Network Working Group
Request for Comments: 2764
Category: Informational

B. Gleeson
A. Lin
Nortel Networks
J. Heinanen
Telia Finland
G. Armitage
A. Malis
Lucent Technologies

February 2000

Основа для построения частных виртуальных сетей на базе IP

A Framework for IP Based Virtual Private Networks

Статус документа

Этот документ содержит информацию для сообщества Internet. Документ не задает каких-либо стандартов Internet и может распространяться свободно.

Авторские права

Примечание IESG

Этот документ не является результатом рабочей группы IETF. В настоящее время IETF не прилагает усилий по стандартизации конкретных моделей VPN.

Тезисы

В этом документе описана модель виртуальных частных сетей (VPN[1]), работающих через магистрали IP. Рассмотрены разные типы VPN, требования к ним и предложены конкретные механизмы, которые могут быть использованы для реализации каждого типа VPN на основе существующих или предлагаемых спецификаций. Задачей этого документа является создание модели для разработки протоколов с целью создания полного набора спецификаций, требуемого для повсеместного развертывания интероперабельных VPN-решений.

Оглавление

[1]Virtual Private Network.

1.0 Введение

В этом документе описана модель виртуальных частных сетей (VPN), работающих через магистрали IP. Рассматриваются различные типы VPN, требования к ним и конкретные механизмы, которые могут применяться для реализации каждого типа VPN с использованием существующих или предлагаемых спецификаций. Задачей этого документа является создание модели для разработки протоколов с целью создания полного набора спецификаций, требуемого для повсеместного развертывания интероперабельных VPN-решений.

Развертывание виртуальных частных сетей через магистрали IP вызывает значительный интерес. Однако повсеместное распространение VPN затрудняется нехваткой интероперабельных реализаций, которая, в свою очередь, обусловлена отсутствием общепринятых определений и трактовок применения VPN, а также путаницей, обусловленной применением термина VPN для описания самых разных решений. В контексте этого документа аббревиатура VPN трактуется, как «эмуляция частной распределенной сети (WAN[1]) с использованием средств IP» (включая сеть Internet и частные сети IP). По причине существования множества типов VPN, а также разных типов WAN, в трактовках VPN зачастую возникает путаница.

В этом документе VPN моделируется, как объект связности (connectivity object). Хосты могут подключаться к VPN, а сами VPN могут соединяться между собой так же, как это происходит при подключении к физическим сетям и организации соединений между физическими сетями (например, через мосты или маршрутизаторы). Многие аспекты сетей такие, как адресация, механизмы пересылки, обнаружение и анонсирование доступности, качество обслуживания (QoS), безопасность и межсетевое экранирование имеют общие решения как для физических, так и для виртуальных сетей, а многие вопросы, возникающие при рассмотрении VPN, имеют прямые аналогии с вопросами реализации физических сетей. Введение VPN не требует заново изобретать сети или создавать новые парадигмы, у которых бы не было прямых аналогий с существующими физическими сетями. Зачастую достаточно просто рассмотреть решение того или иного вопроса в физической сетевой среде и применить те же принципы в среде, содержащей как физические, так и виртуальные сети, для разработки нужных расширений или требуемых улучшений. Очевидно, что наличие общих для физических и виртуальных сетей механизмов упрощает внедрение VPN в существующих сетях, а также снижает издержки на разработку стандартов и продукции, поскольку позволяет воспользоваться имеющимися решениями.

В этом документе предложена классификация типов VPN, показывающая применения каждого тип, специфические для типа требования, а также конкретные механизмы, которые наиболее применимы для реализации типа. Документ предназначен стать основой согласованного обсуждения конкретных модификаций, которые могут потребоваться в существующих механизмах IP для разработки полного спектра интероперабельных решений VPN.

В документе сначала рассматриваются возможные ожидания потребителей разных типов VPN и влияние этих ожиданий на пути реализации VPN. Рассматриваются также различия между решениями на базе пользовательского оборудования (CPE[2]) и на базе сетей. После этого представлена классификация типов VPN и связанных с ними требований. Очерчены также подходы к реализации и, следовательно, аспекты будущей стандартизации.

Отметим, что в этом документе рассматриваются лишь реализации VPN через магистрали IP, будь то частные сети IP или сеть Internet. Описанные здесь модели и механизмы применимы как для IPV4, так и для IPV6. В документе осознанно не рассматриваются VPN на базе естественного отображения на коммутируемые магистрали — например, VPN на основе LANE[3] [1] или MPOA[4] [2], работающие через магистрали ATM. При построении магистралей IP на базе упомянутых протоколов путем соединения маршрутизаторов через коммутируемые магистрали, рассматриваемые VPN работают «поверх» сети IP и, следовательно, не используют напрямую естественные механизмы нижележащих магистралей. Естественные VPN привязаны к службам нижележащих уровней, тогда как VPN на базе IP могут расширяться по мере расширения сетей IP. Протоколы естественных VPN выходят за пределы компетенции IETF и разрабатываются такими организациями, как ATM Forum.

2.0 Приложения VPN и требования к реализациям

2.1 Общие требования к VPN

Интерес к сетям IP VPN растет, поскольку эта модель обеспечивает экономические преимущества по сравнению с другими вариантами при построении и развертывании частных коммуникационных систем для межсайтового обмена информацией.

Существующие частные сети можно разделить на две основных категории — выделенные WAN-сети, соединяющие сайты между собой на постоянной основе и коммутируемые сети, где соединения между сайтами организуются по запросам через телефонную сеть общего пользования (PSTN[5]).

Сети WAN организуются обычно с использованием арендованных линий или выделенных каналов (например, Frame Relay или ATM) между разными сайтами. Оборудование CPE (коммутаторы или маршрутизаторы) на разных сайтах соединяют эти каналы в единую сеть, обеспечивающую связность сайтов. С учетом стоимости и сложности организации каналов, а также сложности настройки оборудования CPE такие сети обычно не являются полносвязными (fully meshed) и в них чаще используется тот или иной вариант иерархической топологии. Например, удаленные офисы могут непосредственно подключаться к ближайшему региональному офису, а те, в свою очередь, образуют полносвязную или многосвязную сеть.

Частные коммутируемые сети используются для подключения удаленных пользователей к сетям предприятий через телефонные сети PSTN или ISDN[6]. Обычно это реализуется за счет развертывания серверов удаленного доступа (NAS[7]) на одном или нескольких центральных сайтах. Пользователи организуют соединение с NAS по коммутируемым

[1]Wide Area Network.
[2]Customer Premises Equipment.
[3]LAN Emulation over ATM — эмуляция ЛВС в сетях ATM.
[4]Multiprotocol over ATM — мультипротокольные сети на базе ATM.
[5]Public Switched Telephone Network — коммутируемая телефонная сеть общего пользования.
[6]Integrated Services Digital Network — цифровая сеть с интеграцией услуг.
[7]Network Access Server — сервер доступа в сеть.

линиям, а сервер доступа взаимодействует с серверами аутентификации и учета (AAA[8]) для идентификации пользователей и предоставления каждому разрешенного набора услуг.

В последнее время рост числа компаний со скоростными каналами доступа в Internet обусловил повышение интереса к развертыванию на базе оборудования CPE сетей VPN, работающих через Internet. Основной причиной этого является отсутствие зависимости расходов при связи через Internet от расстояния, что позволяет существенно снизить стоимость организации VPN по сравнению с использованием арендованных линий и выделенных каналов.

Использование Internet для частных коммуникаций не является чем-то новым и существует множество методов организации такой связи, включая контролируемую утечку маршрутов (controlled route leaking) [3]. Однако лишь недавно появились механизмы IP, удовлетворяющие требованиям по организации VPN, описанным здесь.

2.1.1 Передача пакетов «втемную»

Передаваемый через VPN трафик может не иметь отношения к трафику магистрали IP, поскольку трафик является мультипротокольным или по причине того, что IP-адреса в частной сети могут относиться к пространству IP, не связанному с IP-сетью, через которую передается трафик. В частности, IP-сеть может использовать адреса IP из приватных блоков [4].

2.1.2 Защита данных

В общем случае организациям, применяющим VPN, требуется тот или иной уровень защиты данных существуют различные модели доверия, применимые к VPN. Одна из таких моделей основана на том, что потребитель не полагается на поставщика услуг в части защиты данных, а вместо этого строит VPN на базе устройств CPE, реализующих функции межсетевого экранирования, и соединяет эти устройства между собой через защищенные туннели. В этом случае сервис-провайдер используется исключительно для обеспечения транспортировки пакетов IP.

Другая модель основана на передаче вопросов защиты сервис-провайдеру, предоставляющего услуги защищенных управляемых VPN. Это похоже на доверие к операторам при использовании общественных коммутируемых сетей Frame Relay или ATM, когда потребители услуг верят, что пакеты не могут быть направлены по некорректному пути, невозможно появление обманных пакетов, изменение пакетов в процессе передачи или анализ трафика без соответствующих полномочий.

Во второй модели функции межсетевого экранирования и безопасной доставки пакетов входят в зону ответственности сервис-провайдера. На провайдерской магистрали могут потребоваться различные уровни защиты в зависимости от сценария развертывания. Если трафик VPN передается через одну IP-магистраль (опорную сеть) провайдера, сильной защиты (типа IPSec [5]), может не потребоваться для туннелей между магистральными узлами. Если же трафик VPN проходит через множество сетей или оборудования, администрируемого независимо, может потребоваться реализация сильных механизмов защиты. Организация сильной защиты от провайдера может потребоваться и в тех случаях, когда заказчик считает сети IP (и особенно Internet) небезопасными. Независимо от корректности такого мнения оно означает одну из проблем, которые должны решаться в реализации VPN.

2.1.3 Гарантии QoS

В дополнение к обеспечению конфиденциальности коммуникаций существующие методы организации частных сетей на базе механизмов физического и канального уровней обеспечивают также разного рода гарантии качества обслуживания. В частности, арендованные и коммутируемые линии обеспечивают гарантии в части задержки, а технологии организации выделенных каналов (типа ATM и Frame Relay) имеют широкий набор механизмов для обеспечения подобных гарантий. По мере роста числа VPN на базе IP будет расти и потребность рынка в подобных технологиях для того, чтобы обеспечить сквозную прозрачность работы на уровне приложений. Хотя возможности VPN на базе IP в плане предоставления таких гарантий будут зависеть от соответствующих возможностей нижележащих магистралей IP, модель VPN также должна решать вопросы использования этих возможностей системами VPN.

2.1.4 Механизм туннелирования

Первые два из перечисленных выше требований совместно означают, что для реализации VPN должна использоваться та или иная форма туннелирования IP, когда формат пакетов и/или используемые в VPN адреса могут не принадлежать к используемым на пути туннелирования через магистраль IP. Такие туннели, в зависимости от их типа, могут обеспечивать определенный уровень защиты, который можно повысить за счет применения специальных механизмов (например, IPSec).

Кроме того (как рассматривается ниже), такие механизмы туннелирования могут быть отображены на развивающиеся механизмы управления трафиком IP. В настоящее время уже определено множество механизмов туннелирования IP. Некоторые из таких механизмов хорошо подходят для приложений VPN (см. раздел 3.0).

2.2 VPN на базе сетей и CPE

Большинство современных реализаций VPN основано на оборудовании CPE. Возможности поддержки VPN встраиваются во множество устройств CPE, начиная от межсетевых экранов и заканчивая граничными маршрутизаторами WAN и специализированными шлюзами VPN. Такое оборудование может быть куплено и развернуто самими потребителями или сервис-провайдерами в качестве услуг аутсорсинга (в этом случае обычно с удаленным управлением).

Имеется также значительный интерес к VPN на базе сетей (network based VPN), когда обслуживание VPN передается поставщику услуг Internet (ISP[1]), а сами VPN реализуются на базе сетевого оборудования провайдера, а не устройств CPE. В таких решениях заинтересованы как стремящиеся снизить расходы на поддержку заказчики, так ISP, ищущие новые источники доходов. Поддержка VPN в сети позволяет использовать специальные механизмы, которые могут обеспечивать значительное преимущество в цене и эффективности VPN за счет реализации на одном оборудовании с единой поддержкой VPN большого числа заказчиков.

[8]Authentication, Authorization, Accounting — идентификация, проверка полномочий, учет.
[1]Internet Service Provider.

Большинство рассматриваемых ниже механизмов применимы к VPN на основе CPE или сетей. Однако часть механизмов применима только во втором варианте, поскольку требует средств (например, дополнений к протоколам маршрутизации), доступных ISP, которые вряд ли будут доступны потребителями или реализованы даже на принадлежащих и поддерживаемых ISP устройствах CPE по причине необходимости совместного управления работой CPE со стороны ISP и заказчика. Применимые лишь для VPN на базе сетей решения отмечены в документе явно.

2.3 VPN и Extranet

Термин «экстранет» (extranet) обычно используется для обозначений систем, где две или более компаний предоставляют друг другу ограниченный доступ к своим корпоративным ресурсам через сеть. Например, производственная компания может организовать extranet для своих поставщиков, чтобы обеспечить возможность запросов к базам данных для получения сведений о ценах и доступности компонент, а также отслеживания своих заказов. Другим примером может служить разработка программ — компания A открывает группе разработчиков из компании B доступ к исходным кодам своей операционной системы, а компания B разрешает специалистам компании A доступ к своим программам защиты. Отметим, что правила доступа могут быть неограниченно сложными. Например, компания B может иметь внутренние ограничения на доступ к своим программам защиты для пользователей из отдельных регионов планеты в соответствии с экспортными ограничениями.

Ключевым свойством extranet является контроль доступа к данным и это решение является политическим, а не техническим. Политические решения обычно реализуются в точках соединения между доменами (например, между частной сетью и Internet или между отделом тестирования ПО и остальной сетью компании). Реализация политики может происходить на межсетевом экране, маршрутизаторе с поддержкой списков доступа, прикладном шлюзе или ином устройстве, способном осуществлять фильтрацию трафика на основе правил. В дополнение к правилам межсетевого обмена могут быть реализованы правила внутри корпоративной сети. Соединения между сетями могут быть реализованы в форме множества двухсторонних связей или в виде отдельной сети, которая может поддерживаться отраслевым консорциумом. Такая сеть может представлять собой VPN или физическую сеть.

Добавление VPN в сеть не меняет эту модель. Правила могут исполняться между парами VPN или между VPN и Internet точно так же, как это происходило без VPN. Например, две VPN могут быть соединены между собой и администраторы каждой локально задают свои правила на межсетевом экране для всего внешнего трафика в VPN (из другой VPN или из Internet).

Эта модель VPN позволяет отделить политику от нижележащего реима, используемого для транспортировки пакетов. Например, маршрутизатор может направлять голосовой трафик в ATM VCC[1] для обеспечения гарантий QoS, нелокальный корпоративный трафик — в защищенные туннели, а весь остальной трафик — в канал подключения к сети Internet. В прошлом в качестве защищенных туннелей могли применяться виртуальные канала Frame Relay, а сейчас ими могут служить защищенные туннели IP или пути MPLS (LSP[2])

Возможны и другие модели VPN. Например, существует модель, где множество прикладных потоков отображается в VPN. Поскольку задаваемые сетевыми администраторами правила могут быть достаточно сложными, в базе правил будет множество прикладных потоков и, следовательно, множество VPN, которые могут частично перекрываться между собой. Однако столь сложная модель не обеспечивает заметных преимуществ. Разумней рассматривать VPN, как прямой аналог физической сети, поскольку это позволяет применять существующие протоколы и процедуры, а также использовать имеющийся у администраторов и заказчиков опыт.

3.0 Туннелирование VPN

Как отмечалось в параграфе 2.1, VPN должны реализоваться с применением того или иного механизма туннелирования. В этом параграфе рассматриваются базовые требования к механизмам туннелирования VPN. Рассматривается и сравнивается множество аспектов и характеристик, присущих всем протоколам канального уровня, со свойствами существующих протоколов туннелирования. Это обеспечивает основу для сравнения разных протоколов и может быть полезно для идентификации областей, в которых для существующих протоколов туннелирования могут быть получены дополнительные преимущества в поддержке VPN за счет расширения протоколов.

Туннель IP, соединяющий две оконечные точки VPN, служит базой для построения множества разных служб VPN. Туннель IP работает, как наложение на магистральную сеть IP, и передаваемый через туннель трафик непрозрачен для нижележащей магистрали IP. Магистральная сеть IP используется в качестве технологии канального уровня, а туннели образуют каналы «точка-точка».

