Построение виртуальных частных сетей (VPN) на базе технологии MPLS

Cisco Systems
Empowering the Internet Generation℠

Аннотация

Данный документ представляет собой достаточно подробное описание основных аспектов внедрения технологии MPLS в сетях операторов для предоставления услуги Виртуальная частная сеть и производных услуг. В документе подробно рассматриваются вопросы, связанные с обоснованием выбора технологии MPLS-VPN; приведены примеры решения услуг по построению интранет- и экстранет-сетей, рассмотрены вопросы, связанные с предоставлением внешних услуг, Интернет и сетевого управления, аспекты, связанные с обеспечением качества обслуживания и трафик-инжиниринга, приведены различные варианты организации системы доступа и вопросы организации маршрутизации. Документ ориентирован на инженерно-технический персонал, использующий или планирующий применение данной технологии в своей сети, сетевых дизайнеров и консультантов, чья область интересов распространяется на технологию MPLS.

Разделы 1 и 2 документа, характеризующие общие тенденции развития телекоммуникационного сообщества, содержащие обзоры технологических решений и общее описание услуг и целей решения, могут быть интересны для руководителей и консультантов, отвечающих за бизнес-планирование компаний операторов связи.

Содержание

1. Краткий обзор для руководства

Расширение глобальной сети Интернет, широкое распространение IP-приложений — все это позволило сервис-провайдерам предложить своим заказчикам целый ряд весьма привлекательных новых услуг. Новый Мир телекоммуникаций отражает и демонстрирует фундаментальные перемены в бизнесе сервис-провайдеров, которые уходят от услуг, ориентированных на сеть (и состоящих в простой поддержке полосы пропускания), и переходят к моделям, ориентированным на бизнес и услуги с добавленной ценностью (включая пакетную телефонию и электронную коммерцию), которые предлагаются помимо простых услуг передачи трафика.

Чтобы постоянно поддерживать преимущество над конкурентами, сервис-провайдерам необходимо развертывать сети общего доступа, способные консолидировать трафик разных типов и поддерживать услуги, связанные с передачей данных, голоса и видео. Эта задача становится все более очевидной ввиду перемен, которые происходят в сетях корпоративных заказчиков. По мере того, как их приложения становятся все более сложными и требовательными к сетевым ресурсам, компании все чаще прибегают к внешнему подряду (аутсорсингу), чтобы сократить расходы и получить доступ к передовому опыту в области сетевых технологий. Те провайдеры, которые раньше других воспользуются возможностью установления партнерских отношений с заказчиками и предложат им дифференцированные услуги, добьются финансового успеха, так как получат новые источники доходов и повысят прибыльность своего бизнеса.

Виртуальные частные сети (VPN) станут основой для поддержки услуг Нового Мира. Уже сегодня многие сервис-провайдеры имеют планы развертывания услуг с добавленной ценностью поверх своих транспортных сетей VPN. Новые услуги, такие как электронная коммерция (e-commerce), хостинг приложений и поддержка мультимедиа, дают возможность сервис-провайдерам получать дополнительный доход и поддерживать долгосрочные преимущества в конкурентной борьбе. Более того, сервис-провайдеры смогут воспользоваться «экономией масштаба» в своей транспортной сети и предоставить заказчикам услуги пакетной телефонии.

1.1. Динамика рынка и факторы, стимулирующие развитие бизнеса

Прогнозы доходов сервис-провайдеров и расходов корпоративных заказчиков, связанных с технологией виртуальных частных сетей (VPN), указывают на существенные возможности, которые открываются в этой области для поставщиков аппаратных средств (см. рисунок 1 и рисунок 2). На рисунке 1 приводятся данные Yankee Group, а на рисунке 2 — данные от Infonetics. Оба независимых источника приводят удивительно похожие цифры о предполагаемых затратах заказчиков на сети VPN.

