

## Provider Provisioned Virtual Private Network (VPN) Terminology

### Терминология для предоставляемых провайдером VPN

#### Статус документа

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

#### Авторские права

Copyright (C) The Internet Society (2005).

#### Аннотация

Широкий интерес к предоставляемым провайдерами решениям для виртуальных частных сетей (VPN<sup>1</sup>) привёл к появлению документов, предлагающих различные и перекрывающиеся решения. Рабочие группы IETF (сначала PPVPN<sup>2</sup>, затем L2VPN<sup>3</sup> и L3VPN<sup>4</sup>) обсудили эти предложения и документированные спецификации. Это привело к разработке отчасти нового набора концепций, используемых для описания множества услуг VPN.

В той или иной степени несколько терминов используется для обозначения одного понятия, а иногда один термин применяется для разных понятий. Этот документ стремится сделать терминологию в данной области более чёткой и интуитивно понятной.

## Оглавление

1. Введение.....	2
2. Терминология PPVPN.....	2
3. Предоставляемые провайдером услуги VPN.....	2
3.1. L3VPN.....	3
3.2. L2VPN.....	3
3.3. VPLS.....	3
3.4. VPWS.....	3
3.5. IPLS.....	3
3.6. PW.....	3
3.7. TLS.....	3
3.8. VLAN.....	3
3.9. VLLS.....	3
3.10. VPN.....	4
3.11. VPSN.....	4
4. Классификация VPN.....	4
5. Компоненты сервиса.....	4
5.1. Абонентские краевые устройства (CE).....	4
5.1.1. Именованное CE по типу устройства.....	5
5.1.1.1. Граничный маршрутизатор абонента (CE-R).....	5
5.1.1.2. Граничный коммутатор абонента (CE-S).....	5
5.1.2. Именованное CE по услугам.....	5
5.1.2.1. L3VPN-CE.....	5
5.1.2.2. VPLS-CE.....	5
5.1.2.3. VPWS-CE.....	5
5.2. Граничные устройства провайдера (PE).....	5
5.2.1. Именованное PE по типу устройства.....	5
5.2.1.1. Граничный маршрутизатор провайдера (PE-R).....	5
5.2.1.2. Граничный коммутатор провайдера (PE-S).....	5
5.2.2. Именованное PE по услугам.....	5
5.2.2.1. L3VPN-PE.....	5
5.2.2.2. VPWS-PE.....	5
5.2.2.3. VPLS-PE.....	6
5.2.3. Именованное PE по месту размещения.....	6
5.2.3.1. Обращенное к сети устройство (N-PE).....	6
5.2.3.2. Общественное к клиенту устройство PE (U-PE).....	6
5.3. Ядро сети.....	6
5.3.1. Маршрутизатор провайдера (P).....	6
5.4. Именованное в отдельных документах Internet Draft.....	6
5.4.1. PE канального уровня (L2PE).....	6

<sup>1</sup>Virtual Private Network.

<sup>2</sup>Provider Provisioned VPNs - предоставляемые провайдерами VPN.

<sup>3</sup>Layer 2 VPNs - VPN канального уровня.

<sup>4</sup>Layer 3 VPNs - VPN сетевого уровня.

5.4.2. Логическое устройство PE (LPE).....	6
5.4.3. PE-CLE.....	6
5.4.4. PE-Core.....	6
5.4.5. PE-Edge.....	6
5.4.6. PE-POP.....	6
5.4.7. Краевое устройство VPLS (VE).....	6
6. Функции.....	6
6.1. Устройство присоединения (AC).....	6
6.2. Backdoor Link.....	7
6.3. Обнаружение конечных точек.....	7
6.4. Лавинная рассылка.....	7
6.5. Изучение MAC-адресов.....	7
6.5.1. Квалифицированное обучение.....	7
6.5.2. Неквалифицированное обучение.....	7
6.6. Сигнализация.....	7
7. Физические устройства.....	7
7.1. Устройство агрегирования.....	7
7.2. Абонентское оборудование (CPE).....	7
7.3. MTU.....	7
8. Сети с коммутацией пакетов (PSN).....	7
8.1. Отличие маршрута (RD).....	7
8.2. Рефлектор маршрутов.....	8
8.3. Цель маршрута (RT).....	8
8.4. Туннель.....	8
8.5. Туннельный мультиплексор.....	8
8.6. Виртуальный канал (VC).....	8
8.7. Метка VC.....	8
8.8. Внутренняя метка.....	8
8.9. Маршрутизация и пересылка VPN (VRF).....	8
8.10. Экземпляр пересылки VPN (VFI).....	8
8.11. Экземпляр виртуального коммутатора (VSI).....	8
8.12. Виртуальный маршрутизатор (VR).....	8
9. Вопросы безопасности.....	9
10. Благодарности.....	9
11. Литература.....	9
Адреса авторов.....	9
Полное заявление авторских прав.....	10

## 1. Введение

В бывшую рабочую группу PPVPN, а затем в группы L2VPN, L3VPN и PWE3 было представлено довольно большое число документов, решающих задачи из одной области - предоставления провайдерами виртуальных частных сетей для своих абонентов. Документы были связаны с широким спектром услуг, но среди предложенных решений было много общего.