Устройство VPN может завершать множество туннелей IP и пересылать пакеты между этими туннелями и другими сетевыми интерфейсами различными способами. При обсуждении различных типов VPN в последующих разделах документа основными различиями будут именно способы пересылки между интерфейсами (например, мост или маршрутизатор). Здесь имеется прямая аналогия с характеристиками разных сетевых устройств. Двухпортовый повторитель просто пересылает пакеты между своими портами, не проверяя содержимого пакетов. Мост пересылает пакеты на основе информации уровня MAC[3], содержащейся в пакете, а маршрутизатор при пересылке пакетов использует адреса уровня 3 из заголовков пакетов. Для каждого из этих вариантов имеется прямая аналогия в VPN, как будет показано ниже. Отметим, что туннель IP можно представлять себе, как отдельный тип канала, который может объединяться с другим каналом напрямую, через таблицу пересылки моста или таблицу маршрутизации IP в зависимости от типа VPN.

В последующих параграфах рассмотрены требования к базовому протоколу туннелирования IP, который может служить основной частью различных типов VPN.

[1]Virtual Channel Connection — соединение через виртуальный канал.
[2]Label Switched Path — путь с коммутацией по меткам.
[3]Media Access Control — контроль доступа к среде.

3.1 Требования к протоколам туннелирования для VPN

Существует множество механизмов туннелирования IP, включая IP/IP [6], туннели GRE[1] [7], L2TP[2] [8], IPSec [5], MPLS[3] [9]. Отметим, что хотя некоторые из этих протоколов зачастую не рассматриваются в качестве туннельных, все они обеспечивают транспортировку кадров в полях данных пакетов (packet payload) через сети IP с пересылкой пакетов, не привязанной к адресной информации в инкапсулированных пакетах.

Отметим, однако, одно существенное различие между протоколами туннелирования IP, перечисленными выше, и MPLS. MPLS можно рассматривать, как конкретный канальный уровень для IP, поскольку конкретные механизмы MPLS применяются лишь в зоне действия сети MPLS, тогда как механизмы на базе IP расширяют пределы достижимости IP. По этой причине механизмы VPN, напрямую основанные на туннелировании MPLS, не могут по определению распространяться за пределы сети MPLS, тогда как другие механизмы могут делать это (например механизм LANE может применяться за пределами сетей ATM). Отметим, однако, что сеть MPLS может существовать на базе многих разных технологий канального уровня и, подобно сетям IP, область распространения такой сети не ограничена применением того или иного конкретного канального уровня. Имеется множество предложений по определению набора механизмов для обеспечения интероперабельности VPN (в частности, через сети MPLS [10] [11] [12] [13], [14], [15].

Существует множество требований к механизмам туннелирования VPN, однако не все эти требования могут быть выполнены существующими механизмами туннелирования. Требования к туннелированию рассмотрены ниже.

3.1.1 Поле мультиплексирования

Возникают случаи, когда между парой конечных точек IP требуется организация множества туннелей VPN. Например, это может потребоваться в тех случаях, когда VPN организуется на уровне сети (network based), а каждая конечная точка поддерживает множество пользователей. Трафик разных пользователей проходит между парой физических устройств по разным туннелям. Для связывания пакетов с определенным туннелем требуется поле мультиплексирования. Совместное использование туннелей может также снижать задержки и объем работ при организации туннелей. Из числа имеющихся механизмов туннелирования IP механизмы мультиплексирования поддерживают L2TP (поля tunnel-id и session-id), MPLS (метка) и IPSec (поле SPI[4]). Строго говоря, в GRE поле мультиплексирования отсутствует. Однако поле key, предназначенное для аутентификации источника пакета, в некоторых случаях может служить в качестве поля мультиплексирования. IP/IP не имеет поля мультиплексирования.

IETF [16] и ATM Forum [17] стандартизовали единый формат уникальных в глобальном масштабе идентификаторов для VPN (VPN-ID). Идентификатор VPN-ID можно применять на уровне управления для привязки туннеля к VPN в момент организации туннеля, или на уровне данных для идентификации привязки пакетов к VPN. На уровне данных заголовок инкапсуляции VPN может использоваться MPLS, MPOA и другими механизмами туннелирования для агрегирования пакетов разных VPN в один туннель. В этом случае явная индикация VPN-ID включается в каждый пакет и используется в качестве поля мультиплексирования для данного туннеля. На уровне управления поле VPN-ID может включаться в любой сигнальный протокол организации туннелей для связывания туннеля (идентифицируемого например полем SPI) с VPN. В этом случае не будет необходимости включать VPN-ID в каждый пакет данных. Этот вопрос подробно рассматривается в параграфе 5.3.1.

3.1.2 Протокол сигнализации

Некоторые конфигурационные параметры конечная точка должна знать до организации туннеля (IP-адрес удаленной точки и все относящиеся к делу атрибуты туннеля, включая требуемый уровень защиты). После получения этой информации организацию туннеля можно выполнить двумя способами — с помощью операций управления или с использованием сигнального протокола, позволяющего динамически создавать туннели.

Примером операции управления может служить использование базы SNMP MIB[5] для настройки различных параметров туннеля (например, метки MPLS, адрес отправителя для туннеля IP/IP или GRE, идентификаторы туннеля и сессии L2TP, параметры защищенной связи IPSec).

Применение сигнального протокола может значительно снизить нагрузку на систему управления и по этой причине может быть важно для многих сценариев развертывания. Снижается объем операций по настройке, а также необходимость координации при создании VPN через разные административные домены. Например, описанное выше поле мультиплексирования является локальным для выделившего это значение узла и может храниться локально при использовании протокола сигнализации, но в варианте использования системы управления требуется передать это значение другим вовлеченным узлам. Сигнальный протокол также позволяет работу с мобильными узлами, которые не имеют постоянного подключения к сети, для организации туннелей по запросам.

При использовании в среде VPN сигнальному протоколу следует разрешать транспортировку VPN-ID, чтобы обеспечить возможность связывания туннеля с конкретной VPN. Следует также разрешать обмен и согласование атрибутов туннеля (например, применение восстановления порядка кадров или мультипротокольного транспорта). Отметим, что роль сигнального протокола состоит в согласовании атрибутов туннеля (например, пересылка пакетов через туннель на уровне 2 или 3), а не передаче информации о его использовании (это похоже на сигнализацию ATM Q.2931, который служит для организации логических подсетей Classical IP, а также эмулируемых ЛВС LANE).

Ряд протоколов туннелирования IP поддерживает сигнализацию, которую можно адаптировать для организации туннелей - L2TP (протокол L2TP), IPSec (протокол IKE[6] [18]) и GRE (при использовании с туннелями mobile-ip [19]). Имеется также два сигнальных протокола MPLS, которые можно использовать для организации туннелей LSP. Один протокол использует расширение протокола MPLS LDP[7] [20], называемое CR-LDP[8] [21], а другой — расширение RSVP[9] для туннелей LSP [22].

---

[1] Generic Routing Encapsulation — базовая инкапсуляция маршрутов.
[2] Layer 2 Tunneling Protocol — протокол туннелирования на уровне 2.
[3] Multiprotocol Label Switching — многопротокольная коммутация по меткам.
[4] Security Parameter Index — индекс параметров защиты.
[5] Management Information Base — база информации для управления.
[6] Internet Key Exchange — протокол обмена ключами.
[7] Label Distribution Protocol — протокол распространения меток.
[8] Constraint-Based Routing LDP — основанная на ограничениях маршрутизация LDP.
[9] Resource Reservation Protocol — протокол резервирования ресурсов.

3.1.3 Защита данных

Протокол туннелирования VPN должен поддерживать механизмы, позволяющие пользователям установить тот или иной уровень защиты, включая аутентификацию и/или шифрование разного уровня. Ни один из рассматриваемых механизмов туннелирования, за исключением IPSec, не имеет встроенных механизмов защиты и все они скорее опираются на средства защиты в опорных сетях IP. В частности, MPLS работает на основе явных метод для путей с коммутацией по меткам, что обеспечивает предотвращение перенаправления пакетов. Другие механизмы туннелирования обеспечивают защиту на базе IPSec. Для VPN, реализованных через опорные сети, отличные от IP (например, MPOA, Frame Relay или виртуальные каналы ATM), защита данных неявно обеспечивается сетевой инфраструктурой канального уровня.

Общая защищенность VPN определяется не только возможностями туннелей, но и механизмами пересылки пакетов в эти туннели. Например, для VPRN, реализованных с использованием виртуальных маршрутизаторов, использование раздельных таблиц маршрутизации и пересылки обеспечивает изоляцию трафика разных VPN. Пакеты одной VPN не могут по ошибке попасть в туннель другой VPN, поскольку эти туннели просто не будут присутствовать в таблице пересылки первой VPN.

Если конечная точка VPN использует тот или иной сигнальный механизм для динамической организации туннеля с другой точкой, возникает требование аутентификации стороны, пытающейся организовать соединение. IPSec включает множество схем для решения такой задачи, включая аутентификацию на основе общих (pre-shared) ключей или использование цифровых подписей и сертификатов. В других схемах туннелирования средств аутентификации меньше. В некоторых случаях аутентификация может не требоваться (например, при статической организации туннелей или использовании модели доверия, не требующей аутентификации).

В настоящее время протокол IPSec ESP[1] [23] для организации SA, которые могут поддерживать шифрование и/или аутентификацию. Однако спецификация протокола исключает применение SA, где нет ни шифрования, ни аутентификации. В среде VPN такой вариант null/null может оказаться полезным, поскольку может оказаться достаточным поддержка других аспектов протокола (например, туннелирования и мультиплексирования). Эффективно вариант null/null может рассматриваться просто как некий уровень защиты данных.

3.1.4 Мультипротокольный транспорт

Во многих приложениях через VPN может передаваться «непрозрачный», мультипротокольный трафик. В таких случаях туннельный протокол также должен поддерживать мультипротокольный транспорт. Протокол L2TP разработан для передачи пакетов PPP[2] [24] и, таким образом, может использоваться для передачи мультипротокольного трафика, поскольку сам транспорт PPP является мультипротокольным. Для идентификации туннелируемого протокола используется GRE. Туннели IP/IP и IPSec не имеют идентификационного поля, поскольку предполагают инкапсуляцию трафика IP.

Возможно расширение стека протоколов IPSec для поддержки мультипротокольного транспорта. Это можно реализовать, например, за счет расширения сигнальной компоненты IPSec — протокола IKE — для индикации типа протокола в туннелируемом трафике или за счет передачи заголовка мультиплексирования (например, LLC/SNAP или GRE) в каждом туннелируемом пакете. Это решение похоже на используемый в сетях ATM подход, когда используется сигнализация для указания инкапсуляции, применяемой в VCC, а передаваемые в VCC пакеты могут использовать заголовок LLC/SNAP или помещаться непосредственно в поля данных AAL5 (этот вариант называется VC-мультиплексированием [25]).

3.1.5 Сохранение последовательности кадров

Одним из параметров качества, запрашиваемых пользователями VPN, может быть сохранение порядка доставки кадров, как это происходит на арендованных физических линиях или выделенных каналах. Сохранение последовательности кадров может требоваться для обеспечения эффективной сквозной работы некоторых протоколов или приложений. Для обеспечения упорядоченной доставки кадров механизмы туннелирования должны поддерживать поле порядкового номера. Протоколы L2TP и GRE включают такое поле. В IPSec поле порядкового номера имеется, но оно используется на приемной стороне для предотвращения повторного использования пакетов, а не для соблюдения порядка доставки.

Можно расширить IPSec для поддержки использования поля порядкового номера в целях сохранения порядка доставки пакетов. Это можно сделать, например, за счет использования IKE для согласования упорядочения и выбора поведения конечных точек в части обработки этого поля.

3.1.6 Поддержание туннеля

Конечные точки VPN должны вести мониторинг работы туннелей VPN для предотвращения потери связи и принимать меры (например, перерасчет маршрута) при возникновении отказов в туннелях.

Есть два варианта такого мониторинга. В одном туннельный протокол самостоятельно проверяет связность и обеспечивает явную индикацию отказов. Например, протокол L2TP включает опциональный механизм keep-alive для обнаружения неработающих туннелей.

Другой вариант не требует от протокола туннелирования поддержки функций мониторинга и использует тот или иной внешний (out-of-band) механизм обнаружения потери связи. Например, если протокол маршрутизации типа RIP[3] [26] или OSPF[4] [27] работает через туннельную сеть, отсутствие информации от соседа в течение определенного времени приведет к тому, что протокол сочтет туннельное соединение разорванным. Другим способом может служить регулярная передача пакетов ICMP (ping) по адресу партнера. Это обычно обеспечивает достаточно эффективный способ проверки работы туннеля, поскольку он организован через ту же сеть IP.

При динамической организации туннелей нужно различать требуемую статическую и динамическую информацию. До того, как туннель может быть организован, узлу нужно получить некоторую статическую информацию, такую, как

[1]Encapsulating Security Payload — инкапсуляция защищенных данных.
[2]Point-to-Point Protocol.
[3]Routing Information Protocol.
[4]Open Shortest Path First.

идентификация удаленной точки и атрибуты туннеля. Обычно такая информация задается в процессе настройки конфигурации. В результате сигнального обмена при организации туннеля на каждой конечной точке создается некое динамическое состояние (например, значение поля мультиплексирования или используемые ключи). Например, при использовании IPSec организация защищенной связи (SA[1]) будет сопровождаться появлением ключей, используемых во время существования данной SA.

Организация динамических туннелей может инициироваться разными событиями. Одним из вариантов является организация туннеля по факту появления данных, которые нужно через этот туннель передать, и отключение туннели при отсутствии данных для передачи через него в течение некоторого времени. Такой подход полезен в тех случаях, когда ресурсы для туннелей выделяются с учетом требований QoS. Другим вариантом является организация туннеля в результате настройки статической конфигурации и сохранение туннеля в течение неограниченного времени.

3.1.7 Большие MTU

С туннелями IP связаны значения MTU[2], как для обычных каналов. Можно предположить, что это значение MTU превысит MTU на одном или нескольких интервалах пути между конечными точками туннеля. В таких случаях для туннеля потребуется та или иная форма фрагментации кадров.

Если передаваемый кадр отображается в одну дейтаграмму IP, может происходить обычная фрагментация IP, когда дейтаграмма попадет на интервал пути, где значение MTU окажется меньше, чем MTU в туннеле IP. Это может оказывать негативное влияние на производительность маршрутизаторов, выполняющих такую фрагментацию.

Другим решением является поддержка функций фрагментации и сборки фрагментов на уровне протокола туннелирования (возможно с использованием порядковых номеров и маркеров последнего фрагмента[3]). Это позволит избежать фрагментации IP в самом туннеле. Однако существующие протоколы туннелирования не поддерживают такого механизма.

3.1.8 Минимизация туннельных издержек

Очевидно преимущество от снижения связанных с механизмами туннелирования издержек. В частности, это важно для транспортировки чувствительного к задержке и ее вариациям трафика типа голоса и видео в пакетном режиме. С другой стороны, использование механизмов защиты типа IPSec не вносит дополнительных издержек, следовательно, цель заключается в минимизации издержек, не связанных с защитой.

Одним из случаев со значительными издержками на туннелирование связан с доступом в VPN по коммутируемым телефонным линиям. Этот случай более подробно будет рассмотрен в параграфе 6.3.

3.1.9 Управление потоком и контроль перегрузки

При разработке протокола L2TP были созданы процедуры для контроля потоков и перегрузок. Это было вызвано, прежде всего, необходимостью обеспечить производительность при работе в сетях с большими потерями с использованием компрессии PPP, которая, в отличие от IPComp[4] [28], связана с состояниями пакетов. Другим мотивом послужила необходимость использования устройств с малым размером буферов, которыми часто завершаются низкоскоростные коммутируемые линии. Однако механизмы контроля потоколв и перегрузок, определенные в финальной спецификации L2TP, используются только для управления каналами, а не трафиком данных.

В общем случае взаимодействие между множеством уровней систем контроля потоков и перегрузок может быть весьма сложным. С учетом преобладания в современных сетях трафика TCP и наличия у протокола TCP встроенных механизмов контроля потоков и перегрузок, преимущества от реализации аналогичных механизмов в протоколах туннелирования становятся не очевидными. Хорошие схемы контроля потоков данных и перегрузок, которые способны адаптироваться к разным условиям в сети и схемам развертывания, достаточно сложны в разработке как сами по себе, так и в плане взаимодействия с другими схемами, которые могут применяться параллельно. Однако могут обеспечиваться некоторые преимущества за счет возможности отправителя формировать трафик с учетом возможностей получателя и обеспечения протокольных механизмов, позволяющих получателю уведомить отправителя о своих возможностях. Эта направление может обеспечить преимущества после дополнительных исследований.