Рисунок 1: Прогнозы Yankee Group о расходах на VPN

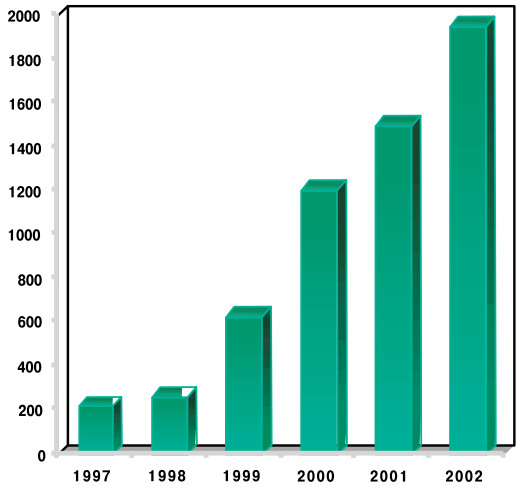
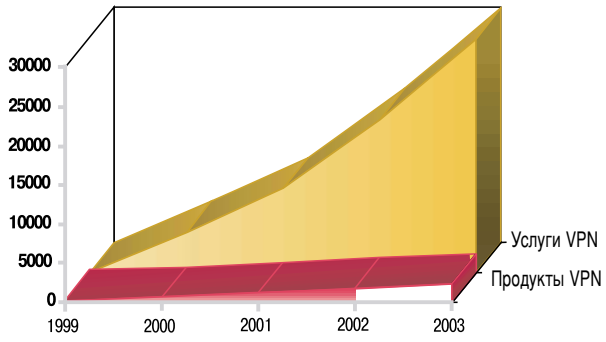
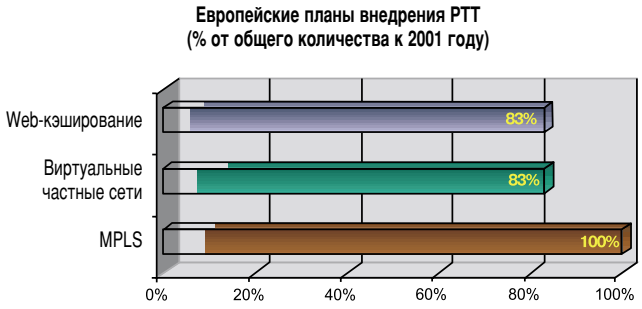


Рисунок 2: Данные Infonetics о предполагаемых затратах на VPN (в млн. долларов США)



Кроме того, еще один отчет Infonetics (за май 2000 года) говорит о широком признании и распространении технологии MPLS среди сервис-провайдеров, которые рассматривают эту технологию в качестве основы для поддержки услуг VPN. В этом отчете говорится, что к 2004 году европейские сервис-провайдеры затратят на сетевое оборудование более 9,1 млрд. долларов, причем абсолютно все провайдеры планируют воспользоваться технологией MPLS для поддержки качества услуг, а 83% респондентов планируют с помощью MPLS развернуть виртуальные частные сети уже к 2001 году (см. рисунок 3).

Рисунок 3: Данные Infonetics о планах европейских традиционных операторов связи по внедрению VPN к 2001 году



Хотя в этом анализе рассматривается только европейский рынок, мы считаем, что здесь подмечена глобальная тенденция развития рынка сервис-провайдеров, поскольку все больше малых и средних предприятий думают о передаче своих сетей VPN на аутсорсинг сервис-провайдерам, которые смогут предложить привлекательные условия, отвечающие потребностям бизнеса.

Cahners In-stat Group считает, что к 2003 году сетевые VPN (то есть виртуальные частные сети, отданные на аутсорсинг операторам) станут самым распространенным на рынке видом VPN. Конечные пользователи будут все чаще требовать соглашений о гарантированном качестве обслуживания (SLA), масштабируемости и гибкости сетей и широкого выбора постоянно доступных услуг VPN. Все это вынудит большинство компаний перейти от своих собственных «доморощеных» VPN к сетям, которые будут эксплуатироваться и обслуживаться внешними профессионалами.

Рисунок 4: Данные Cahners In-stat Group о росте спроса на VPN-услуги, предоставляемые операторами

Источник: Cahners In-stat Group, 1999

Причина столь пристального интереса к VPN состоит не столько в их новизне, сколько в том, что их функциональность переносится с Уровня 2 на Уровень 3. Развертывание VPN с функциональностью Уровня 3 позволит сервис-провайдерам предлагать экономичные услуги и высокую производительность широкому кругу корпоративных заказчиков. В прошлом услуги VPN для данных, голоса и видео опирались на разные технологии, и все они (в терминах IP) относились к Уровню 2.

Цель VPN состоит в создании сети совместного использования, которая, с точки зрения заказчика, будет функционировать как выделенная линия. На первый взгляд, это широкое определение позволяет включить в состав VPN такие технологии, как Frame Relay и ATM. Однако их можно назвать всего лишь сетями VPN Уровня 2. Для поддержки IP-функциональности Уровня 3 такие сети должны пользоваться каким-то оверлейным (наложенным) решением, включающим постоянные виртуальные каналы, эмулирующие соединения типа «точка–точка». Однако таким решением трудно управлять, и оно плохо масштабируется.