Это привело к разработке частичного набора новых понятий, применяемых для описания множества услуг VPN. В той или иной степени несколько терминов используется для обозначения одного понятия, а иногда один термин применяется для разных понятий.

Этот документ предлагает основу для унифицированной терминологии рабочим группам L2VPN и L3VPN. В некоторых случаях близкие концепции рабочей группы PWE3 использованы как ссылки.

## 2. Терминология PPVPN

Концепции и термины в рассмотренном ниже списке собраны из документов Internet Draft, присланных в почтовые конференции L2VPN и L3VPN (ранее в PPVPN), и RFC, относящихся к рабочим группам L2VPN и L3VPN. Основное внимание уделяется терминам и понятиям, относящимся к PPVPN, но это не соблюдается строго. Например, некоторые понятия и термины в областях PWE3 и (G)MPLS тесно связаны с рассматриваемой темой. Авторы пытались найти истоки терминов и понятий.

Документ рассчитан на полный охват концепций основных документов рабочих групп L2VPN и L3VPN, т. е. [L3VPN-REQ], [L2VPN-REQ], [L3VPN-FRAME], [L2VPN] и [RFC3809]. Цель заключается в создании полного и унифицированного набора понятий для этих документов и, как следствие, всей области PPVPN. Для этого нужно рассмотреть аспекты разработки концепций.

Документ разбит на 4 основных раздела. В разделе 4 рассмотрены различные услуги, которые описаны или будут описаны, в разделе 5 описаны компоненты, используемые для спецификации этих услуг, а в разделе 6 перечислены требуемые для услуг функции. В разделе 7 рассмотрены некоторые типовые устройства, используемые в сетях абонентов и провайдеров.

## 3. Предоставляемые провайдером услуги VPN

В этом разделе определяется терминология, связанная с набором услуг, заданным рабочими группами L2VPN и L3VPN. Понятие «псевдопровода» относится к рабочей группе PWE3 и включено для справки. Требования к предоставляемым провайдерами VPN заданы в [L3VPN-REQ].

Все приведённые термины и сокращения снабжены кратким описанием сервиса. Список структурирован и сначала представлена наиболее общая информация. Имена служб, над которыми работает IETF помещены в начало списка, а более старые термины - в конец.

### 3.1. L3VPN

L3VPN<sup>1</sup> соединяет множество хостов и маршрутизаторов на основе адресов L3, как описано в [L3VPN-FRAME].

### 3.2. L2VPN

В этом документе описаны три типа L2VPN<sup>2</sup> - виртуальные частные провода - VPWS<sup>3</sup> (параграф 3.4), виртуальные частные ЛВС - VPLS<sup>4</sup> (параграф 3.3) и услуги ЛВС для протокола IP - IPLS<sup>5</sup> (параграф 3.5).

### 3.3. VPLS

VPLS представляет собой услугу провайдера, эмулирующую полную функциональность традиционной ЛВС. VPLS позволяет соединить несколько сегментов ЛВС через сеть с коммутацией пакетов (PSN<sup>6</sup>) и позволяет удаленным сегментам вести себя как часть единой ЛВС. Первыми работами, определившими решение и протокол для VPLS были [L2VPN-REQ], [VPLS-LDP] и [VPLS].

В VPLS сеть провайдера эмулирует обучающийся мост и решения о пересылке принимаются на основе MAC-адреса или MAC-адреса и тега VLAN.

### 3.4. VPWS

VPWS представляет собой устройство (канал) «точка-точка», соединяющее два граничных устройства клиента (CE<sup>7</sup>). Канал является логическим и организуется через сеть с коммутацией пакетов. CE в сети абонента соединяется с PE<sup>8</sup> в сети провайдера через устройство присоединения - AC<sup>9</sup> (параграф 6.1), которое может быть логическим или физическим.

Устройства PE в ядре сети соединяются псевдопроводом - PW<sup>10</sup>.

Устройствами CE могут быть маршрутизаторы, мосты, коммутаторы или хосты. В некоторых реализациях набор VPWS служит для создания многосайтовой сети L2VPN. Пример решения VPWS представлен в [PPVPN-L2VPN].

VPWS отличается от VPLS (параграф 3.3) в том, что VPLS имеет многоточечную структуру (point to multipoint), а VPWS - структуру «точка-точка» (см. [L2VPN]).

### 3.5. IPLS

Сервис IPLS очень похож на VPLS (параграф 3.3), за исключением перечисленных ниже отличий.

- Предполагается что устройствами CE (параграф 5.1) служат хосты или маршрутизаторы, но не коммутаторы.
- Предполагается, что сервис будет применяться только для пакетов IP и протоколов поддержки, таких как ICMP и ARP (кадры L2, содержащие другие протоколы, не поддерживаются).
- К пакетам IP относятся пакеты IPv4 и IPv6.