Отметим также работу группы IETF PILC[5], исследующей влияние свойств каналов на производительность работы протоколов Internet через такие каналы.

3.1.10 Управление трафиком и QoS

Как было отмечено выше, потребителям могут потребоваться от VPN характеристики, близкие к параметрам физических линий или выделенных каналов, в части QoS, уровня потерь, флуктуаций задержки, гарантированных значений полосы пропускания и задержек. Обеспечение таких характеристик в общем случае зависит от самих узлов VPN, а также от параметров соединяющих узлы сетей.

Полное рассмотрение вопросов QoS для VPN выходит за рамки этого документа, за счет моделирования туннелей VPN, как специального типа канального уровня, многие из существующих механизмов обеспечения QoS для физических соединений могут буть применены для VPN. Например, на узле VPN механизмы правил, маркировки, очередей и планирования могут применяться к специфическому трафику VPN, как к обычному (не VPN) трафику. Применимы также методы, разработанные группами Diffserv, Intserv и TE[6] в MPLS. Обсуждение вопросов QoS в VPN приведено в работе [29].

Следует отметить, что упомянутая здесь модель работы туннеля не обязательно будет соответствовать современной модели конкретного туннельного протокола. Модели разрабатываются для облегчения понимания и не являются частью спецификации протокола, однако наличие разных моделей может вызывать ненужные дискуссии, особенно при

[1]Security Association.
[2]Maximum Transmission Unit — максимальный размер передаваемого блока.
[3]Отметим, что протокол multilink PPP использует для фрагментации похожий механизм.
[4]IP Payload Compression Protocol — протокол сжатия полей данных IP.
[5]Performance Implications of Link Characteristics — влияние характеристик каналов на производительность.
[6]Traffic engineering/

ложном восприятии модели, как части спецификации или метода реализации. Например, обработка туннелей IPSec может моделироваться, как интерфейс или как атрибут конкретного потока пакетов.

3.2 Рекомендации

IPSec требуется в тех случаях, когда нужно надежное шифрование или строгая аутентификация. Поддерживается также мультиплексирование и сигнализация (протокол IKE). Однако расширение стека протоколов IPSec на перечисленные ниже области обеспечит преимущества в плане улучшения поддержки требований туннелирования в средах VPN:

- транспортировка VPN-ID в процессе организации SA (3.1.2);
- опции пустого шифрования (null encryption) и пустой аутентификации (null authentication) (3.1.3);
- работа с множеством протоколов (3.1.4);
- упорядочение кадров (3.1.5).

L2TP не обеспечивает защиты данных сам по себе и механизмы защиты PPP не применимы для протокола L2TP, поэтому для надежной защиты протокол L2TP должен работать на основе IPSec. Определение конкретных режимов работы IPSec для поддержки трафика L2TP будет повышать уровень совместимости. Это направление предложено в настоящее время для разработки группе L2TP.

4.0 Типы VPN — виртуальные выделенные линии

Простейшим вариантом VPN являются «виртуальные выделенные линии» (VLL[1]). В этом случае заказчик получает соединение типа «точка-точка» между двумя устройствами CPE, как показано ниже. На канальном уровне для подключения устройств CPE к узлам ISP могут использоваться разные технологии (например, ATM VCC или каналы Frame Relay). Устройствами CPE могут служить маршрутизаторы, мосты или хосты.

Оба узла ISP подключены к сети IP и между ними организуется туннель IP. Каждый узел ISP настраивается на привязку оконечного канала к туннелю IP на уровне 2 (например, ATM VCC связывается с туннелем IP). Кадры передаются между двумя каналами. Например, данные AAL5[2]) инкапсулируются в туннель IPSec. Содержимое полей данных AAL5 «непрозрачно» для узла ISP и не просматривается им.

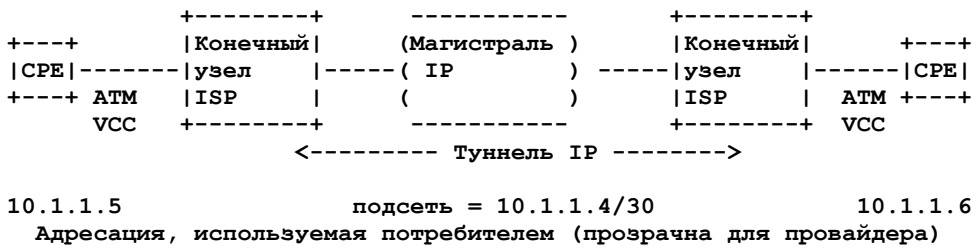

Рисунок 4.1 Пример VLL

С точки зрения потребителя услуги это выглядит, как обычный канал ATM VCC или Frame Relay, соединяющий между собой устройства CPE и потребитель может просто не думать о том, что часть канала фактически реализована через сеть IP. Это может оказаться полезным в тех случаях, когда провайдер, например, желает обеспечить связь между ЛВС через интерфейсы ATM, но не имеет собственной инфраструктуры ATM для непосредственного соединения сайтов заказчика.

Два канала, используемых для подключения устройств CPE к узлам ISP, могут быть организованы через разные среды, но в этом случае трафик не будет прозрачным для узлов ISP, как описано выше. Узлы ISP в такой ситуации должны поддерживать функции межсетевых устройств, соединяющих разнотипные среды (например, ATM и Frame Relay), а также выполнять функции преобразования LLC/SNAP в NLPID, отображения для разных вариантов протокола ARP или иные специфические операции, которые могут потребоваться для устройств CPE (например, обработка ячеек ATM OAM или обмен Frame Relay XID).

Используемый протокол туннелирования IP должен поддерживать мультипротокольные операции, а также может потребоваться поддержка упорядочения, если это важно для пользовательского трафика. Если туннели организуются с использованием протоколов сигнализации, они могут создаваться по мере поступления данных, а также по времени и сохраняться в рабочем состоянии.

Отметим, что использование термина VLL в данном документе отличается от принятой в EF-PHB[3] [30], где VLL рассматривается, как соединение с малой и стабильной задержкой и гарантированной полосой пропускания, которое может быть организовано с использованием упомянутого PHB. Т. е., внимание фокусируется на характеристиках канала, которые по природе своей зависят от времени. В данном же документе для VLL не предполагается использование какого-либо конкретного механизма QoS, Diffserv или иного. Здесь принимаются во внимание прежде всего топологические характеристики (например, организация канала с туннелем IP в одном из сегментов). Для полной эмуляции канального уровня следует принимать во внимание как временные, так и топологические параметры.

[1]Virtual Leased Line.
[2]ATM Adaptation Layer 5.
[3]Diffserv Expedited Forwarding Per Hop Behaviour.

5.0 Типы VPN — виртуальные маршрутизируемые сети (VPRN)

5.1 Характеристики VPRN

Виртуальная частная сеть с маршрутизацией (VPRN[1]) определяется, как эмуляция распределенной маршрутизируемой сети со множеством сайтов, использующей инфраструктуру IP. В этом разделе рассматривается организация сервиса VPRN на базе сетей. VPRN на базе CPE также возможны, но здесь они не рассматриваются. Для VPRN на базе сетей многие вопросы, требующие решения, связаны с конфигурацией и эксплуатацией, что внимания к распределению зон ответственности между поставщиком и потребителями услуг.

Отличительной чертой VPRN по сравнению с другими типами VPN является пересылка пакетов на сетевом уровне. VPRN включает многосвязную сеть туннелей IP между маршрутизаторами ISP и функции маршрутизации, требуемые для пересылки каждым узлом VPRN полученного трафика соответствующему сайту-получателю. К маршрутизаторам ISP подключаются маршрутизаторы CPE с использованием одного или нескольких оконечных (stub) каналов. На каждом маршрутизаторе ISP имеется специфическая для VPRN таблица пересылки. Трафик пересылается между маршрутизаторами ISP, а также между этими маршрутизаторами и сайтами заказчиков с использованием упомянутых таблиц пересылки, которые содержат информацию о доступности на сетевом уровне (в отличие от сетей VPLS[2], где таблицы пересылки содержат информацию о доступности на уровне MAC, как описано в разделе 7.0).

Пример VPRN показан на приведенном ниже рисунке, где три граничных маршрутизатора ISP соединены через полносвязную сеть туннелей IP и служат для связи между 4 маршрутизаторами CPE. Один из маршрутизаторов CPE имеет два соединения с ISP. В этом случае оба канала могут быть активны или может применяться, показанный на рисунке вариант «основной-резервный». Термином «обходной» канал на рисунке означено соединение между двумя пользовательскими сайтами, не использующее сеть ISP.

Рисунок 5.1 Пример VPRN

Основным преимуществом VPRN является минимизация сложностей, связанных с настройкой маршрутизаторов CPE. Для таких маршрутизаторов граничный маршрутизатор ISP выглядит, как соседний маршрутизатор своей сети, которому трафик передается с использованием принятого по умолчанию маршрута. Туннельная сеть для передачи трафика организуется между граничными маршрутизаторами ISP и не затрагивает маршрутизаторов CPE. В результате издержки, связанные с организацией и поддержкой туннелей, а также настройкой маршрутизации, переносятся на ISP. Кроме того, дополнительные службы, требующиеся для работы VPN (такие, как межсетевое экранирование и поддержка QoS), могут обеспечиваться небольшим числом граничных маршрутизаторов ISP вместо их развертывания на многочисленных и потенциально разнородных устройствах CPE. Организацию и поддержку новых служб также можно существенно упростить, поскольку для этого не потребуется обновление оборудования CPE. Это преимущество особенно важно в тех случаях, когда имеется множество абонентов, использующих услуги VPN для доступа в корпоративные сети. В этом смысле данная модель похожа на классическую телефонную сеть, где новые услуги (например, ожидание вызова) могут быть реализованы без замены абонентского оборудования.

VPRN отличаются от сетей VPN, где сеть туннелей включает маршрутизаторы CPE, а сеть ISP обеспечивает также услуги канального уровня. Такие сети могут быть реализованы с использованием множества VLL между маршрутизаторами CPE (см. раздел 4.0), когда сеть ISP обеспечивает множество соединений «точка-точка» на канальном уровне или с помощью VPLS (см. раздел 7.0), где сеть ISP используется для эмуляции сегмента ЛВС с множественным доступом. Такие сценарии обеспечивают потребителям большую гибкость (например, между сайтами заказчика можно использовать любую маршрутизацию IGP и любые протоколы), но обычно дороже и сложнее в настройке. Таким образом, в зависимости от требований заказчика может оказаться более подходящим решение на основе VPRN или VPLS.

Поскольку VPRN обеспечивает пересылку на сетевом уровне, единичная сеть VPRN может непосредственно поддерживать только один протокол сетевого уровня. При реализации многопротокольных систем можно использовать отдельную сеть VPRN для каждого протокола сетевого уровня или туннелировать дополнительные протоколы с использованием основного (например, туннелировать отличные от IP протоколы через IP VPRN). Кроме того, можно использовать сеть ISP для обеспечения соединений на канальном уровне, как для VPLS (см. выше).

[1]Virtual Private Routed Network.
[2]Virtual Private LAN Segment - сегмент виртуальной частной ЛВС.

Вопросы, которые нужно решать для VPRN, включают начальную настройку конфигурации, определение граничным маршрутизатором ISP набора каналов в каждой сети VPRN, установка других маршрутизаторов, которые будут входить в VPRN, а также указание адресных префиксов IP, которые будут доступны через каждый оконечный канал, определение маршрутизатором CPE набора адресных префиксов IP, для которых пакеты будут пересылаться граничному маршрутизатору ISP, механизм распространения информации о доступности оконечных узлов соответствующему множеству маршрутизаторов ISP и организация использования туннелей для передачи трафика данных. Отметим также, что многие из связанных с VPRN вопросов относятся и к описанному ниже сценарию VPLS с заменой адресации сетевого уровня на адресацию канального уровня.

Отметим, что работа VPRN не привязана к механизмам, используемым на сайтах потребителей для доступа в Internet. В типовом сценарии один граничный маршрутизатор ISP будет обеспечивать пользовательскому сайту подключение к VPRN и доступ в Internet. В этом случае маршрутизатор CPE будет просто использовать принятый по умолчанию маршрут, указывающий на граничный маршрутизатор ISP, а тот будет направлять трафик в сеть VPRN и Internet, а также обеспечивать межсетевое экранирование на границах доменов. Пользовательский сайт может подключаться к Internet через маршрутизатор ISP, не участвующий в работе VPRN, или даже относящийся к другому ISP. В этом случае устройство CPE должно самостоятельно отделять частный трафик от трафика Internet и обеспечивать межсетевое экранирование.

5.1.1 Топология

Топология VPRN может представлять собой полносвязную (full mesh) сеть туннелей между всеми узлами VPRN или использовать иной вариант соединений (например, подключение каждого удаленного офиса к ближайшему региональному узлу и многосвязная сеть соединений между региональными узлами). В сетях VPRN с использованием туннелей IP организация полносвязной сети соединений будет стоить существенно дешевле, нежели организация такой сети на физическом уровне (например, по арендуемым линиям) или использование метода туннелирования, требующего выделения ресурсов (например, Frame Relay DLCI) на устройствах, используемых для подключения к граничным маршрутизаторам. Полносвязная топология обеспечивает оптимальную маршрутизацию, когда трафик между парой сайтов передается напрямую без прохождения через транзитные узлы. Другим преимуществом полносвязной сети является отсутствие необходимости настройки топологии VPRN. Топология соединений между маршрутизаторами VPRN в данном случае просто задается неявно. Однако, если число граничных маршрутизаторов ISP в сети VPRN слишком велико, использование полносвязной топологии может стать неприемлемым по причине сложности масштабирования, связанных, например, с очень большим числом туннелей (n(n-1)/2 для n сайтов) или числом маршрутов к партнерам. Сетевая политика также может препятствовать организации полносвязной сети (например, администратор может принять решение о прохождении всего трафика через центральный сайт). Следует также принимать во внимание, что при возникновении ошибок в опорной сети IP часть туннелей может терять работоспособность (например, сайт A будет видеть сайт B, B будет видеть C, но для сайта A сайт C не будет доступен напрямую) в зависимости от политики маршрутизации.

Для основанных на сетях VPRN предполагается, что маршрутизатор CPE на каждом пользовательском сайте подключается к граничному маршрутизатору ISP через один или несколько каналов «точка-точка» (например, арендованные линии, соединения ATM или Frame Relay). Маршрутизаторы ISP отвечают за получение и распространение данных о доступности между собой. Маршрутизаторы CPE должны знать множество адресатов, доступных через каждый из каналов, хотя они могут просто пользоваться маршрутом по умолчанию.

Подключение абонентов может быть статическим (организуются на постоянной основе) или динамическим (организуется по запросу) на основе PPP, туннелей (см. параграф 6.3) или сигнализации ATM. Для динамических соединений требуется аутентификация подписчиков и определение ресурсов, которые могут им предоставляться (например, VPRN, к которым подписчик может подключаться). После подключения подписчика к VPRN (и выполнения дополнительных операций типа выделения динамических адресов IP) последующее использование механизмов и служб VPRN не будет зависеть от типа подключения абонента.

5.1.2 Адресация

Используемая в VPRN адресация может быть не связанной с адресами опорной сети IP, на основе которой организована эта VPRN. В частности, могут использоваться адреса IP из приватных блоков [4]. Через один набор физических устройств может быть организовано множество VPRN, причем их адресные пространства могут перекрываться.

5.1.3 Пересылка

Сеть туннелей VPRN формирует наложенную сеть поверх опорной сети IP. В каждом из граничных маршрутизаторов ISP должно присутствовать специфичное для VPN состояние, позволяющее пересылать пакеты из оконечных каналов (входящий трафик) на соответствующий маршрутизатор следующего интервала, а пакеты из ядра сети (исходящий трафик) — в соответствующий оконечный канал. Для случаев поддержки на маршрутизаторе ISP множества оконечных каналов одной сети VPRN, туннели могут завершаться как на этом маршрутизаторе, так и на оконечных каналах. В первом случае нужна специфичная для VPN таблица пересылки исходящего трафика, а во втором такая таблица не требуется. В общем случае специфичная для VPN таблица пересылки нужна для входящего направления, чтобы отправлять трафик из оконечного канала в соответствующий туннель IP в направлении ядра.