По мере разработки бизнес-моделей Нового Мира и перехода от простого предоставления полосы пропускания к услугам с добавленной ценностью, сервис-провайдеры все чаще пытаются использовать повсеместно распространившийся протокол IP в качестве основного протокола для своих сетей. Разумеется, это ставит в повестку дня задачи поддержки безопасных, масштабируемых соединений с гарантированным качеством услуг на базе общих или частных IP-сетей, которые исторически были предназначены для передачи трафика «по мере возможности» и не имели средств защиты. Для этого нужны новые протоколы и услуги для IP-сетей.

Упрощенно все требования к VPN можно разделить на две части. С одной стороны, это возможности, которые нужны сервис-провайдеру для экономичного предоставления заказчикам услуг VPN, а с другой стороны — функции безопасности, которые нужны корпоративным заказчикам для защиты своей информации в совместно используемой сети. Считается, что в будущем предприятия будут больше доверять возможностям провайдеров в плане защиты своих данных, однако сегодня многие из них предпочитают полагаться на свои собственные системы безопасности. В будущем, когда взаимное доверие укрепится, сервис-провайдеры смогут за отдельную плату предлагать предприятиям помимо простых соединений VPN дополнительные услуги безопасности, включая шифрование и услуги аутентификации.

Для сервис-провайдеров технология MPLS в сочетании с системой управления MPLS-VPN — это возможность экономичной поддержки масштабируемых услуг VPN в сети IP. При этом для защиты данных разных клиентов ис-

пользуется технология разделения трафика. Инжиниринг трафика, качество услуг (QoS) и функции протокола MPLS, предусматривающие работу без установления соединений (connectionless features), предоставляют сервис-провайдерам небывалые возможности для наращивания VPN в своей инфраструктуре без ущерба для производительности. Если предприятие озабочено проблемами безопасности, оно может использовать набор протоколов (например, IPSec), которые позволяют защитить данные в любых каналах, где может возникать угроза несанкционированного доступа.

1.2. Целевой рынок для сервис-провайдера, ценность предложения, потенциальная структура тарификации и преимущества для конечных пользователей

Независимо от того, на каком рыночном сегменте работает тот или иной сервис-провайдер, его деловые предложения, направленные на продажу доступа к сети MPLS конечному пользователю, будут опираться на один и тот же набор преимуществ. Вначале сервис-провайдеры с помощью управляемых сетей MPLS будут предлагать услуги, сходные с услугами частных линий. После того, как сервис-провайдер привлечет внимание заказчика, предложив ему «выделенную линию» по низкой цене, он может предложить дополнительные услуги, включая дифференцированные уровни обслуживания и защиту определенных видов трафика. Если конечный пользователь захочет поддерживать голосовую связь по глобальной виртуальной частной сети, построенной оператором, он вполне сможет это сделать с помощью функций быстрой перемаршрутизации MPLS (fast re-route).

Управляемое решение MPLS имеет целый ряд свойств, которые позволяют сокращать плату за соединения и в то же время получать дополнительные доходы. Вот краткий перечень этих свойств:

- С помощью функций MPLS, связанных с инжинирингом трафика, сервис-провайдеры смогут максимально повысить эффективность использования полосы пропускания в своих сетях.
- Средства технического обеспечения услуг, такие как VPNSC (Cisco VPN Solutions Center), позволяют использовать в этой области гораздо менее квалифицированные кадры с невысокой зарплатой и в то же время предоставлять услуги гораздо быстрее, чем в сетях VPN Уровня 2.
- Если в решении MPLS используются опорные сети ATM (IP + ATM), то PNNI заменяется протоколами MPLS, что упрощает и оптимизирует административные процессы.

Хотя все это выглядит довольно заманчиво, нужно внимательно подходить к формулированию ценности своего предложения. Некоторым операторам не нужны функции MPLS, направленные на поддержку QoS и дифференцированных услуг. Они считают, что качество услуг лучше всего поддерживать за счет постоянного расширения полосы пропускания с тем, чтобы никогда не иметь дефицита сетевых ресурсов.

Модели тарификации для сетей MPLS-VPN все еще разрабатываются, но среди них уже сейчас можно выделить следующие возможные варианты:

- по размеру канала доступа;
- по пиковой скорости доступа (через CAR);
- по количеству переданных в VRF пакетов и байтов;
- в зависимости от класса обслуживания (CoS), т.е. правил передачи пакетов и их маркировки;
- по размерам таблицы маршрутизации VRF;
- за членство в VPN;
- в зависимости от протокола маршрутизации PE — CE.