Хотя этот сервис является функциональным подмножеством VPLS, он рассматривается отдельно, поскольку может поддерживаться на основе других механизмов, что позволяет реализовать сервис на некоторых аппаратных платформах не поддерживающих полную функциональность VPLS [L2VPN].

### 3.6. PW

Рабочая группа IETF PWE3 создала спецификации псевдопроводов, которые представляют собой эмулируемые соединения «точка-точка» через сеть с коммутацией пакетов и позволяют соединить пару узлов с любой технологией L2. PW используют некоторые общие компоненты и архитектурные конструкции с решениями «точка-множество точек», например, PE (параграф 5.2) и CE (параграф 5.1). Первое решение для PW предложено в [TRANS-MPLS]. Форматы инкапсуляции используемые в VPWS, VPLS и PW, описаны в [ENCAP-MPLS]. Требования к PW представлены в [RFC3916], а в работе [PWE3-ARCH] описана архитектурная модель PW.

### 3.7. TLS

Обозначение TLS<sup>11</sup> изначально применялось для сервиса VPLS, но сейчас от него отказались.

### 3.8. VLAN

Термин VLAN<sup>12</sup> был введён стандартом IEEE 802.1Q и обозначает метод разделения трафика ЛВС путём размещения специальных меток (тегов) в кадрах Ethernet. В расширенном смысле термин VLAN используется для обозначения трафика, разделяемого с помощью тегов Ethernet или похожих механизмов.

### 3.9. VLLS

Термин VLLS<sup>13</sup> был заменён термином VPWS. Обозначение VLLS использовалось в устаревшем документе по созданию метрик, позволяющих сравнивать различные решения L2VPN, работа над которым была прервана.

<sup>1</sup>Layer 3 VPN - услуги VPN на сетевом уровне.

<sup>2</sup>Layer 2 VPN - услуги VPN на канальном уровне.

<sup>3</sup>Virtual Private Wire Service.

<sup>4</sup>Virtual Private LAN Service.

<sup>5</sup>IP-only LAN-like Service.

<sup>6</sup>Packet switched network.

<sup>7</sup>Customer Edge.

<sup>8</sup>Provider Edge.

<sup>9</sup>Attachment Circuit.

<sup>10</sup>Pseudowire.

<sup>11</sup>Transparent LAN Service - «прозрачные» услуги ЛВС.

<sup>12</sup>Virtual LAN - виртуальная ЛВС.

<sup>13</sup>Virtual Leased Line Service - услуги виртуальной арендованной линии.

### 3.10. VPN

Термин VPN является базовым обозначением публичных и частных виртуальных сетей для групп пользователей, отделённых от других пользователей сети, которые могут взаимодействовать между собой как будто в частной сети. Уровень разделения пользователей можно повысить (например, с помощью сквозного шифрования), но это выходит за рамки задач рабочей группы IETF VPN. Определение VPN заимствовано из [RFC2764].

В работе [L3VPN-FRAME] термин VPN обозначает конкретный набор сайтов как сеть intranet или extranet, которая может быть настроена для взаимодействия. Отметим, что сайт входит по крайней мере в одну сеть VPN и может участвовать во множестве сетей.

В этом документе термин VPN служит также базовым обозначением всех типов сервиса, перечисленных в разделе 3.

### 3.11. VPSN

Термин VPSN<sup>1</sup> заменён термином VPLS. Требования к сервису были собраны из требований к L3VPN [L3VPN-REQ] и L2VPN [L2VPN-REQ].

## 4. Классификация VPN

Терминология в [RFC3809] определена на основе рисунка 1.

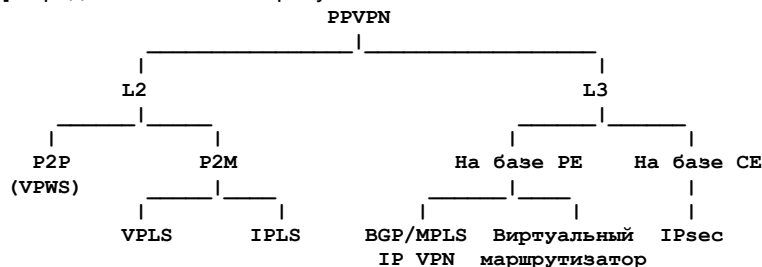


Рисунок 1.

На рисунке 1 представлена систематика технологий PPVPN, а ниже приведены некоторые определения.

#### CE-based VPN - VPN на основе CE

Подход к организации VPN, при котором сеть провайдера не знает об абонентских VPN, которые известны лишь устройствам CE. Все связанные с VPN процедуры выполняются на устройствах CE, а PE ничего не знают о принадлежности трафика к VPN (см. также [L3VPN-FRAME]).