Поскольку VPRN работает на межсетевом уровне, для пакетов IP, передаваемых через туннель, поле времени жизни (TTL[1]) будет декрементироваться, как обычно, для предотвращения бесконечной циркуляции пакетов по сети в случае возникновения маршрутной петли в VPRN.

5.1.4 Множество VPRN через одно соединение

Отметим, что один и тот же пользователь услуг может иметь множество VPRN, которые он вместе с трафиком Internet пожелает передавать через общий оконечный канал. Для решения этой задачи существует множество вариантов, но их рассмотрение выходит за рамки данного документа.

[1]Time to Live.

5.2 Работы, связанные с VPRN

Требования и механизмы VPRN обсуждались ранее во множестве разных документов. Одной из первых была работа [10], где было показано, что в сетях с поддержкой и без поддержки MPLS может быть реализована одинаковая функциональность VPN. Некоторые другие работы кратко рассмотрены ниже.

Существует два основных варианта механизмов обеспечения в VPRN функций распространения информации о принадлежности и доступности — наложение (overlay) и совмещение (piggybacking). Эти варианты подробно рассматриваются ниже в параграфах 5.3.2, 5.3.3 и 5.3.4. Пример модели с наложением описан в [14], где рассматривается обеспечение функциональности VPRN с помощью отдельного экземпляра протокола маршрутизации для каждой VPN с организацией таблицы маршрутизации и пересылки — такое решение называют виртуальной маршрутизацией. Каждый экземпляр маршрутизации VPN изолирован от маршрутизации остальных VPN, а также от маршрутизации опорной сети. Это позволяет использовать в сетях VPRN любые протоколы маршрутизации (например, OSPF, RIP2, IS-IS), независимо от маршрутизации в других VPRN и и опорной сети. Модель VPN, описанная в [12], также работает на основе наложения с использованием виртуальной маршрутизации. Этот документ специально ориентирован на обеспечение функциональности VPRN на основе опорных сетей MPLS и описывает, как можно автоматизировать распространение информации о принадлежности к VPRN через сеть MPLS путем обнаружения соседей VPN через базовую сеть туннелей MPLS. В работе [31] модель виртуальной маршрутизации расширена путем включения областей VPN и граничных маршрутизаторов VPN между такими областями. Области VPN могут определяться в соответствии с техническими (например, тип сетевой инфраструктуры ATM, MPLS, IP) или административными аспектами.

В работе [15] описано обеспечение функциональности VPN на основе модели совмещения в плане распространения информации о принадлежности и доступности, которая передается в пакетах протокола маршрутизации BGP4[1] [32]. VPN создаются с использованием правил BGP, которые служат для контроля взаимодействия между сайтами. В [13] также используется распространение информации по протоколу BGP и сведения о доступности из этого протокола служат для организации MPLS LSP (CR-LDP или расширенных RSVP). В отличие от других вариантов в данной модели для реализации функций VPN требуется участие маршрутизаторов CPE.

5.3 Базовые требования VPRN

Имеется множество общих требований, которым должны соответствовать все решения VPRN на базе сетей, и есть множество разных механизмов, которые могут применяться для выполнения таких требований. Базовые требования включают:

1) Использование глобально уникальных идентификаторов VPN для обеспечения возможности указать конкретную VPN.

2) Определение принадлежности к VPRN. Граничный маршрутизатор должен определить оконечные соединения с каждой VPRN, а также набор маршрутизаторов данной VPRN.

3) Информация о доступности оконечных соединений. Граничный маршрутизатор должен определить адреса и префиксы, доступные через каждый оконечный канал.

4) Информация о доступности внутри VPRN. После того, как граничный маршрутизатор определит множество префиксов, связанных с каждым из своих оконечных каналов, эта информация должна быть распространена всем остальным граничным маршрутизаторам VPRN.

5) Механизм туннелирования. Граничный маршрутизатор должен организовать требуемые туннели к другим маршрутизаторам, входящим в VPRN, и выполнять инкапсуляцию и декапсуляцию для передачи пакетов через туннели.

5.3.1 Идентификатор VPN

IETF [16] и ATM Forum [17] стандартизовали единый формат уникальных в глобальном масштабе идентификаторов VPN — VPN-ID. Формат VPN-ID является единым, но семантика и применение различаются. Причина этого обусловлена желанием использовать один и тот же идентификатор для различных технологий и механизмов. Например, VPN-ID может включаться в базу MIB для идентификации VPN с целями управления. VPN-ID может использоваться на уровне управления, например, для привязки туннеля к VPN в момент организации этого туннеля. Все проходящие через туннель пакеты будут неявно связываться с данной VPN. Идентификатор VPN-ID может применяться в инкапсуляции на уровне данных, что позволяет явно различать пакеты каждой сети VPN. Если VPN реализуется с использованием разных технологий, (например, IP и ATM), для всех технологий может использоваться один идентификатор. Точно так же один идентификатор может применяться для VPN, организованных через множество административных доменов.

Большинство разработанных схем VPN (например, [11], [12], [13], [14]) требует использования VPN-ID в пакетах управления и/или данных для привязки каждого пакета к конкретной VPN. Хотя такое использование VPN-ID применяется широко, оно не является повсеместным. В работе [15] описана схема, где поле протокола не применяется для идентификации VPN описанным способом. В этой схеме VPN с точки зрения пользователя являются административными конструкциями на основе правил BGP. Имеется множество атрибутов, связанных с маршрутами VPN (идентификаторы маршрутов, VPN отправителя и получателя), которые применяются нижележащими протоколами для и эти же атрибуты используются механизмами BGP при создании VPN, но в этой схеме нет никакого аналога VPN-ID, используемого в данном документе.

Отметим также, что в [33] определена мультипротокольная инкапсуляция для использования с ATM AAL5 и стандартных VPN-ID.

5.3.2 Настройка и распространение конфигурационных данных VPN

Для организации VPRN или добавления новых пользовательских сайтов в существующую VPRN граничный маршрутизатор ISP должен определить, какие оконечные каналы связаны с какими VPRN. Для статических соединений (например, ATM VCC) эта информация должна указываться в конфигурации граничного маршрутизатора, поскольку он

[1] Border Gateway Protocol 4.

не может учесть такие привязки самостоятельно. Одним из решений являются базы SNMP MIB, позволяющие связать локальные оконечные каналы с VPN.

Для абонентов с динамическим подключением к сети (например, туннели PPP) можно организовать привязку оконечных соединений к VPRN, как часть процесса аутентификации пользователя, который применяется для таких динамических соединений. Например, VPRN, к которой привязывается пользователь, может определяться по доменному имени, использованному при аутентификации PPP. Если аутентификация пользователя завершилась успешно (например, с помощью сервера), новое динамическое соединение может быть привязано к нужной VPRN. Отметим, что статические конфигурационные данные по прежнему нужны (например, список уполномоченных пользователей для каждой VPRN), но эти конфигурационные данные могут храниться на внешнем сервере аутентификации, а не на граничном маршрутизаторе ISP. Независимо от того, является соединение статическим или динамическим, с ним может быть связан идентификатор VPN-ID, указывающий на конкретную VPRN.

После определения привязок оконечных каналов к VPRN каждый граничный маршрутизатор должен идентифицировать другие граничные маршрутизаторы (или, по крайней мере, пути к ним), поддерживающие другие оконечные каналы в данной VPRN. Последнее неявно указывает на существование некого механизма, с помощью которого настроенные граничные маршрутизаторы могут использовать такие данные о граничных маршрутизаторах и/или оконечных каналах для последующей организации между ними подходящих туннелей. Задача распространения информации о принадлежности к VPRN между вовлеченными в дело граничными маршрутизаторами может быть решена несколькими способами, рассмотренными ниже.

5.3.2.1 Просмотр каталогов

Участники конкретной VPRN (т. е., граничные маршрутизаторы, поддерживающие оконечные каналы в VPRN, и множества оконечных каналов, привязанных к граничным маршрутизаторам VPRN) могут быть указаны в каталоге (directory), к которому граничные маршрутизаторы могут при старте обращаться с помощью того или иного механизма (например, LDAP[1] [34]).

использование каталогов возможно как при полносвязной, так и при произвольной топологии. В случае полносвязной топологии повсеместно распространяется полный список маршрутизаторов, входящих в VPRN. Для произвольной топологии разные маршрутизаторы могут получать различные списки участников VPRN.

Использование каталогов позволяет проверить полномочия до распространения информации о принадлежности к VPRN, что может быть полезно для случаев, когда VPRN проходит через множество административных доменов. В таких случаях могут также использоваться протокольные механизмы обмена между каталогами информацией о принадлежности к VPRN.

Требуется также тот или иной механизм синхронизации баз данных (например, триггерный или регулярный опрос каталога граничными маршрутизаторами или активное «выталкивание» обновлений в граничные маршрутизаторы самим каталогом) для того, чтобы все граничные маршрутизаторы имели актуальную информацию о принадлежности к VPRN.

5.3.2.2 Явная конфигурация

Можно определить VPRN MIB для централизованного управления системой с возможностью настройки каждого маршрутизатора, обеспечивающей идентификацию вовлеченных граничных маршрутизаторов и статических оконечных каналов, привязанных к VPRN. Этот механизм, подобно каталогам, поддерживает полносвязную и произвольную топологию. Другим механизмом централизованного управления может служить сервер управления и протокол COPS[2] [35] для распространения информации о принадлежности к VPRN и правилах (например, атрибуты туннелей, используемые при организации туннелей, как описано в [36]).

Отметим, что такой механизм позволяет управляющей станции требовать строгой проверки полномочий, а с другой стороны он может затруднять настройку граничных маршрутизаторов, находящихся за пределами системы управления. Данная модель может рассматриваться, как частный случай модели с каталогами в том смысле, что каталоги управления могут использовать базы MIB для «выталкивания» информации о принадлежности к VPRN в вовлеченные граничные маршрутизаторы в процессе настройки локальных оконечных каналов или по его завершению.

5.3.2.3 Совмещение с протоколами маршрутизации

Информация о принадлежности к VPRN может быть добавлена к пакетам протоколов маршрутизации на каждом граничном маршрутизаторе опорной сети IP, поскольку это обеспечит эффективный способ распространения данных через сеть между участвующими в процессах граничными маршрутизаторами. В частности, каждый маршрутный анонс каждого граничного маршрутизатора может включать по меньшей мере набор идентификаторов VPN, связанных с этим маршрутизатором, а также адекватную информацию, которая позволит другим граничным маршрутизаторам идентифицировать данный маршрутизатор и/или путь к нему. Другие граничные маршрутизаторы будут проверять полученные маршрутные анонсы на предмет наличия в них относящейся к делу информации о поддерживаемых (т. е., включенных в конфигурацию VPRN. Такая проверка может быть выполнена путем сопоставления полученных идентификаторов VPN с заданными в локальной конфигурации VPN. Характер добавляемой в пакеты информации и связанные с этим вопросы (в частности, область действия и средства, с помощью которых идентифицируются узлы, анонсирующие принадлежность к конкретной VPN) будут зависеть от применяемого протокола маршрутизации и используемого транспорта.

Применение такого метода на всех маршрутизаторах сети будет обеспечивать одинаковое представление информации о принадлежности к сети и обеспечивает простоту поддержки полносвязной топологии. Поддержка произвольных топологий сложнее, поскольку требует реализации того или иного метода отсечки ненужных данных.

Преимуществом данной схемы является эффективное распространение информации, однако для этого требуется поддержка измененных маршрутных анонсов на всех узлах пути, а не только на принимающих участие граничных маршрутизаторах. Недостатком является существенное усложнение администрирования, связанное с настройкой области действия и области распространения измененных маршрутных анонсов. Да и сама настройка конфигурации для VPRN, проходящих через множество маршрутных доменов (и автономных систем) не является простым делом.

[1] Lightweight Directory Access Protocol — облегченный протокол доступа к каталогам.
[2] Common Open Policy Service — открытая служба правил общего назначения.

Кроме того, пока не применяется тот или иной механизм защиты маршрутных обновлений, обеспечивающий возможность их чтения только вовлеченным в процесс граничным маршрутизаторам, эта схема полагается на модель доверия, где предполагается, что все маршрутизаторы на пути могут получать эту информацию. В зависимости от применяемого протокола маршрутизации на промежуточных маршрутизаторах (в частности на граничных маршрутизаторах AS[1]) может потребоваться кэширование таких анонсов и, возможно, их распространение в другие протоколы маршрутизации.

Каждая из описанных схем хороша для определенных условий. Отметим, что на практике почти всегда имеется некий централизованный каталог или система управления для поддержки информации о принадлежности к VPRN — такой, как список граничных маршрутизаторов, которым позволена поддержка конкретной VPRN, привязки статических оконечных соединений к VPRN или данные для аутентификации и проверки полномочий пользователей, подключающихся к сети по динамическим каналам. Эта информация должна сохраняться в той или иной базе данных так, чтобы дополнительные действия по передаче конфигурационных данных в граничные маршрутизаторы и/или обеспечение доступа граничных маршрутизаторов к такой информации не было слишком обременительным.

5.3.3 Информация о доступности оконечных каналов

Есть два аспекта доступности тупиковых сайтов — способ, с помощью которого граничные маршрутизаторы VPRN определяют набор адресов и префиксов VPRN, доступных на каждом тупиковом сайте, и способ, с помощью которого маршрутизаторы CPE узнают об адресатах, доступных через каждый тупиковый канал. В обоих случаях граничному маршрутизатору ISP нужна одинаковая операция — набор адресов VPRN на сайте заказчика, но маршрутизаторам CPE нужна другая информация.

5.3.3.1 Сценарии подключения оконечных каналов

5.3.3.1.1 Общее соединение для VPRN и Internet

Маршрутизатор CPE подключен одним каналом к граничному маршрутизатору ISP, который обеспечивает сервис VPRN и подключение к Internet.

Это простейший случай и маршрутизатору CPE нужен лишь используемый по умолчанию маршрут к граничному маршрутизатору ISP.

5.3.3.1.2 Отдельное соединение для VPRN

Маршрутизатор CPE соединяется одним каналом с граничным маршрутизатором ISP, который обеспечивает услуги VPRN без доступа в Internet.

Маршрутизатор CPE должен знать множество нелокальных адресатов VPRN, доступных через этот канал. Это может быть общий префикс или группа разрозненных префиксов. Эти данные должны быть включены в конфигурацию маршрутизатора CPE статически или определены им с помощью запущенного процесса IGP[2]. Для простоты будем предполагать, что в качестве IGP используется протокол RIP, хотя это может быть и любой другой IGP. Краевой маршрутизатор ISP будет передавать этому экземпляру RIP маршруты VRPN, которые он узнал с помощью того или иного механизма определения доступности в рамках VPRN (см. параграф 5.3.4). Отметим, что экземпляр RIP на устройстве CPE и любой экземпляр протокола маршрутизации, служащий для определения доступности внутри VPRN (даже если это RIP), не связаны между собой и маршруты между ними распространяет граничный маршрутизатор ISP.

5.3.3.1.3 Многодомые подключения

Маршрутизатор CPE имеет множество подключений к сети ISP, которые обеспечивают соединение в VPRN.

В этом случае все граничные маршрутизаторы ISP могут анонсировать одинаковые маршруты VPRN к маршрутизатору CPE, который в результате будет видеть, что префиксы VPRN одинаково доступны через все каналы. Возможно также распространение более специфичных маршрутов, когда каждый граничный маршрутизатор ISP анонсирует свой набо префиксов для маршрутизатора CPE.

5.3.3.1.4 Обходные каналы

Маршрутизатор CPE соединен с сетью ISP, обеспечивающей подключение к VPRN, и имеет также «обходной» канал к одному из сайтов организации.

В этом случае граничный маршрутизатор ISP будет анонсировать маршруты VPRN устройству CPE (как в случае 2). Однако в этом случае один и тот же адресат может быть доступен как через граничный маршрутизатор ISP, так и по обходному каналу. Если маршрутизаторы CPE соединены с обходным каналом и используют корпоративный IGP, обходной канал может оказаться более предпочтительным во всех ситуациях, поскольку он представляется внутренним, тогда как маршруты от граничного маршрутизатора ISP будут внешними по отношению к IGP. Для предотвращения возможных проблем (в предположении, что заказчик желает передавать трафик через сеть ISP) следует использовать отдельный экземпляр RIP между маршрутизаторами CPE на обоих концах обходного канала (так же, как протокол RIP используется на оконечном или резервном канале между маршрутизатором CPE и граничным маршрутизатором ISP. В этом случае обходной канал будет выглядеть, как внешний, и с помощью подбора «стоимости» пути маршрут через ISP можно сделать предпочтительным, используя обходной канал в случае отказа.

