.

[RFC4031] Carugi, M. and D. McDysan, "Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks (PPVPNs)", RFC 4031, April 2005.

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

[IEEE_802.1D] ISO/IEC 15802-3: 1998 ANSI/IEEE Std 802.1D, 1998 Edition (Revision and redesignation of ISO/IEC 10038:98), "Part 3: Media Access Control (MAC) Bridges", 1998.

[ITU_Y.1311.1] Carugi, M. (editor), "Network Based IP VPN over MPLS architecture",Y.1311.1 ITU-T Recommendation, May 2001.

[IEEE_802.10] EEE Std 802.10-1998 Edition (Revision IEEE Std 802.10-1992, incorporating IEEE Std 802.10b-1992, 802.10e-1993, 802.10f-1993, 802.10g-1995, and 802.10h-1997), "Standard for Interoperable LAN/MAN Security (SILS)", 1998.

[IEEE_802.1AE] IEEE 802.1AE/D5.1, "Draft Standard for Local and Metropolitan Area Networks - Media Access Control (MAC) Security", P802.1AE/D5.1, January 19, 2006.

[IEEE_802.1s] IEEE Std 802.1s-2002, "Virtual Bridged Local Area Networks-Amendment 3: Multiple Spanning Trees", 2002.

Адреса авторов

Waldemar Augustyn
EMail: waldemar@wdmsys.com

Yetik Serbest
AT&T Labs
9505 Arboretum Blvd.
Austin, TX 78759
EMail: yetik_serbest@labs.att.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Интеллектуальная собственность

Подтверждение

Финансирование функций RFC Editor обеспечено IETF Administrative Support Activity (IASA).