#### PE-Based VPNs - сети VPN на основе PE

Модель L3 VPN, в которой сеть сервис-провайдера служит для соединения сайтов абонента с использованием общих ресурсов. В частности, устройства PE поддерживают состояние VPN и изолируют пользователей одной сети VPN от пользователей других сетей. Поскольку все требуемые для VPN состояния поддерживаются в PE, устройства CE могут вести себя как при подключении к частной сети. В частности, на устройствах CE в сети VPN на основе PE не требуется вносить каких-либо изменений или расширять функциональность при подключении к PPVPN вместо частной сети.

Устройства PE знают, что часть трафика относится к VPN и пересылают трафик (через туннели) по IP-адресам получателей и могут учитывать при пересылке другую информацию из заголовка IP в пакете. Конечными точками туннелей являются устройства PE. Для туннелей может применяться разная инкапсуляция при пересылке через сеть SP (например, туннели GRE, IP-in-IP, IPsec, MPLS) [L3VPN-FRAME].

#### Virtual Router (VR) style - виртуальные маршрутизаторы

Основанная на PE модель VPN, где маршрутизатор PE поддерживает полнофункциональный логический маршрутизатор для каждой обслуживаемой им сети VPN. Каждый логический маршрутизатор поддерживает уникальную таблицу пересылки и свои экземпляры протоколов маршрутизации. Этот тип VPN описан в [L3VPN-VR].

#### BGP/MPLS IP VPNs - сети IP VPN на основе BGP/MPLS

Основанная на PE модель VPN, где маршрутизатор PE поддерживает отдельную среду пересылки и таблицу пересылки для каждой сети VPN. Для поддержки множества экземпляров таблиц пересылки при использовании единственного экземпляра BGP анонсы маршрутов в BGP/MPLS IP VPN помечаются атрибутами, указывающими контекст VPN. Это решение VPN основано на подходе, описанном в [RFC2547bis].

#### RFC 2547 Style - стиль RFC 2547

Этот термин применялся в L3VPN для описания расширений для VPN, определённых в информационном RFC 2547 [RFC2547]. Сейчас взамен применяется термин BGP/MPLS IP VPN.

## 5. Компоненты сервиса

Начиная со спецификаций L3VPN (например, [RFC2547] и [RFC2547bis], а также [L3VPN-VR]), был разработан способ описания компонентов и распределения функций в решениях VPN. В повседневных разговорах о компонентах говорят, как будто они являются физическими устройствами, общими для всех типов сервиса.

Однако по разным причинам это является чрезмерным упрощением. Любые компоненты могут быть реализованы в нескольких физических устройствах. Рассмотрение общности таких реализаций выходит за рамки этого документа.

### 5.1. Абонентские краевые устройства (CE)

Абонентское граничное устройство CE представляет собой устройство, функциональность которого нужна на площадке абонента для доступа к услугам, заданным бывшей рабочей группой PPVPN, применительно к L3VPN [L3VPN-FRAME]. Концепция была изменена при определении L2VPN и VPN на основе CE. Об этом подробнее сказано ниже.

<sup>1</sup>Virtual Private Switched Network - виртуальная частная коммутируемая сеть.

Имеется два разных аспекта именованя устройств CE. Можно начать с типа устройства, служащего для реализации CE (параграф 5.1.1), а можно использовать предоставляемую CE услугу, в результате чего будут получены CE с префиксами (параграф 5.1.2).

Обычно термин CE применяют для всех таких устройств, поскольку контекст обычно позволяет устранить неоднозначность.

### **5.1.1. Именованне CE по типу устройства**

#### **5.1.1.1. Граничный маршрутизатор абонента (CE-R)**

CE-R<sup>1</sup> является маршрутизатором в сети абонента, взаимодействующим с сетью провайдера. Имеется много причин применения маршрутизатора в сети клиента, например при использовании приватных адресов IP для L3VPN этот маршрутизатор сможет обеспечить пересылку на основе приватных адресов IP. Другой причиной может служить желание ограничить число MAC-адресов, которые нужно знать в сети провайдера.

Устройства CE-R могут применяться для сервиса L2 и L3.

#### **5.1.1.2. Граничный коммутатор абонента (CE-S)**

CE-S<sup>2</sup> - это осведомлённый о сервисе VPN коммутатор L2 в сети абонента, взаимодействующий с сетью провайдера. В службах VPWS и VPLS не обязательно применять в сети абонента граничный маршрутизатор, поскольку с задачами может справиться коммутатор L2.

### **5.1.2. Именованне CE по услугам**

Ниже рассмотрены примеры использования функциональности для именованя устройств CE. Существует много примеров такого именованя и здесь рассмотрены лишь наиболее распространённые функциональные имена. Поскольку имена являются функциональными, вполне возможно наличие в одном физическом устройстве платформ с разными типами функций. Например, маршрутизатор может одновременно играть роли L2VPN-CE и L3VPN-CE. Возможно также разделение функций, требуемых для L2VPN-CE или L3VPN-CE между несколькими платформами.