Описанные выше варианты подключения предполагают, что информация о доступности нужна краевым маршрутизаторам ISP и маршрутизаторам CPE. Рассмотрены некоторые механизмы распространения такой информации. Ниже эти механизмы описаны более подробно.

5.3.3.2 Экземпляр протокола маршрутизации

Между граничными маршрутизаторами CPE и ISP может использоваться протокол маршрутизации для обмена информацией о доступности. Это позволяет граничному маршрутизатору ISP узнать префиксы VPRN, доступные на сайте заказчика, а маршрутизатору CPE — префиксы адресатов, доступных через сеть провайдера.

[1] Автономная система.
[2] Interior Gateway Protocol — протокол внутреннего шлюза.

Домен маршрутизации для этого экземпляра протокола обычно включает лишь граничный маршрутизатор ISP и маршрутизатор CPE, хотя этот же протокол заказчик может использовать в качестве IGP и домен маршрутизации будет включать сайт заказчика. Если на сайте применяется другой протокол маршрутизации, маршрутизатор CPE будет распространять маршруты между экземпляром протокола, работающим с маршрутизатором ISP, и экземпляром протокола на сайте.

С учетом обычно ограниченной области действия этого экземпляра протокола маршрутизации достаточно самых простых протоколов. Чаще всего для этой цели используется протокол RIP, хотя применимы и более сложные протоколы типа OSPF или BGP (в режиме IBGP).

Отметим, что экземпляр протокола маршрутизации на оконечном канале отличается от любого экземпляра протоколов маршрутизации, связанных с доступностью маршрутов внутри VPRN. Например, если граничный маршрутизатор ISP использует протокол маршрутизации для распространения информации о принадлежности к VPRN и данных о доступности через ядро, он может распространять помеченные подходящим способом маршруты от протокола маршрутизации CPE в протокол маршрутизации ядра. Используемые для каждого экземпляра протоколы маршрутизации не связаны между собой и в каждом из случаев может применяться любой подходящий протокол. Нет требования использовать один протокол и даже один механизм сбора сведений о доступности на маршрутизаторах CPE и связанных с ними маршрутизаторах ISP в той или иной VPRN — этот вопрос решается локально.

Отсутствие привязки между протоколами маршрутизации позволяет ISP использовать единый (для всех VPRN) механизм определения доступности внутри VPRN и единый механизм определения доступности через оконечные каналы, поскольку эти механизмы изолированы один от другого, а также от протоколов IGP, используемых в сетях заказчиков. В первом случае, благодаря реализованной на краевом маршрутизаторе ISP границе IGP-IGP, ISP может изолировать механизм определения доступности внутри VPRN от некорректного поведения протоколов маршрутизации на оконечных соединениях. Во втором случае от ISP не требуется принимать во внимание протоколы IGP, используемые на сайтах заказчиков. Возможны и другие варианты, когда на граничном маршрутизаторе ISP используется тот же экземпляр протокола маршрутизации, что и IGP у заказчиков, но это решение непрактично, поскольку не соответствует цели VPRN упростить конфигурацию маршрутизаторов CPE. Для случаев, когда заказчик желает использовать IGP на множестве сайтов, более подходящим решением будет VPLS.

Отметим, что в тех случаях, когда тот или иной сайт заказчика входит одновременно в несколько VPRN (или хочет одновременно использовать VPRN и доступ в Internet), граничный маршрутизатор ISP должен иметь способ однозначного отображения адресных префиксов оконечного канала на конкретные VPRN. Простым решением является использование отдельного оконечного канала для каждой VPRN, однако можно подключать и множество VPRN через общий оконечный канал. Это можно сделать с помощью отображения (и соответствующей настройки граничного маршрутизатора ISP) на разные VPRN непересекающихся адресных префиксов или за счет маркировки маршрутных анонсов от CPE идентификаторами VPN. Например, при использовании MPLS для передачи данных о доступности оконечного соединения можно применять разные метки MPLS для непересекающихся адресных префиксов различных VPRN. В любом случае для решения этой задачи нужна та или иная административная процедура.

5.3.3.3 Настройка конфигурации

Информация о доступности через оконечный канал может быть задана вручную, если набор адресных префиксов невелик и статичен.

5.3.3.4 Администрируемые ISP адреса

Множество адресов, используемых каждым тупиковым сайтом может администрироваться и выделяться через граничный маршрутизатор VPRN и такое решение может быть приемлемо для небольших сайтов, которые зачастую состоят из одного хоста или одной подсети. Выделение адресов может выполняться с помощью протоколов типа PPP или DHCP [37], а граничный маршрутизатор может служить клиентом Radius, получающим IP-адреса для пользователей от сервера Radius, или служить транслятором DHCP, проверяя отклики DHCP, транслируемые сайту заказчика. В этом случае граничный маршрутизатор может самостоятельно построить таблицу доступности адресов через оконечный канал. Хотя упомянутые механизмы обычно используются для выделения адресов отдельным хостам, некоторые производители добавили расширения, позволяющие выделять префиксы, а устройства CPE могут выполнять функции серверов DHCP и выделять адреса для хостов на сайте заказчика.

Отметим, что в этих схемах сервер распределения адресов отвечает за выделение каждому сайту в VPN неперекрывающихся адресных блоков. Отметим также, что ISP используют такие механизмы обычно лишь для небольших тупиковых сайтов, у которых нет каналов в обход данного провайдера.

5.3.3.5 Протокол распространения меток MPLS

В случаях использования на маршрутизаторе технологии MPLS можно использовать LDP для передачи набора префиксов на оконечной стороне граничного маршрутизатора VPRN. Использование незапрошенного нисходящего распространения меток маршрутизатором CPE позволяет распространить метки для каждого маршрута на тупиковый сайт. Отметим, что в данном случае обработка на граничном маршрутизаторе не ограничивается обычными операциями LDP и включает дополнительно определение новых маршрутов через LDP, используемое вместо обычного определения меток существующих маршрутов через стандартные механизмы маршрутизации.

5.3.4 Информация о доступности внутри VPN

После того, как граничных маршрутизатор определил набор префиксов, связанных с каждым из его оконечных каналов, эта информация может быть распространена другим краевым маршрутизаторам в VPRN. Отметим наличие неявного требования о том, что множество достижимых адресов в VPRN должно быть локально уникальным, т. е. каждый оконечный канал VPRN (не обеспечивающий распределения нагрузки) должен поддерживать адресное пространство, не пересекающееся с адресами на других оконечных каналах, для обеспечения однозначной маршрутизации. На практике желательно (хотя и не требуется) иметь не связанные адресные префиксы для каждого граничного маршрутизатора, чтобы избавиться от необходимости поддержки и распространения большого числа маршрутов к хостам.

Задача распространения информации о доступности адресов внутри VPN может быть решена множеством способом. Некоторые из этих решений описаны ниже.

5.3.4.1 Просмотр каталога

Наряду с информацией о принадлежности к VPRN центральный каталог может включать список адресных префиксов, связанных с каждым из сайтов заказчика. Такая информация может быть получена сервером путем протокольного взаимодействия с каждым граничным маршрутизатором. Отметим, что вопросы синхронизации каталогов, рассмотренные в параграфе 5.3.2, применимы и в данном случае.

5.3.4.2 Явная настройка конфигурации

Адресное пространство, связанное с каждым граничным маршрутизатором, может быть явно указано в конфигурации всех остальных граничных маршрутизаторов. Ясно, что такое решение не обеспечивает достаточного уровня масштабирования (особенно для произвольных топологий), а также не решает вопроса передачи информации в системы сетевого управления.

5.3.4.3 Локальные экземпляры маршрутизации внутри VPRN

В этом варианте каждый граничный маршрутизатор запускает отдельный экземпляр протокола маршрутизации (виртуальный маршрутизатор) для каждой VPRN через туннели VPRN с остальными краевыми маршрутизаторами этой сети для распространения информации о доступности внутри VPRN. Обеспечивается простая поддержка как полносвязной, так и произвольных топологий, если сам протокол маршрутизации может работать в такой топологии. Внутренние маршрутные анонсы VPRN можно отличить от обычных пакетов данных в туннелях путем их прямой адресации граничным маршрутизаторам или с помощью специфических для туннеля механизмов.

Отметим, что этот протокол маршрутизации внутри VPRN не требуется связывать с IGP на сайтах заказчика или протоколами маршрутизации, используемыми ISP в опорной сети IP. В зависимости от размера и масштабов VPRN может использоваться простой протокол типа RIP или более изощренный протокол типа OSPF. Поскольку протокол маршрутизации внутри VPRN работает «поверх» опорной сети IP, он не заметен для всех промежуточных маршрутизаторов и граничных маршрутизаторов, не относящихся к VPRN. Это также предполагает, что такая информация будет непонятной (opaque) для этих маршрутизаторов, что в некоторых случаях может оказаться важным с точки зрения безопасности. Отметим также, что при использовании протокола маршрутизации через те же туннели, которые служат для передачи данных, для пакетов маршрутизации будет обеспечиваться такая же защита (например, шифрование и аутентификация источника).

Если туннели, через которые работает протокол маршрутизации VPRN, выделены для конкретной VPN (например, за счет использования различных значений поля мультиплексирования для каждой VPN), вносить какие-либо изменений в сам протокол маршрутизации не требуется. С другой стороны, при использовании разделяемых туннелей требуется расширение протокола маршрутизации для включения поля VPN-ID в пакеты маршрутных обновлений, чтобы обеспечить возможность привязки набора адресных префиксов к конкретной VPN.

5.3.4.4 Протокол доступности канала

Протокол доступности канала обеспечивает двум узлам, соединенным каналом «точка-точка» обмениваться данными о доступности. Для случая полносвязной топологии на каждом граничном маршрутизаторе может применяться протокол доступности канала (например, та или иная вариация MPLS CR-LDP) через туннели со всеми граничными маршрутизаторами VPRN. Этот протокол передает VPN-и информацию о доступности каждой VPRN, работающей через туннель между двумя граничными маршрутизаторами. Если информация о принадлежности к VPRN уже была передана граничному маршрутизатору, используемое в традиционных протоколах маршрутизации обнаружение соседей уже не требуется, поскольку соседи известны. Для организации надежных соединений с соседями может применяться транспорт TCP. Такая модель может снижать издержки, связанные с использованием отдельных экземпляров протокола маршрутизации для каждой VPRN, и может обеспечивать преимущества за счет применения общего туннеля для соединения множества граничных маршрутизаторов, поддерживающих разные VPRN.

Другой основой для разработки протокола доступности канала может быть протокол маршрутизации IBGP. Задачи, которые должны решаться протоколом доступности канала очень похожи на задачи протокола IBGP — надежная передача адресных префиксов между граничными маршрутизаторами.

Использование протокола доступности канала достаточно просто для полносвязной топологии — каждый граничный маршрутизатор передает свои данные о доступности всех остальных маршрутизаторов, не распространяя полученной от них информации. Однако для произвольной топологии требуется превращение протокола доступности канала в полный протокол маршрутизации, поскольку требуется реализовать механизм предотвращения петель. Разработка для этого случая дополнительного протокола маршрутизации вряд ли обеспечит какие-то значимые преимущества. Некоторые причины использования неполносвязных топологий в средах на основе туннелей рассмотрены в параграфе 5.1.1.

5.3.4.5 Совмещение в протоколах маршрутизации опорных сетей IP

Как и данные о принадлежности к VPRN, набор адресных префиксов, связанных с каждым интерфейсом в оконечный канал, может добавляться в маршрутные анонсы от каждого граничного маршрутизатора и распространяться через сеть. Другие граничные маршрутизаторы будут извлекать эту информацию из маршрутных анонсов так же, как данные о принадлежности к VPRN (которые в данном случае подразумеваются в идентификации источника каждого маршрутного анонса). Отметим, что эта схема может потребовать (в зависимости от протокола маршрутизации) кэширования информации о маршрутах внутри VPRN на промежуточных устройствах. Этот факт оказывает влияние на модель доверия и уровень защиты информации о внутренних маршрутах VPRN.

Отметим, что в любой из рассмотренных выше ситуаций граничный маршрутизатор имеет возможность распространения информации о префиксах своих оконечных соединений, позволяющего организовать прямые туннели с удаленных граничных маршрутизаторов непосредственно на выход оконечного канала. Кроме того, он может распространять информацию так, чтобы все префиксы связывались с граничным маршрутизатором, а не с конкретным оконечным каналом. В этом случае граничному маршрутизатору потребуется реализовать специфический для VPN механизм пересылки выходного трафика с целью определения корректного выходного канала. Это может существенно снижать число туннелей или объем информации о туннельных метках, которые требуется создавать и поддерживать. Отметим, что это решение принимается на локальном уровне и не видно для удаленных граничных маршрутизаторов.

5.3.5 Механизмы туннелирования

После распространения информации о принадлежности к VPRN могут быть построены туннели, составляющие ядро VPRN.

Одним из вариантов построения сети туннелей является организация туннельных соединений IP «точка-точка»; требования к таким туннелям и связанные с ними вопросы рассмотрены в разделе 3.0. Например, конфигурация туннельных соединений может задаваться вручную, но такое решение явно не обеспечивает должного масштабирования с учетом квадратичной зависимости трудоемкости настройки от числа туннелей. По этой причине для организации туннелей следует использовать ту или иную форму сигнального протокола, позволяющую узлам попарно строить туннели между собой на основе взаимной идентификации.

Другим вариантом является использование туннелей «точка — много точек», обеспечиваемых MPLS. Как отмечено в [38], MPLS можно рассматривать как форму IP-туннелирования, поскольку метки в пакетах MPLS позволяют отвязать принятие решений о маршрутизации от адресной информации в самих пакетах. Механизмы распространения меток MPLS могут служить для связывания конкретного множества меток MPLS с определенными адресными префиксами VPRN, поддерживаемых на конкретных точках выхода (т.е., оконечных соединениях граничных маршрутизаторов), и, следовательно, другим граничным маршрутизаторам обеспечивается возможность явно помечать и маршрутизировать трафик в конкретные оконечные каналы VPRN.

Одним из привлекательных результатов использования MPLS в качестве туннельного механизма является снижение издержек на обработку в каждом граничном маршрутизаторе по сравнению с другими механизмами туннелирования. Это обусловлено тем, что защита данных в сети MPLS неявно обеспечивается явным связыванием меток, по аналогии с ориентированными на соединения сетями типа Frame Relay. Это может, следовательно, уменьшить опасения заказчиков в плане безопасности данных и снизить издержки на ресурсоемкие средства защиты (например, IPSec). Однако с MPLS связаны другие потенциальные проблемы безопасности. Здесь нет прямой поддержки таких защитных функций, как аутентификация, защита конфиденциальности и невозможность отказа, а модель доверия для MPLS предполагает, что промежуточные маршрутизаторы (которые могут располагаться в других административных доменах), через которые передается информация о принадлежности и доступности, должны быть доверенными, как и сами граничные маршрутизаторы.

5.4 Многодомные оконечные маршрутизаторы

Выше неявно предполагалось, что каждый оконечный маршрутизатор соединяется с одним (и только с одним) граничным маршрутизатором VPRN. В общем случае следует отказываться от такого допущения без внесения изменений в работу VPRN — это диктуется тенденциями организации многодомных подключений с целью повышения надежности и по иным причинам. В частности, для случая, когда оконечный маршрутизатор поддерживает множество соединений (из которых в каждый момент активно лишь одно) с одним маршрутизатором VPRN или множеством таких маршрутизаторов, механизм доступности оконечных каналов будет детектировать разрыв основного соединения и активизировать в таком случае одно из резервных. В описанной ситуации подключенный изначально граничный маршрутизатор VPRN перестает анонсировать доступность оконечному узлу, а активизированный вновь граничный маршрутизатор VPRN начнет анонсировать доступность активного канала, восстанавливая тем самым связность.

В другом варианте оконечный узел поддерживает множество активных одновременно каналов с использованием того или иного механизма распределения нагрузки. В этом случае множество граничных маршрутизаторов VPRN может иметь активные пути к оконечному узлу и анонсировать их через VPRN. В этом случае не должно возникать проблем с доступностью через VPRN, если используемый внутри VPRN механизм доступности поддерживает множество путей к одному адресному префиксу и используются подходящие механизмы предотвращения петель (например, с каждым анонсируемым префиксом связывается вектор удаленности).