#### **5.1.2.1. L3VPN-CE**

L3VPN-CE - это устройство или набор устройств на площадке абонента, которые служат для подключения к предоставляемому провайдером сервису L3VPN, например, реализация RFC 2547bis.

#### **5.1.2.2. VPLS-CE**

VPLS-CE - это устройство или набор устройств на площадке абонента, которые служат для подключения к предоставляемому провайдером сервису VPLS.

#### **5.1.2.3. VPWS-CE**

VPWS-CE - это устройство или набор устройств на площадке абонента, которые служат для подключения к предоставляемому провайдером сервису VPWS.

## **5.2. Граничные устройства провайдера (PE)**

Термином PE обозначают устройство или набор устройств на границе сети провайдера, функциональность которых обеспечивает интерфейс с абонентами. Термин PE часто используется без уточнения типа устройства, понятного из контекста.

При именовании PE следует учитывать три аспекта - тип поддерживаемого сервиса, возможность распределения функциональности между несколькими устройствами и тип устройства.

### **5.2.1. Именованне PE по типу устройства**

Для реализации функций PE могут применяться коммутаторы и маршрутизаторы, однако возможности расширения сервиса кардинально различаются в разных типах устройств.

#### **5.2.1.1. Граничный маршрутизатор провайдера (PE-R)**

PE-R<sup>3</sup> представляет собой устройство сетевого уровня (L3), участвующее в маршрутизации и пересылке пакетов PSN (раздел 8) на основе маршрутных данных.

#### **5.2.1.2. Граничный коммутатор провайдера (PE-S)**

PE-S<sup>4</sup> представляет собой устройство канального уровня (L2), которое участвует, например, в коммутации Ethernet, принимая решение о пересылке на основе адресов L2.

### **5.2.2. Именованне PE по услугам**

#### **5.2.2.1. L3VPN-PE**

L3VPN-PE - устройство или набор устройств с функциональностью L3VPN на краю сети провайдера для взаимодействия с сетью абонента.

#### **5.2.2.2. VPWS-PE**

VPWS-PE - устройство или набор устройств с функциональностью VPWS на краю сети провайдера для взаимодействия с сетью абонента.

<sup>1</sup>Customer Edge Router.

<sup>2</sup>Customer Edge Switch.

<sup>3</sup>Provider Edge Router.

<sup>4</sup>Provider Edge Switch



### 5.2.2.3. VPLS-PE

VPLS-PE - устройство или набор устройств с функциональностью VPLS на краю сети провайдера для взаимодействия с сетью абонента.

### 5.2.3. Именованное PE по месту размещения

Для обеспечения расширяемости в случаях VPLS/VPWS иногда бывает желательно распределить функции PE между несколькими устройствами. Например, можно назначить функции изучения MAC-адресов сравнительно небольшому и недорогому устройству, расположенному близко к сайту абонента, а участие в сигнализации PSN и организацию туннелей PE - PE выполнять на маршрутизаторах, расположенных ближе к ядру сети.

При распределении функций между устройствами нужен протокол обмена информацией между обращёнными в сторону сети - N-PE<sup>1</sup> (параграф 5.2.3.1) и в сторону пользователя - U-PE<sup>2</sup> (параграф 5.2.3.2) устройствами PE.

#### 5.2.3.1. Обращенное к сети устройство (N-PE)

N-PE является устройством, которому назначаются функции сигнализации и управления в распределенном VPLS-PE.

#### 5.2.3.2. Обращенное к клиенту устройство PE (U-PE)

U-PE представляет собой устройство, выполняющее функции пересылки и принятия решений о коммутации на входе в сеть провайдера.

## 5.3. Ядро сети

### 5.3.1. Маршрутизатор провайдера (P)

Маршрутизатор провайдера P<sup>3</sup> определяется как маршрутизатор в ядре сети, который не имеет интерфейсов непосредственно к абонентам. Следовательно P не хранит состояний VPN и не знает о VPN.

## 5.4. Именованное в отдельных документах Internet Draft

### 5.4.1. PE канального уровня (L2PE)

L2PE - общее имя устройств в сети провайдера, реализующих функции L2, требуемые для VPLS или VPWS.

### 5.4.2. Логическое устройство PE (LPE)

Термин LPE<sup>4</sup> берет своё начало в просроченном документе Internet Draft «VPLS/LPE L2VPNs: Virtual Private LAN Services using Logical PE Architecture» и служил для описания набора устройств, используемых в сети провайдера для реализации VPLS. В LPE функции VPLS распределены между небольшими устройствами U-PE (PE-edge) и устройствами в ядре сети N-PE (PE-Core). В решениях LPE устройства PE-edge и PE-Core могут быть соединены через коммутируемый транспорт Ethernet или восходящие каналы (uplink). LPE может также присутствовать в ядре сети в форме одного устройства PE. В этом документе устройства, составляющие LPE, называются N-PE и U-PE.

### 5.4.3. PE-CLE

Другое название U-PE, предложенное в просроченном документе Internet Draft «VPLS architectures».

### 5.4.4. PE-Core

См. параграф 5.4.2.

### 5.4.5. PE-Edge

См. параграф 5.4.2.

### 5.4.6. PE-POP

Другое название U-PE, предложенное в просроченном документе Internet Draft «VPLS architectures».

### 5.4.7. Краевое устройство VPLS (VE)

Термин VE<sup>5</sup> берет своё начало в просроченном документе Internet Draft по распределенным «прозрачным» услугам ЛВС и служил для описания устройств, используемых в сети провайдера для передачи VPLS абоненту. В этом документе VE называются VPLS-PE. Термин считается устаревшим.

## 6. Функции

В этом разделе собраны термины и понятия, связанные с работой сервиса VPN.

### 6.1. Устройство присоединения (AC)

В L2 VPN устройство CE подключается к PE с помощью устройства присоединения (AC). AC может быть физическим или логическим каналом.

<sup>1</sup>Network Facing PE.

<sup>2</sup>User Facing PE.

<sup>3</sup>Provider Router.

<sup>4</sup>Logical PE.

<sup>5</sup>VPLS Edge.

## 6.2. Backdoor Link

Backdoor Links - это «закулисный» канал между устройствами CE, организованный конечным пользователем, а не SP. Такие каналы могут служить для соединения устройств CE в многодомных конфигурациях [L3VPN-FRAME].

## 6.3. Обнаружение конечных точек

Обнаружение конечных точек представляет собой процесс, в котором устройства, осведомленные о конкретном сервисе VPN, будут находить обращённые в сторону абонентов порты, которые относятся к тому же сервису.

Требования к обнаружению конечных точек и сигнализации рассмотрены в [L3VPN-REQ]. Они также являются темой уже просроченного документа Internet Draft от команды разработчиков по обнаружению VPN.

## 6.4. Лавинная рассылка

Функция лавинной рассылки относится к службам L2 - когда PE принимает кадр с неизвестным MAC-адресом получателя, этот кадр требуется переслать во все интерфейсы.

## 6.5. Изучение MAC-адресов

Функция изучения MAC-адресов относится к службам L2 - когда PE принимает кадр с неизвестным MAC-адресом отправителя, привязка MAC-адреса к порту фиксируется для использования при пересылке в будущем. В решении для VPN канального уровня от рабочей группы L2VPN WG эта функция назначается устройствам VPLS-PE.

### 6.5.1. Квалифицированное обучение

В квалифицированном обучении на уровне U-PE выполняется изучение в абонентских кадрах Ethernet адресов MAC и тегов VLAN (при наличии тега). Если тегов в кадре нет, предполагается принятая по умолчанию VLAN.

### 6.5.2. Неквалифицированное обучение

При неквалифицированном обучении изучаются только MAC-адреса в абонентских кадрах Ethernet.

## 6.6. Сигнализация

Сигнализация представляет собой процесс, с помощью которого PE, имеющие за собой VPN, обмениваются данными для организации PW, туннелей PSN и туннельных мультиплексов. Это процесс может быть автоматизирован с помощью того или иного протокола или задаваться вручную через конфигурацию. Для организации туннелей PSN и обмена туннельными мультиплексами может применяться множество протоколов.

## 7. Физические устройства

Ниже приведён список устройств, которые обычно применяются в средах, поддерживающих различные типы услуг VPN. Представлены также некоторые устройства, не связанные напрямую со спецификациями протоколов.

### 7.1. Устройство агрегирования

Устройствами агрегирования обычно служат коммутаторы L2, которые не знают о VPN и лишь агрегируют трафик к узлам сети с большей функциональностью.

### 7.2. Абонентское оборудование (CPE)

Оборудованием CPE<sup>1</sup> называют устройства, которые провайдер размещает на площадке абонента. Эти устройства служат двум целям - предоставление портов для подключения абонента и обеспечение провайдеру возможности мониторинга соединения с сайтом абонента. CPE обычно является недорогим устройством с ограниченной функциональностью, не знающим об услугах VPN, предоставляемых сетью провайдера. CPE не обязательно выполняет функции CE, но является частью сети провайдера и служит для мониторинга.

Термин CPE обычно используется в описании работы сети и в контексте развёртывания и его не следует применять в спецификациях протоколов.

### 7.3. MTU

MTU<sup>2</sup> - обычно коммутатор L2, размещаемый сервис-провайдером в здании, где размещается несколько абонентов данного провайдера. Термин введён документом Internet Draft, задающим решение VPLS с распределением функций между MTU и PE в контексте [VPLS].

Термин MTU обычно используется в описании работы сети и в контексте развёртывания и его не следует применять в спецификациях протоколов, поскольку такая же аббревиатура служит для обозначения максимального размера передаваемого блока (Maximum Transmit Unit).

## 8. Сети с коммутацией пакетов (PSN)

PSN<sup>3</sup> - это сеть, через которую организуются туннели для поддержки сервиса VPN.