5.5 Поддержка групповой адресации

Групповой и широковещательный трафик может поддерживаться через VPRN путем граничной репликации или за счет естественной поддержки групповой адресации в опорной сети. Оба случая более подробно рассматриваются ниже.

5.5.1 Граничная репликация

В этом варианте каждый граничный маршрутизатор VPRN реплицирует multicast-трафик для передачи через каждый канал в VPRN. Отметим, что такую же операцию выполняют маршрутизаторы CPE, завершающие физические каналы или выделенные соединения. Как и в случае с маршрутизаторами CPE протоколы групповой маршрутизации могут работать на каждом граничном маршрутизаторе VPRN для определения дерева распространения группового трафика и, следовательно, снижения уровня ненужного лавинного трафика. Это можно реализовать с помощью экземпляров стандартных протоколов групповой маршрутизации (например, PIM[1] [39] или DVMRP[2] [40]) между всеми граничными маршрутизаторами VPRN через туннели VPRN так же, как обычные протоколы маршрутизации могут работать на каждом граничном маршрутизаторе VPRN для определения доступности внутри VPN (см. параграф 5.3.4). Другим вариантом может служить использование протоколов доступности канала на туннелях VPRN для определения доступности внутри VPRN, который дополнительно может позволять граничным маршрутизаторам VPRN индицировать конкретные группы, запрашивающие прием информации на каждом сайте, а также источники групповой информации на каждом сайте.

В любом случае требуется тот или иной механизм, который позволил бы граничным маршрутизаторам VPRN определять какие конкретные multicast-группы были запрошены и какие источники имеются на каждом сайте. Реализация такого механизма в общем случае определяется возможностями оконечных маршрутизаторов CPE на каждом сайте. Если используются протоколы групповой маршрутизации, они могут напрямую взаимодействовать с эквивалентными протоколами на каждом граничном маршрутизаторе VPRN. Если CPE не использует протоколов групповой маршрутизации тогда в отсутствии IGMP[3]-прокси [41] пользовательский сайт будет ограничен одной подсетью, подключенной к граничному маршрутизатору VPRN через устройство с функциями моста, поскольку область действия сообщений IGMP ограничена подсетью. Однако за счет применения IGMP-прокси маршрутизатор CPE может

[1]Protocol Independent Multicast — независимая от протокола групповая адресация.
[2]Distance Vector Multicast Routing Protocol — протокол групповой маршрутизации на основе векторов удаленности.
[3]Internet Group Management Protocol — протокол управления группами в Internet.

реализовать групповую пересылку без использования протокола групповой маршрутизации (с некоторыми топологическими ограничениями). На своих интерфейсах в сторону пользовательского сайта маршрутизатор CPE выполняет функции маршрутизации IGMP, а на интерфейсе к граничному маршрутизатору VPRN - функции хоста IGMP.

5.5.2 Естественная поддержка групповой адресации

В этом варианте граничные маршрутизаторы VPRN отображают внутренний (intra-VPRN) групповой трафик на естественный механизм распространения группового трафика IP через опорную сеть. Отметим, что для внутреннего группового трафика предъявляются такие же требования по изоляции от общего трафика опорной сети, как и для индивидуального трафика внутри VPRN. В настоящее время единственным механизмом туннелирования IP с такой поддержкой является MPLS. С другой стороны, хотя MPLS поддерживает механизмы естественной транспортировки групповых пакетов IP, для поддержки внутреннего группового трафика VPRN требуется усиление этих механизмов.

Например, каждый маршрутизатор VPRN может добавлять перед групповым адресом в каждой VPRN идентификатор VPN-ID для данной VPRN и распространять такую связку далее, трактуя пару «VPN-ID-групповой адрес внутри VPRN», как обычный групповой адрес в рамках магистральных протоколов групповой маршрутизации, как это делается в рассмотренном выше случае доступности индивидуальных адресов. Механизмы группового распространения меток MPLS могут применяться для организации подходящих групповых LSP с целью соединения сайтов внутри каждой VPRN, поддерживающей конкретные групповые адреса. Отметим, однако, что это потребует от каждого промежуточного LSR не только знать о multicast-группах внутри VPRN, но и поддерживать интерпретацию измененных анонсов. Могут быть также определены механизмы отображения multicast-групп из VPRN на группы опорной сети.

В других механизмах туннелирования IP нет естественной поддержки групповой адресации. Может оказаться целесообразным расширение таких механизмов туннелирования за счет выделения групповых адресов IP для VPRN в целом и, следовательно, распространение внутреннего группового трафика VPRN в групповых пакетах опорной сети. Граничные маршрутизаторы VPRN могут отфильтровывать пакеты нежелательных групп. В дополнение к этому могут быть определены механизмы, позволяющие выделить групповые адреса опорной сети для конкретных групп в VPRN и потом использовать их через протоколы групповой маршрутизации опорной сети, как описано выше, для ограничения пересылки группового трафика VPRN только входящим в группу узлам.

С использованием естественной поддержки групповой адресации связан вопрос обеспечения защиты для multicast-трафика. В отличие от случая с граничной репликацией, где наследуются параметры защиты туннеля, для естественной поддержки группового трафика потребуется применение тех или иных механизмов защиты multicast-трафика. Разработка архитектуры и решений по защите группового трафика является областью исследований (см., например, [42] и [43]). Рабочая группа SMuG[1] в рамках IRTF подготовила прототипы решений, которые были переданы в рабочую группу IETF IPSec для стандартизации.

Однако для развертывания масштабируемых механизмов защиты при естественной поддержке групповой адресации этого пока не достаточно.

5.6 Рекомендации

Множество предложений, разработанных для поддержки тех или иных форм функциональности VPRN, можно разделить на две больших группы — в одной используется модель добавления в пакеты протоколов маршрутизации для распространения сведений о принадлежности к VPN и/или доступности ([13],[15]), а в другой те же цели достигаются за счет применения виртуальных маршрутизаторов ([12],[14]). В некоторых случаях описанные механизмы опираются на свойства конкретной архитектуры (например, MPLS), а не IP.

В контексте модели виртуальной маршрутизации может оказаться полезной разработка протокола распространения информации о принадлежности на основе каталога или MIB. При объединении с протокольными расширениями для протоколов туннелирования IP, как описано в параграфе 3.2, это обеспечит основу для полного набора протоколов и механизмов, поддерживающих интероперабельные VPRN, которые могут распространяться через множество административных доменов в опорной сети IP. Отметим, что основными функциональными компонентами, которые требуются, являются определение и распространение информации о доступности, которые могут быть реализованы с помощью экземпляров стандартных протоколов маршрутизации без каких-либо расширений.

Для полносвязной топологии полезность разработки протокола доступности канала может быть проверена, однако ограничения и проблема масштабирования, связанные с такой топологией, снижают осмысленность такой разработки, поскольку стандартные протоколы могут применяться и в этом случае.

Рассмотрены также расширения протоколов маршрутизации, позволяющие передавать VPN-ID в маршрутных обновлениях, и отмечено, что при использовании специфических для VPN туннелей такие расширения не требуется.

6.0 Типы VPN — коммутируемые соединения

Виртуальные сети VPDN[2] позволяют удаленным пользователям подключаться к сети через организованный по запросу туннель. Пользователь соединяется с IP-сетью общего пользования по коммутируемой линии PSTN или ISDN и пакеты туннелируются через публичную сеть на желаемый сайт, как будто пользователь подключился к этому сайту напрямую. Основной характеристикой таких соединений является необходимость аутентификации пользователей, поскольку потенциально доступ к сайту через коммутируемую телефонную сеть открыт для всех.

Сегодня во многих корпоративных сетях разрешен доступ пользователей по коммутируемым линиям через сети PSTN, когда пользователь организует соединение PPP с сервером доступа, на котором сессия PPP аутентифицируется с использованием систем AAA на основе стандартных протоколов типа Radius [44]. С учетом повсеместного развертывания подобных систем любая система VPDN на практике должна позволять почти прозрачное взаимодействие с ними.

[1]Secure Multicast Group.
[2]Virtual Private Dial Network — виртуальная частная сеть с доступом по коммутируемым линиям.

В рамках IETF был разработан протокол L2TP[1] [8], который позволяет организовывать пользовательские сессии PPP через связку между LAC[2] и удаленным сервером LNS[3]. Сам протокол L2TP основан на двух более ранних протоколах - L2F[4] [45] и PPTP[5] [46], что отразилось в двух достаточно разных сценариях применения L2TP (вынужденное и добровольное туннелирование), описанных в параграфах 6.2 и 6.3.

В этом документе рассматривается применение L2TP в сетях IP (с использованием UDP), но протокол L2TP может и напрямую работать «поверх» таких протоколов, как ATM или Frame Relay. Вопросы, связанные с использованием L2TP в сетях без протокола IP (например, защита туннелей), в этом документе не рассматриваются.

6.1 Характеристики протокола L2TP

В этом разделе рассматриваются характеристики туннельного протокола L2TP в свете категорий, отмеченных в разделе 3.0.

6.1.1 Мультиплексирование

L2TP имеет встроенную поддержку мультиплексирования вызовов множества пользователей через один канал. Между парой конечных точек IP может существовать множество туннелей L2TP (различаются по tunnel-id), а через один туннель может быть организовано множество сессий (различаются по session-id).

6.1.2 Сигнализация

Сигнализация поддерживается встроенным протоколом соединений, позволяющим динамически организовывать как туннели, так и сессии.

6.1.3 Защита данных

Обеспечивая прозрачное расширение PPP для пользователей через связку от LAC до LNS, протокол L2TP позволяет для организации соединений и передачи данных применять любые механизмы защиты, которые могут использоваться с обычными соединениями PPP. Однако это не обеспечивает защиты для самого протокола L2TP. По этой причине для защиты L2TP можно использовать его совместно с IPSec для сетей IP [47], [48] или аналогичными механизмами для опорных сетей без IP [49].

Взаимодействие L2TP с системами AAA для аутентификации и проверки полномочий пользователей зависит от конкретного применения L2TP и устройств, поддерживающих функции LAC и LNS. Эти вопросы подробно рассмотрены в [50].

Средства определения хостом корректного LAC для подключения и определения устройством LAC пользователей для направления трафика в туннель, а также параметры LNS, связанные с каждым пользователем, выходят за рамки VPDN. Эти вопросы могут быть решены, например, с помощью спецификаций Internet-роуминга [51].

6.1.4 Мультипротокольный транспорт

L2TP транспортирует пакеты PPP (и только их) и, таким образом, может служить для поддержки мультипротокольного трафика, поскольку PPP является мультипротокольным.

6.1.5 Упорядочивание

L2TP поддерживает упорядоченную доставку пакетов. Эта возможность может быть согласована при организации сессии, а также может быть отключена или включена LNS непосредственно в сессии. Поле порядкового номера в L2TP может также служить для индикации отбрасывания пакетов, которая нужна для корректной работы разных алгоритмов сжатия PPP. Если сжатие не используется и LNS считает, что используемому протоколу (указанному при согласовании PPP NCP) не требуется упорядоченной доставки пакетов (например, IP), сохранение порядка может быть отключено.

6.1.6 Поддержка туннелей

L2TP использует протокол keepalive для того, чтобы отличать отказы в туннелях от продолжительных периодов бездействия.

6.1.7 Большие MTU

Протокол L2TP не имеет встроенной поддержки фрагментации и сборки пакетов, но при необходимости может воспользоваться IP для случаев работы «поверх» UDP/IP. Отметим, что устройства LAC и LNS для предотвращения фрагментации могут изменять значение MRU[6], согласованное через PPP, если им известно значение MTU на пути между LAC и LNS. Для этого предложено разрешить применение MTU в тех случаях, когда L2TP служит для транспортировки IP [52].

6.1.8 Туннельные издержки

L2TP при использовании в сетях IP работает на основе транспорта UDP и должен применяться для переноса трафика PPP. Это приводит к значительным издержкам как на уровне данных в заголовках UDP, L2TP и PPP, так и на уровне управления L2TP и PPP. Более подробно эти вопросы рассмотрены в параграфе 6.3.

6.1.9 Управление потоками и контроль перегрузок

L2TP поддерживает механизмы управления потоками и контроля перегрузок для протокола управления, но не для трафика данных. Более подробная информация приведена в параграфе 3.1.9.

---

[1] Layer 2 Tunneling Protocol — протокол туннелирования на уровне 2.
[2] L2TP Access Concentrator — концентратор доступа L2TP.
[3] L2TP Network Server — сетевой сервер L2TP.
[4] Layer 2 Forwarding protocol — протокол пересылки на уровне 2.
[5] Point-to-Point Tunneling Protocol — протокол туннелирования «точка-точка».
[6] Maximum Receive Unit — максимальный принимаемый блок.

6.1.10 QoS и управление трафиком

Заголовок L2TP содержит 1-битовое поле приоритета, которое может быть установлено для пакетов, обладающих преимуществами (например, keepalive) при размещении в локальных очередях и передаче. Благодаря прозрачному расширению PPP, L2TP имеет встроенную поддержку таких механизмов PPP, как multi-link PPP [53] и связанные с ним протоколы управления [54], что позволяет управлять полосой канала по запросам пользователей.

Кроме того, вызовы L2TP могут отображаться на базовые механизмы управления трафиком, которые могут существовать в сети, и есть предложения по передаче через сигнализацию L2TP запросов на выбор дифференцированного обслуживания [55].

6.1.11 Разное

Поскольку протокол L2TP разработан для прозрачного расширения PPP, он не пытается заменить обычные механизмы выделения адресов, связанные с PPP. Следовательно, инициирующий сессию PPP хост будет получать адрес через LNS, используя процедуры PPP. Эта адресация может быть не связана с адресацией, используемой для коммуникаций между LAC и LNS. LNS потребуется также поддерживать механизмы пересылки, которые нужны для маршрутизации трафика удаленного хоста.

6.2 Вынужденное туннелирование

Вынужденным туннелирование называют ситуацию, когда сетевой узел (например, сервер доступа в сеть), действующий как LAC, расширяет сессию PPP через опорную сеть с помощью L2TP до удаленного LNS, как показано ниже. Эта операция прозрачна для пользователя, инициирующего сессию PPP с LAC. Это позволяет избавиться от привязки места и принадлежности модемных пулов, используемых для телефонных соединений, к сайту, с которым пользователю нужно соединиться. Поддержка такого сценария была исходной задачей разработки спецификации L2F, которая послужила основой для L2TP .

Существует множество разных сценариев развертывания. В одном из примеров, показанном на рисунке, абонентский хост соединяется с NAS, действующим в качестве LAC, и организуется туннель через сеть IP (например, Internet) до шлюза, действующего как LNS. Шлюз обеспечивает доступ в корпоративную сеть и может быть устройством данной сети или граничным маршрутизатором ISP, если поддержка функций LNS передана на обслуживание ISP. Другим примером может служить использование ISP протокола L2TP для предоставления пользователям доступа в Internet. Пользовательский хост соединяется с NAS, действующим в качестве LAC, и организуется туннель через сеть доступа до граничного маршрутизатора ISP, который служит LNS. Этот граничный маршрутизатор ISP пробрасывает пользовательский трафик в Internet. В других сценариях ISP применяет L2TP для обеспечения пользователям доступа в VPRN или одновременного соединения с VPRN и Internet.

VPDN с использованием вынужденного или добровольного туннелирования можно рассматривать как другой метод доступа для пользовательского трафика, который может обеспечивать соединения между разными типами сетей (например, корпоративная сеть, Internet или VPRN). Последний вариант может также служить примером обеспечения услуг VPN для случая разнотипных VPN.

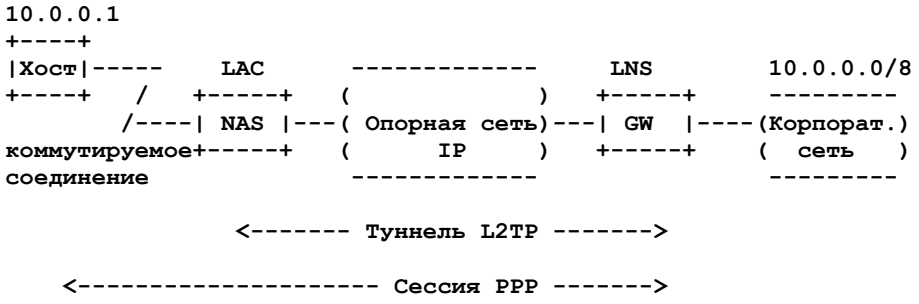

Рисунок 6.1. Пример вынужденного туннелирования.