### 8.1. Отличие маршрута (RD)

RD<sup>4</sup> [RFC2547bis] — 8-байтовое значение, которое вместе с 4 байтами адреса IPv4 указывает адрес семейства VPN-IPv4. Если в двух VPN используется общий префикс IPv4, устройства PE будут транслировать его в уникальные

<sup>1</sup>Customer Premises Equipment.

<sup>2</sup>Multi-Tenant Unit - устройство с множеством арендаторов.

<sup>3</sup>Packet Switched Network

<sup>4</sup>Route Distinguisher.

префиксы VPN-IPv4. Это позволяет использовать одни и те же адреса в разных VPN, поскольку можно в каждой VPN организовать уникальный маршрут к данному префиксу.

## 8.2. Рефлектор маршрутов

Рефлектором маршрутов называют элемент сети SP, используемый для распространения маршрутов BGP среди поддерживающих протокол BGP маршрутизаторов SP [L3VPN-FRAME].

## 8.3. Цель маршрута (RT)

Атрибут RT<sup>1</sup> [RFC2547bis] можно рассматривать как идентификатор набора сайтов или, более точно, набора таблиц VRF (параграф 8.9).

Связывание конкретного RT с маршрутом позволяет поместить этот маршрут во все таблицы VRF<sup>2</sup>, используемый для маршрутизации трафика, полученного от соответствующих сайтов.

Атрибут RT относится также BGP extended community, используемым в [RFC2547] и [BGP-VPN]. Группа RT служит для ограничения распространения информации VPN заданным набором таблиц VRF. Цель маршрута можно рассматривать как указание набора сайтов или, более точно, набора таблиц VRF.

## 8.4. Туннель

Туннель является соединением через сеть PSN, которое применяется для передачи трафика через сеть от одного PE к другому. Туннель обеспечивает способы транспортировки пакетов между устройствами PE. Разделение трафика абонентов в туннели обеспечивается с помощью туннельных мультиплексоров (параграф 8.5). Организация туннеля зависит от механизмов туннелирования, предоставляемых PSN, например, туннели могут создаваться на основе заголовков IP, меток MPLS, идентификаторов сессий L2TP или полей GRE Key.

## 8.5. Туннельный мультиплексор

Туннельный мультиплексор — это просто элемент, передаваемый с пакетом, проходящим через туннель, и позволяющий отличить пакеты разных экземпляров сервиса и отправителей на приёмной стороне. В [PPVPN-L2VPN] туннельный мультиплексор имеет формат метки MPLS.

## 8.6. Виртуальный канал (VC)

VC<sup>3</sup> существует внутри туннеля и указывается туннельным мультиплексором. Виртуальный канал идентифицируется VCI (Virtual Channel Identifier). В контексте PPVPN идентификатором VCI служит метка VC или туннельный мультиплексор, а в случае Martini это VCID.

## 8.7. Метка VC

В сетях IP с поддержкой MPLS метка VC является меткой MPLS, служащей для идентификации трафика в туннеле, относящегося к конкретной сети VPN, т. е. метка VC служит туннельным мультиплексором в сети, использующей метки MPLS.

## 8.8. Внутренняя метка

Термин Inner label служит другим названием метки VC (параграф 8.6).

## 8.9. Маршрутизация и пересылка VPN (VRF)

В сетях VPN на основе [RFC2547] маршрутизаторы PE поддерживают таблицы VRF, определяющие маршрутизацию и пересылку на уровне сайта. Каждый сайт, к которому подключён маршрутизатор PE, связан с одной из таких таблиц. Поиск адреса IP для получателя конкретного пакета выполняется в данной таблице VRF лишь в том случае, когда пакет принят непосредственно с сайта, связанного с этой таблицей.

## 8.10. Экземпляр пересылки VPN (VFI)

VFI (VPN Forwarding Instance) — это логический элемент в PE, включающий базу маршрутной информации и данных пересылки для экземпляра VPN [L3VPN-FRAME].

## 8.11. Экземпляр виртуального коммутатора (VSI)

В контексте канального уровня VSI<sup>4</sup> представляет собой экземпляр виртуального коммутатора, который обслуживает один сервис VPLS [L2VPN]. VSI выполняет функции стандартного моста ЛВС (т. е. Ethernet). Пересылку VSI выполняет на основе MAC-адресов и тегов VLAN, возможно с учётом другой информации, относящейся к экземпляру VPLS. Экземпляры VSI выделяются устройством VPLS-PE или (в распределённом варианте) U-PE.

## 8.12. Виртуальный маршрутизатор (VR)

Виртуальный маршрутизатор (VR<sup>5</sup>) - это программный или аппаратный модуль для эмуляции физического маршрутизатора. Виртуальные маршрутизаторы имеют независимые таблицы маршрутизации и пересылки IP и изолированы один от другого (см. [L3VPN-VR]).

<sup>1</sup>Route Target.

<sup>2</sup>VPN Routing and Forwarding — маршрутизация и пересылка VPN.