Вынужденное туннелирование изначально предназначалось для развертывания серверов доступа с поддержкой коммутируемых линий, позволяющих подключаться через сети общего пользования к корпоративным сайтам без необходимости организовывать на этих сайтах свои серверы доступа. Другим примером может служить передача ISP функций доступа по телефонным линиям сторонней организации (такой, как LEC[1] в США), которая обслуживает множество ISP. Позднее было предложено использовать вынужденное туннелирование для служб DSL[2] [56] [57], использующих существующую инфраструктуру AAA.

Маршрутизация вызовов для вынужденного туннелирования требует возможности использования некоторых аспектов организации соединений PPP, позволяющих LAC определить идентичность LNS. Как отмечено в [50], эти аспекты могут включать идентификацию пользователей с помощью тех или иных сети доступа или атрибутов вызывающей стороны (например, FQDN[3]) для использования в процедурах аутентификации PPP.

Можно также связать воедино два туннеля L2TP, когда LAC будет инициировать туннель с промежуточным устройством, которое играет роль LNS для этого первого LAC и роль LAC для конечного LNS. Такое решение может потребоваться в соответствии с административными, организационными или нормативными требованиями в части разделения сетей доступа, опорных сетей IP и корпоративных сетей.

6.3 Добровольные туннели

Добровольным туннелированием называют случай, когда отдельные хосты подключаются к удаленному сайту с использованием туннеля, начинающегося на данном хосте и не включающего промежуточных сетевых узлов, как показано на рисунке ниже. Спецификация PPTP, частично включенная в L2TP, служит базой для таких туннелей.

[1]Local Exchange Carrier — локальный коммутатор (телефонный).
[2]Digital Subscriber Line — цифровая абонентская линия.
[3]Fully Qualified Domain Name — полное доменное имя.

Как и для вынужденного туннелирования здесь возможны разные сценарии развертывания. На рисунке ниже показан абонентский хост, подключающийся к корпоративной сети с использованием L2TP или IPSec в качестве механизма туннелирования. К другим вариантам добровольного туннелирования относится доступ пользователей в VPRN.

6.3.1 Вопросы использования L2TP для добровольных туннелей

Спецификация протокола L2TP поддерживает добровольное туннелирование, поскольку LAC может размещаться на хостах, а не только на узлах сети. Отметим, что такой хост имеет два адреса IP — один для туннеля LAC-LNS, а другой (обычно выделяется протоколом PPP) — для сети, к которой этот хост подключается. Преимущество использования L2TP для добровольного туннелирования заключается в возможности применения имеющихся механизмов аутентификации и выделения адресов PPP без каких-либо изменений. Например, LNS может включать клиент Radius и взаимодействовать с сервером Radius для аутентификационного обмена PPP PAP или CHAP, а также для получения конфигурационных данных для хоста (IP-адрес и список серверов DNS). Эта информация может быть передана хосту по протоколу PPP IPCP.

Рисунок 6.2. Пример добровольного туннелирования.

Однако приведенная выше процедура не является дармовой. Здесь возникают существенные издержки, связанные со стеком протоколов, особенно в тех случаях, когда для обеспечения безопасности требуется использовать, а также в случаях подключения хоста по низкоскоростному коммутируемому каналу. Издержки включают дополнительные заголовки в пакетах данных, а также дополнительные протоколы, которые приходится использовать на уровне управления. Например, при использовании L2TP с защитой IPSec приложение web будет работать через стек

HTTP/TCP/IP/PPP/L2TP/UDP/ESP/IP/PPP/AHDLC

В работе [58] предложено снижать издержки для добровольных туннелей за счет использования только IPSec

HTTP/TCP/IP/ESP/IP/PPP/AHDLC

В этом случае IPSec используется в туннельном режиме и туннель завершается на граничном шлюзе IPSec в сети предприятия или граничном маршрутизаторе провайдера, подключенном к корпоративной сети. Для адресации хоста есть два варианта. Может использоваться два адреса, как в случае L2TP. Хост может также использовать один публичный адрес IP в поле источника для внутренних и внешних заголовков IP при использовании шлюза NAT[1] на пути пересылки пакетов в корпоративную сеть. Для других хостов корпоративной сети хост всегда будет виден с «внутренним» адресом IP. Использование NAT связано с некоторыми ограничениями, рассмотренными в [58].

Другой возможной проблемой, связанной с PPP, является тот факт, что характеристики канального уровня в туннеле L2TP через опорную сеть IP достаточно сильно отличаются от характеристик канального уровня на последовательной линии, как указано в спецификации L2TP. Например, неаккуратно выбранные параметры PPP могут приводить к частым сбросам и тайм-аутам, особенно при использовании компрессии. Это связано с тем, что туннель L2TP может изменять порядок следования пакетов, а также отбрасывать их без уведомления, чего обычно не происходит в последовательных линиях. Частота потери пакетов также может оказаться значительно выше в результате перегрузок в сети. Использование порядковых номеров в заголовках L2TP позволяет решить проблему нарушения порядка и для случаев, когда LAC и LNS являются конечными точками PPP (как при добровольном туннелировании) поле порядкового номера может применяться для обнаружения отбрасывания пакетов и передачи соответствующей информации функциям компрессии, которым эти данные позволяют поддерживать синхронизацию сторон. Однако проблема сохраняется для вынужденного туннелирования, поскольку в этом случае LAC может осознанно передавать поврежденные кадры хосту PPP для индикации потери пакетов, но часть оборудования не будет это позволять.

6.3.2 Вопросы использования IPSec для добровольных туннелей

При использовании IPSec для добровольного туннелирования функции аутентификации пользователей и настройки конфигурации хоста, выполняемые с помощью PPP, для случая L2TP также нужно обеспечивать. Следует отметить различия между аутентификацией пользователя и аутентификацией устройства. Двухфакторная аутентификация выполняется с использованием двух элементов из числа перечисленных — компьютер или смарт-карта с цифровым сертификатом, пароль пользователя и т. п. (вариант двухфакторной аутентификации используется в банкоматах — нужно предъявить карту и номер PIN). Многие из унаследованных систем аутентификации пользователей асимметричны по своей природе и не могут поддерживаться IKE. Для систем удаленного доступа в большинстве случаев применяется аутентификация PPP между пользователем и сервером доступа и Radius между серверами доступа и аутентификации. Аутентификационный обмен в этом случае (например, PAP или CHAP) является асимметричным. CHAP поддерживает возможность повтора аутентификации пользователя в любой момент в течение сессии для проверки того, что пользователем является тот же человек, который организовал сеанс.

Протокол IKE обеспечивает строгую аутентификацию машин, однако поддержка аутентификации пользователей ограничена и асимметричная аутентификация пользователей не поддерживается. Хотя пользовательский пароль может применяться для создания ключей, используемых в качестве preshared, его невозможно использовать с IKE Main Mode в среде удаленного доступа, поскольку у пользователя не будет фиксированного адреса IP, а в режиме

[1]Network Address Translation — трансляция сетевых адресов.

Aggressive Mode не обеспечивается защиту идентичности. По этой причине предложено множество решений для поддержки традиционных схем асимметричной аутентификации пользователей с IPSec. В работе [59] определен новый обмен сообщениями IKE (transaction exchange), разрешающий последовательности сообщений Request/Reply и Set/Acknowledge, а также определены атрибуты, которые могут применяться для настройки клиентского стека IP. В работах [60] и [61] описаны механизмы использования такого обмена сообщениями в промежутке между обменами IKE Phase 1 и Phase 2 для аутентификации пользователей. Другое предложение (без расширения самого протокола IKE) описано в [62]. В этой модели пользователь организует Phase 1 SA со шлюзом защиты, а потом организует Phase 2 SA со шлюзом, через который работает существующий протокол аутентификации. Шлюз служит посредником и транслирует протокольные сообщения серверу аутентификации.

Кроме того, были предложения настраивать для удаленного хоста адрес IP и другие протоколы конфигурации через IPSec. Например, в работе [63] описан метод, в котором удаленный хост сначала организует Phase 1 SA с защитным шлюзом, а затем Phase 2 SA со шлюзом, через который работает протокол DHCP. Шлюз служит посредником и транслирует протокольные сообщения серверу DHCP. Подобно предложению из [62], здесь не вносится изменений в сам протокол IKE.

Еще один аспект функциональности PPP, поддержка которого может потребоваться в мультипротокольной среде, - это необходимость передачи протоколов сетевого уровня, отличных от IP, и даже протоколов канального уровня (например, Ethernet) для организации мостов через IPSec. Этот вопрос рассмотрен в параграфе 3.1.4.

Методы поддержки традиционной аутентификации пользователей и настройки конфигурации хостов в среде с удаленным доступом в настоящее время являются предметом обсуждения в рабочей группе IPSec.

6.4 Хосты в локальных сетях

Основанная на протоколе PPP современная модель доступа по коммутируемым линиям предполагает прямое соединение хоста с ориентированной на соединения телефонной сетью. Разработанные позднее новые технологии доступа (например, DSL) пытались воспользоваться это моделью [57], чтобы сохранить существующие системы AAA. Однако распространение ПК, принтеров и других сетевых приложений в домах и небольших компаниях, а также снижение стоимости сетей породили альтернативу модели прямого подключения хостов. В результате возникла модель подключения хостов к Internet через небольшие (обычно, Ethernet) локальные сети.

Следовательно, возникла потребность приспособить существующую у сервис-провайдеров инфраструктуру AAA для поддержки подключения множества хостов с одного сайта. Основным осложнением, связанным с таким сценарием, является необходимость поддержки диалога при входе в сеть (login), в котором осуществляется обмен информацией AAA. Ниже описано несколько вариантов преодоления этих сложностей.

6.4.1 Расширение PPP на хосты с использованием L2TP

Было внесено множество предложений (например, [56]) по расширению L2TP через Ethernet, позволяющему сетевым хостам организовывать сессии PPP за пределы сети так же, как это делается для обычных хостов.

6.4.2 Непосредственное расширение PPP на хосты

Существует также спецификация для отображения PPP непосредственно в Ethernet (PPPOE) [64], в которой используется широковещательный механизм для обеспечения хостам возможности поиска серверов доступа для подключения к ним. Такие серверы могут при необходимости туннелировать сессии PPP дальше, используя L2TP или похожий механизм.

6.4.3 Использование IPSec

Рассмотренные выше механизмы добровольного туннелирования на основе IPSec могут применяться как для подключенных непосредственно, так и для сетевых хостов.

Отметим, что для всех этих методов на хостах требуется использовать дополнительные программы, которые поддерживают функциональность LAC, клиента PPPOE или клиента IPSec.

6.5 Рекомендации

Спецификация L2TP завершена и будет широко применяться для вынужденного туннелирования. Как было отмечено в параграфе 3.2, определение конкретных режимов работы IPSec для защиты L2TP будет обеспечивать преимущества.

Для добровольных туннелей с применением IPSec требуется дополнительная работа с целью обеспечить поддержку:

- традиционной асимметричной аутентификации пользователей (6.3);
- выделение адресов и настройку конфигурации хостов (6.3).

Требуется также решение ряда других вопросов, связанных с поддержкой удаленных хостов. В настоящее время имеется много несовместимых между собой решений.

7.0 Типы VPN - VPLS

VPLS[1] представляет собой эмуляцию сегмента ЛВС с использованием Internet. VPLS может использоваться для организации прозрачного транспорта TLS[2], который может служить для соединения множества оконечных узлов CPE (мостов и маршрутизаторов) независимо от протоколов. VPLS эмулирует сегмент ЛВС через сеть IP так же, как LANE эмулирует сегмент ЛВС через сеть ATM. Основным преимуществом VPLS является полная прозрачность для протоколов, что может быть важно как с точки зрения поддержки разных протоколов, так и в плане выполнения требований регуляторов в контексте конкретных сервис-провайдеров.

[1]Virtual Private LAN Segment — сегмент виртуальной частной ЛВС.
[2]Transparent LAN Service — прозрачные услуги ЛВС.

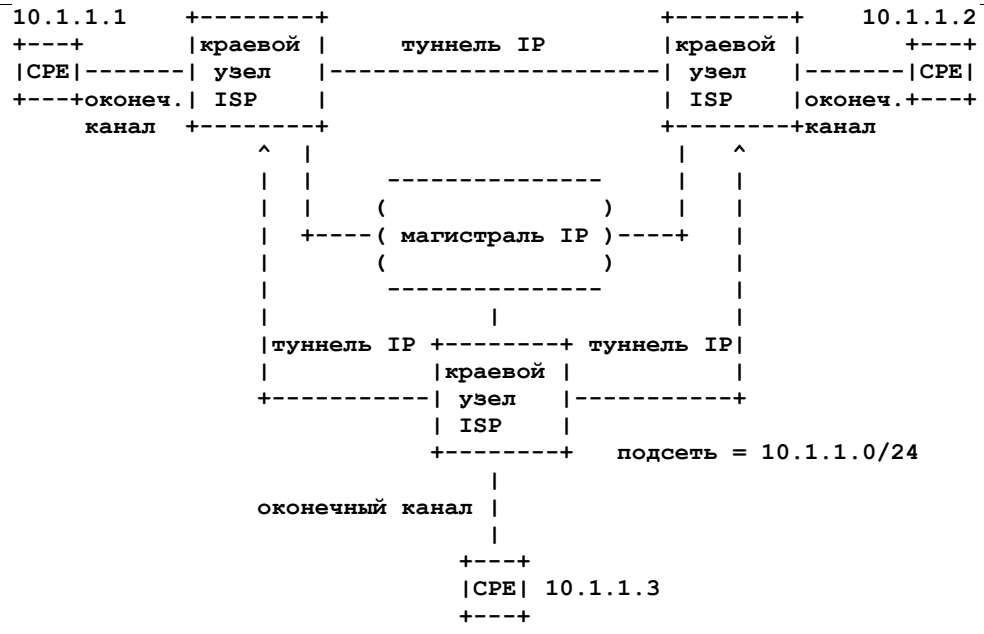

Рисунок 7.1. Пример VPLS.

7.1 Требования VPLS

С точки зрения топологии и работы VPLS очень напоминают VPRN, за исключением того, что каждый граничный узел VPLS реализует мост канального уровня, а не маршрутизацию на сетевом уровне. Таким образом, большая часть рассмотренных выше механизмов туннелирования и настройки VPRN может использоваться для VPLS с соответствующими изменениями для работы с канальным уровнем, взамен сетевого. В последующих параграфах описаны основные изменения, которые нужно внести в работу VPRN для поддержки VPLS.

7.1.1 Протоколы туннелирования

Используемые в VPLS протоколы туннелирования могут в точности совпадать с применяемыми для VPRN, если соответствующий протокол позволяет туннелировать мультипротокольный трафик. Ниже предполагается, что это условие выполнено.

7.1.2 Поддержка групповой и широковещательной адресации

Для VPLS требуется поддержка широковещания. Это нужно как для широковещательных кадров, так и для лавинной рассылки пакетов на канальном уровне, когда индивидуальный (unicast) кадр рассылается всем (лавинно) по причине отсутствия данных о пути к адресату. Протокол преобразования адресов, работающий в сети на базе мостов, обычно тоже использует широковещательные кадры (например, ARP). Набор механизмов с поддержкой группового трафика, рассмотренный выше для VPRN, может использоваться и для VPLS, хотя более частое в общем случае применение широковещания в VPLS может оказывать сильное давление на естественную поддержку групповой адресации (например, снизить издержки репликации на граничных узлах VPLS).

7.1.3 Конфигурация принадлежности к VPLS и топология

Настройка конфигурации VPLS аналогична случаю VPRN, поскольку требует лишь информации о локальной связи каналов с VPN только для данного граничного узла VPLS и идентификация других граничных маршрутизаторов VPLS или маршрутов к ним. В частности, конфигурация не зависит от природы пересылки на каждом граничном узле VPN. Поэтому все механизмы определения принадлежности к VPN и распространения этой информации, описанные выше для VPRN, применимы и для конфигурации VPLS. Как и для случая VPRN, топологией VPLS можно легко управлять на уровне конфигурации партнерских узлов в каждом граничном маршрутизаторе VPLS в предположении, что механизм распространения информации о принадлежности позволяет это делать. Ясно, что типовая VPLS будет полносвязной, однако для исключения необходимости передачи трафика между двумя узлами VPLS через третий (транзитный) узел VPLS требуется использовать протокол Spanning Tree [65] предотвращающий возникновение петель.