<sup>3</sup>Virtual Channel

<sup>4</sup>Virtual Switch Instance.

<sup>5</sup>Virtual Router.



## 9. Вопросы безопасности

Этот терминологический документ не оказывает прямого влияния на безопасность. Вопросы безопасности, относящиеся к решениям, схемам и спецификациям, термины из которых собраны здесь, рассмотрены в соответствующих документах.

## 10. Благодарности

Большая часть этого документа основана на обсуждениях в командах разработчиков PPVPN auto discovery и l2vpn.

Dave McDysan, Adrian Farrel и Thomas Narten рецензировали документ и внесли много ценных предложений.

Thomas Narten преобразовал близкий к финальному вариант этого документа в формат XML, после того как извлечение приемлемого варианта из Word стало слишком тяжёлым. Avri Doria сильно помогла в использовании XML.

## 11. Литература

- [L2VPN] Andersson, L. and E. Rosen, "Framework for Layer 2 Virtual Private Networks (L2VPNs)", Work in Progress<sup>1</sup>, June 2004.
- [L2VPN-REQ] Augustyn, W. and Y. Serbest, "Service Requirements for Layer 2 Provider Provisioned Virtual Private Networks", Work in Progress<sup>2</sup>, October 2004.
- [VPLS] Kompella, K., "Virtual Private LAN Service", Work in Progress<sup>3</sup>, January 2005.
- [VPLS-LDP] Lasserre, M. and V. Kompella, "Virtual Private LAN Services over MPLS", Work in Progress<sup>4</sup>, September 2004.
- [BGP-VPN] Ould-Brahim, H., Rosen, E., and Y. Rekhter, "Using BGP as an Auto-Discovery Mechanism for Layer-3 and Layer-2 VPNs", Work in Progress, May 2004.
- [L3VPN-FRAME] Callon, R. and M. Suzuki, "A Framework for Layer 3 Provider Provisioned Virtual Private Networks", Work in Progress<sup>5</sup>, July 2003.
- [RFC3809] Nagarajan, A., "Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN)", RFC 3809, June 2004.
- [L3VPN-REQ] Carugi, M. and D. McDysan, "Service requirements for Layer 3 Virtual Private Networks", Work in Progress<sup>6</sup>, July 2004.
- [RFC2547bis] Rosen, E., "BGP/MPLS IP VPNs", Work in Progress<sup>7</sup>, October 2004.
- [L3VPN-VR] Knight, P., Ould-Brahim, H. and B. Gleeson, "Network based IP VPN Architecture using Virtual Routers", Work in Progress, April 2004.
- [PWE3-ARCH] Bryant, S. and P. Pate, "PWE3 Architecture", Work in Progress<sup>8</sup>, March 2004.
- [RFC3916] Xiao, X., McPherson, D., and P. Pate, "Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)", [RFC 3916](#), September 2004.
- [PPVPN-L2VPN] Kompella, K., "Layer 2 VPNs Over Tunnels", Work in Progress, June 2002.
- [ENCAP-MPLS] Martini, L., "Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks", Work in Progress, September 2004.
- [TRANS-MPLS] Martini, L. and N. El-Aawar, "Transport of Layer 2 Frames Over MPLS", Work in Progress<sup>9</sup>, June 2004.
- [RFC2547] Rosen, E. and Y. Rekhter, "BGP/MPLS VPNs", [RFC 2547](#), March 1999.
- [RFC2764] Gleeson, B., Lin, A., Heinanen, J., Armitage, G., and A. Malis, "A Framework for IP Based Virtual Private Networks", [RFC 2764](#), February 2000.

## Адреса авторов

**Loa Anderson**  
Acreo AB  
E-Mail: [loa@pi.se](mailto:loa@pi.se)

**Tove Madsen**  
Acreo AB  
E-Mail: [tove.madsen@acreo.se](mailto:tove.madsen@acreo.se)

## Перевод на русский язык

Николай Малых  
[nmalykh@protokols.ru](mailto:nmalykh@protokols.ru)

<sup>1</sup>Работа опубликована в [RFC 4664](#). Прим. перев.

<sup>2</sup>Работа опубликована в [RFC 4665](#). Прим. перев.

<sup>3</sup>Работа опубликована в [RFC 4761](#). Прим. перев.

<sup>4</sup>Работа опубликована в [RFC 4762](#). Прим. перев.

<sup>5</sup>Работа опубликована в RFC 4110. Прим. перев.

<sup>6</sup>Работа опубликована в RFC 4031. Прим. перев.

<sup>7</sup>Работа опубликована в [RFC 4364](#). Прим. перев.

<sup>8</sup>Работа опубликована в [RFC 3985](#). Прим. перев.

<sup>9</sup>Работа опубликована в RFC 4906. Прим. перев.

## **Полное заявление авторских прав**

Copyright (C) The Internet Society (2005).

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

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

### **Интеллектуальная собственность**

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

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

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

### **Подтверждение**

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