7.1.4 Типы оконечных узлов CPE

VPLS может поддерживать в качестве устройств CPE мосты или маршрутизаторы.

CPE-маршрутизаторами будут прозрачно организовывать партнерские связи через VPLS без необходимости организации между ними партнерских отношений в рамках VPLS. Проблемы масштабирования, возникающие для полносвязной топологии VPRN, применимы и для этого случая, но в данной ситуации число маршрутизаторов-партнеров потенциально больше, поскольку маршрутизаторы ISP не являются больше точками агрегирования.

Области широковещания CPE-мостов охватывают все CPE сайтов, а также саму VPLS. Это создает существенные ограничения по масштабированию, поскольку требует лавинной рассылки пакетов и любое изменение топологии в домене на базе мостов является нелокальным и затрагивает весь домен. По этой причине данный вариант подходит лишь для поддержки немаршрутизируемых протоколов.

Природа CPE определяет протоколы инкапсуляции, адресации, пересылки и определения доступности в VPLS, которые будут рассмотрены ниже.

7.1.5 Инкапсуляция пакетов оконечного канала

7.1.5.1 CPE-мост

В этом случае пакеты передаются в сеть VPLS и из нее через канал доступа в кадрах канального уровня с подходящей для канала доступа инкапсуляцией. Наиболее частым является использование кадров Ethernet к подходящей для конкретной технологии доступа инкапсуляцией (например, использование ATM для подключения мостов CPE к граничным узлам VPLS). Такие кадры тогда пересылаются на уровне 2 в туннель, используемый в VPLS. Как было отмечено выше, это требует использовать протокол туннелирования IP, позволяющий транспортировать такие кадры канального уровня. Отметим, что это обязательно не всегда, однако применение поля идентификации протокола в каждом туннельном пакете, как природа инкапсулированного трафика (например, кадров Ethernet) может быть указано при организации туннеля.

7.1.5.2 CPE-маршрутизатор

В этом случае маршрутизаторы CPE обмениваются пакетами с VPLS через оконечные каналы, адресуя их на канальном уровне партнерским маршрутизаторам CPE. Могут оказаться полезными и другие типы инкапсуляции. Однако, поскольку VPLS, к которой подключены только маршрутизаторы CPE, требуется сравнительно ограниченное адресное пространство, дополнительная инкапсуляция может использоваться, как показано ниже.

7.1.6 Адресация CPE и трансляция адресов

7.1.6.1 CPE-мост

Поскольку VPLS работает на канальном уровне, все хосты на оконечных сайтах в случае CPE-моста обычно будут находиться в одной подсети (возможно и наличие множества подсетей в одной ЛВС, но такие случаи не типичны). Кадры пересылаются в VPLS и через нее на основе адресов канального уровня (например, IEEE MAC), связанных с отдельными хостами. В VPLS требуется поддержка широковещательного трафика, поскольку он обычно используется механизмами преобразования адресов для отображения адресов сетевого уровня на адреса канального уровня. Для VPLS требуются также алгоритмы пересылки и определения доступности с целью обработки лавинного трафика.

7.1.6.2 CPE-маршрутизатор

Для соединения маршрутизаторов CPE через VPLS обычно применяется одна подсеть сетевого уровня. Хосты за каждым маршрутизатором CPE находятся в разных подсетях сетевого уровня. Маршрутизаторы CPE передают пакеты через VPLS отображая сетевой адрес следующего интервала на адрес партнерского маршрутизатора на канальном уровне. Инкапсуляция канального уровня (обычно Ethernet) используется как для случая мостов.

Однако, как отмечено выше, в случаях, когда все узлы CPE, подключенные к VPLS, являются маршрутизаторами, по причине ограничений адресного пространства VPLS для инкапсуляции может применяться адресное пространство, отличное от MAC. Например, в [11] предложен механизм для организации VPLS через сети MPLS, основанный на более раннем механизме организации VPRN через MPLS [38], где предлагается использовать MPLS в качестве механизма туннелирования и локально присваивать метки MPLS в качестве адресов канального уровня для идентификации маршрутизаторов CPE LSR, соединенных с VPLS.

7.1.7 Механизмы пересылки и доступности для краевых узлов VPLS

7.1.7.1 CPE-мост

Единственным практичным механизмом пересылки на границе VPLS в этом случае будет стандартная лавинная рассылка пакетов на канальном уровне и определение MAC-адресов, как описано в [65]. По этой причине нет необходимости в отдельном протоколе проверки доступности для VPLS, хотя нужен широковещательный механизм для лавинной рассылки, как отмечено выше. В общем случае нет необходимости поддерживать протокол Spanning Tree между граничными узлами VPLS, если топология VPLS такова, что граничные узла VPLS не используются для транзита трафика между любыми другими узлами VPLS (иными словами, имеется полная связность и транзит явно исключается). С другой стороны, CPE-мосты могут реализовать протокол остовного дерева для защиты от возникновения «обходных путей» мимо VPLS.

7.1.7.2 CPE-маршрутизатор

В этом случае могут использоваться стандартные технологии мостов. Кроме того, меньшее адресное пространство канального уровня в такой VPLS позволяет также использовать другие технологии с явными маршрутами канального уровня между маршрутизаторами CPE. В работе [11], например, предложено при добавлении в VPLS нового маршрутизатора CPE организовывать MPLS LSP между всеми CPE LSR. Это позволяет избавиться от необходимости лавинной рассылки пакетов. В более общем случае при использовании механизмов доступности для настройки в конфигурации граничных узлов VPLS адресов канального уровня подключенных к узлу маршрутизаторов CPE, модификации всех механизмов определения доступности внутри VPN, рассмотренные для VPRN, могут использоваться для распространения информации о доступности всем другим граничным узлам VPLS. Это позволяет организовать передачу пакетов через VPLS без лавинной рассылки.

Могут быть также разработаны механизмы для дальнейшего распространения адресов канального уровня партнерских маршрутизаторов CPE и соответствующих им адресов сетевого уровня через оконечные каналы к маршрутизаторам CPE, которые могут использовать полученную информацию для вставки в свои таблицы преобразования адресов. Это избавляет от необходимости использования широковещательных протоколов преобразования адресов через VPLS.

Ясно, что при определении явных маршрутов канального уровня через VPLS отпадает необходимость поддержки протоколов остовного дерева. При использовании обычных механизмов лавинной рассылки остовное дерево нужно лишь в тех случаях, когда организовать полносвязную сеть невозможно и узлы VPLS вынуждены пересылать транзитный трафик.

7.2 Рекомендации

Между сетями VPRN и VPLS много общего и, по возможности, эти сходства следует использовать для упрощения разработки и настройки. В частности, в сетях VPLS следует применять те же механизмы туннелирования и настройки принадлежности с учетом специфических характеристик VPLS.

8.0 Итоговые рекомендации

В этом документе разные типы VPN рассматривались по отдельности, однако есть множество общих требований и механизмов, применимых ко всем типам VPN, а во многих сетях используются комбинации разнотипных VPN. Общие свойства разнотипных VPN будут весьма полезны. В частности, эффективна будет стандартизация минимально возможного числа механизмов, которые позволили бы реализовать различные типы VPN.

Следует пристально изучить целесообразность добавления поддержки перечисленных ниже механизмов.

Для IKE/IPSec:

- транспортировка VPN-ID при организации SA (3.1.2);
- опции пустых (null) шифрования и аутентификации (3.1.3);
- мультипротокольная работа (3.1.4);
- упорядочение кадров (3.1.5);
- традиционная асимметричная аутентификация пользователей (6.3);
- выделение и настройка адресов хостов (6.3).

Для L2TP:

- определение режимов работы IPSec при использовании для поддержки L2TP (3.2).

Для VPN в целом:

- определение механизмов настройки и распространения информации о принадлежности к VPN на основе каталога или MIB (5.3.2);
- обеспечение в новых разработках поддержки максимального числа типов VPN вместо создания решений для единственного типа VPN.

9.0 Вопросы безопасности

Вопросы безопасности являются важной частью всех механизмов VPN и рассмотрены в параграфах, посвященных этим механизмам.

10.0 Благодарности

Спасибо Anthony Alles из Nortel Networks за его помощь при написании этого документа и разработку значительной части материала, на котором были основаны ранние версии документа. Спасибо также Joel Halpern за его полезные комментарии.

11.0 Литература

[1] ATM Forum. "LAN Emulation over ATM 1.0", af-lane-0021.000, January 1995.

[2] ATM Forum. "Multi-Protocol Over ATM Specification v1.0", af-mpoa-0087.000, June 1997.

[3] Ferguson, P. and Huston, G. "What is a VPN?", Revision 1, April 1 1998; http://www.employees.org/~ferguson/vpn.pdf.

[4] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[5] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401[1], November 1998.

[6] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[7] Hanks, S., Li, T., Farinacci, D. and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994.

[8] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. And B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[9] Rosen, E., et al., "Multiprotocol Label Switching Architecture", Work in Progress[2].

[10] Heinanen, J., et al., "MPLS Mappings of Generic VPN Mechanisms", Work in Progress.

[11] Jamieson, D., et al., "MPLS VPN Architecture", Work in Progress.

[12] Casey, L., et al., "IP VPN Realization using MPLS Tunnels", Work in Progress.

[13] Li, T. "CPE based VPNs using MPLS", Work in Progress.

[14] Muthukrishnan, K. and A. Malis, "Core MPLS IP VPN Architecture", Work in Progress[3].

[15] Rosen, E. and Y. Rekhter, "BGP/MPLS VPNs", RFC 2547, March 1999.

[1]Документ признан устаревшим и заменен RFC 4301. *Прим. перев.*
[2]Работа завершена и опубликована в RFC 3031. *Прим. перев.*
[3]Работа завершена и опубликована в RFC 2917. *Прим. перев.*

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

[17] Petri, B. (editor) "MPOA v1.1 Addendum on VPN support", ATM Forum, af-mpoa-0129.000.

[18] Harkins, D. and C. Carrel, "The Internet Key Exchange (IKE)", RFC 2409[1], November 1998.

[19] Calhoun, P., et al., "Tunnel Establishment Protocol", Work in Progress.

[20] Andersson, L., et al., "LDP Specification", Work in Progress[2].

[21] Jamoussi, B., et al., "Constraint-Based LSP Setup using LDP" Work in Progress[3].

[22] Awduche, D., et al., "Extensions to RSVP for LSP Tunnels", Work in Progress.

[23] Kent, S. and R. Atkinson, "IP Encapsulating Security Protocol (ESP)", RFC 2406[4], November 1998.

[24] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[25] Perez, M., Liaw, F., Mankin, A., Hoffman, E., Grossman, D. And A. Malis, "ATM Signalling Support for IP over ATM", RFC 1755, February 1995.

[26] Malkin, G. "RIP Version 2 Carrying Additional Information", RFC 1723, November 1994.

[27] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[28] Shacham, A., Monsour, R., Pereira, R. and M. Thomas, "IP Payload Compression Protocol (IPComp)", RFC 2393[5], December 1998.

[29] Duffield N., et al., "A Performance Oriented Service Interface for Virtual Private Networks", Work in Progress.

[30] Jacobson, V., Nichols, K. and B. Poduri, "An Expedited Forwarding PHB", RFC 2598, June 1999.

[31] Casey, L., "An extended IP VPN Architecture", Work in Progress.

[32] Rekhter, Y., and T. Li, "A Border Gateway Protocol 4 (BGP-4)," RFC 1771, March 1995.

[33] Grossman, D. and J. Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", RFC 2684, September 1999.

[34] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[35] Boyle, J., et al., "The COPS (Common Open Policy Service) Protocol", RFC 2748, January 2000.

[36] MacRae, M. and S. Ayandeh, "Using COPS for VPN Connectivity", Work in Progress.

[37] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[38] Heinanen, J. and E. Rosen, "VPN Support with MPLS", Work in Progress.

[39] Estrin, D., Farinacci, D., Helmy, A., Thaler, D., Deering, S., Handley, M., Jacobson, V., Liu, C., Sharma, P. and L. Wei, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", RFC 2362, June 1998.

[40] Waitzman, D., Partridge, C., and S. Deering, "Distance Vector Multicast Routing Protocol", RFC 1075, November 1988.

[41] Fenner, W., "IGMP-based Multicast Forwarding (IGMP Proxying)", Work in Progress.

[42] Wallner, D., Harder, E. and R. Agee, "Key Management for Multicast: Issues and Architectures", RFC 2627, June 1999.

[43] Hardjono, T., et al., "Secure IP Multicast: Problem areas, Framework, and Building Blocks", Work in Progress.

[44] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[45] Valencia, A., Littlewood, M. and T. Kolar, "Cisco Layer Two Forwarding (Protocol) "L2F"", RFC 2341, May 1998.

[46] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. And G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999.

[47] Patel, B., et al., "Securing L2TP using IPSEC", Work in Progress.

[48] Srisuresh, P., "Secure Remote Access with L2TP", Work in Progress.

[49] Calhoun, P., et al., "Layer Two Tunneling Protocol "L2TP" Security Extensions for Non-IP networks", Work in Progress.

[50] Aboba, B. and Zorn, G. "Implementation of PPTP/L2TP Compulsory Tunneling via RADIUS", Work in progress.

[51] Aboba, B. and G. Zorn, "Criteria for Evaluating Roaming Protocols", RFC 2477, January 1999.

[52] Shea, R., "L2TP-over-IP Path MTU Discovery (L2TPMTU)", Work in Progress.

[53] Sklower, K., Lloyd, B., McGregor, G., Carr, D. and T. Coradetti, "The PPP Multilink Protocol (MP)", RFC 1990, August 1996.

[54] Richards, C. and K. Smith, "The PPP Bandwidth Allocation Protocol (BAP) The PPP Bandwidth Allocation Control Protocol (BACP)", RFC 2125, March 1997.

[55] Calhoun, P. and K. Peirce, "Layer Two Tunneling Protocol "L2TP" IP Differential Services Extension", Work in Progress.

[1] Документ признан устаревшим и заменен RFC 4306. *Прим. перев.*
[2] Работа завершена и опубликована в RFC 3036, впоследствии замененном RFC 5036. *Прим. перев.*
[3] Работа завершена и опубликована в RFC 3212. *Прим. перев.*
[4] Документ признан устаревшим и заменен RFC 4303 и RFC 4305. *Прим. перев.*
[5] Документ признан устаревшим и заменен RFC 3173. *Прим. перев.*

[56] ADSL Forum. "An Interoperable End-to-end Broadband Service Architecture over ADSL Systems (Version 3.0)", ADSL Forum 97-215.

[57] ADSL Forum. "Core Network Architectures for ADSL Access Systems (Version 1.01)", ADSL Forum 98-017.

[58] Gupta, V., "Secure, Remote Access over the Internet using IPSec", Work in Progress.

[59] Pereira, R., et al., "The ISAKMP Configuration Method", Work in Progress.

[60] Pereira, R. and S. Beaulieu, "Extended Authentication Within ISAKMP/Oakley", Work in Progress.

[61] Litvin, M., et al., "A Hybrid Authentication Mode for IKE", Work in Progress.

[62] Kelly, S., et al., "User-level Authentication Mechanisms for IPsec", Work in Progress.

[63] Patel, B., et al., "DHCP Configuration of IPSEC Tunnel Mode", Work in Progress.

[64] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D. and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.

[65] ANSI/IEEE - 10038: 1993 (ISO/IEC) Information technology - Telecommunications and information exchange between systems - Local area networks - Media access control (MAC) bridges, ANSI/IEEE Std 802.1D, 1993 Edition.

12.0 Сведения об авторах

Bryan Gleeson

Nortel Networks

4500 Great America Parkway

Santa Clara CA 95054

USA

Phone: +1 (408) 548 3711

EMail: bgleeson@shastanets.com

Juha Heinanen

Telia Finland, Inc.

Myyrmaentie 2

01600 VANTAA

Finland

Phone: +358 303 944 808

EMail: jh@telia.fi

Arthur Lin

Nortel Networks

4500 Great America Parkway

Santa Clara CA 95054

USA

Phone: +1 (408) 548 3788

EMail: alin@shastanets.com

Grenville Armitage

Bell Labs Research Silicon Valley

Lucent Technologies

3180 Porter Drive,

Palo Alto, CA 94304

USA

EMail: gja@lucent.com

Andrew G. Malis

Lucent Technologies

1 Robbins Road

Westford, MA 01886

USA

Phone: +1 978 952 7414

EMail: amalis@lucent.com

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru

13.0 Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.