В настоящее время сервис-провайдеры используют следующие два основных подхода к тарификации:

- первые сервис-провайдеры устанавливают цену на соединения MPLS на уровне 75% от стоимости полносвязных соединений Frame Relay DLCI;
- вторые — тарифицируют по скорости доступа к сети MPLS без учета расстояния, которое всегда учитывается в услугах выделенных линий. И дополнительная плата начисляется за услуги типа шифрования и поддержку быстрой перемаршрутизации.

1.3. Обзор решения Cisco

Управляемое решение Cisco Managed MPLS-VPN Solutions решает многие проблемы сервис-провайдеров, которые хотят иметь масштабируемую инфраструктуру VPN, позволяющую с максимальной эффективностью использовать полосу пропускания и удовлетворять абонентские требования к производительности и качеству.

MPLS представляет собой привлекательный способ использования транспортных возможностей ATM для передачи трафика IP. При использовании MPLS для сопряжения IP и ATM мы уже не используем PNNI для назначения пар VCI/VPI. Вместо этого используется протокол распределения меток (Label Distribution Protocol), который присваивает метки, занимающие пространство VPI/VCI в ячейке ATM, и превращает все коммутаторы ATM в коммутирующие по меткам маршрутизаторы (Label Switch Routers — LSR). Несмотря на эти привлека-

тельные возможности, ожидается, что большинство сетей MPLS будет основано на фреймах, а не на ячейках, причем фреймы будут, в основном, передаваться по оптическим каналам SONET/SDH, DWDM или используя темные волокна. Если в сети провайдера используется технология ATM, то MPLS позволяет коммутаторам ATM (превращенным в коммутирующие метки маршрутизаторы LSR) восстанавливать фреймы из ячеек, чтобы идентифицировать метки, необходимые для передачи фреймов по следующему сетевому сегменту (функция VC-merge).

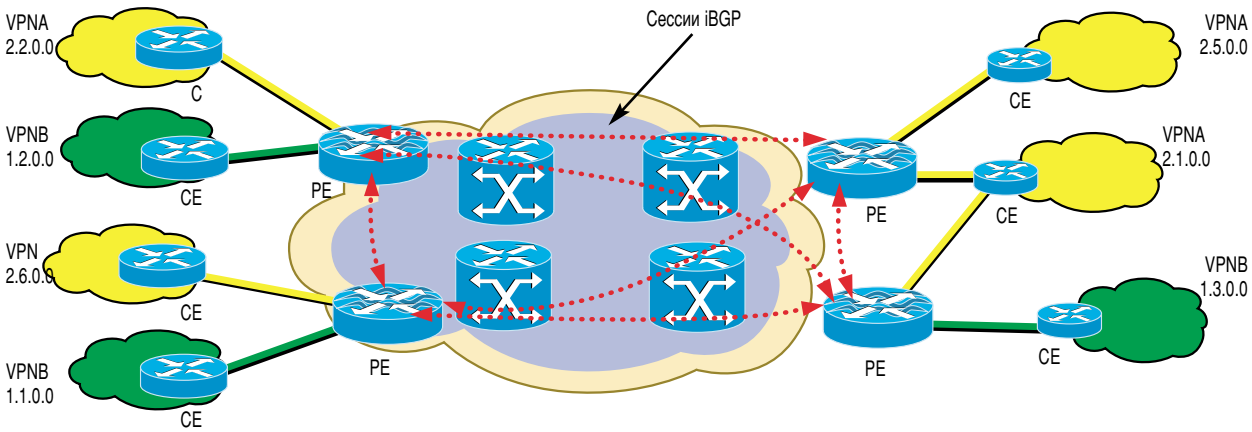
Однако независимо от технологии опорной транспортной сети управляемое решение MPLS может быть представлено с помощью элементов, показанных ниже на рисунке 5.

В этом документе используются термины, которые могут быть незнакомы тем, кто не знает технологии MPLS. Полный список терминов приведен в Приложении A, однако мы хотим сделать некоторые пояснения прямо сейчас, чтобы помочь читателю понять содержание рисунка.

В состав опорной части сети (core network) входят P-маршрутизаторы (латинская буква «P» обозначает провайдера). В терминологии MPLS эти P-маршрутизаторы называются коммутирующими по меткам маршрутизаторами (Label Switch Routers — LSR). Как уже говорилось, даже если в опорной сети используется технология ATM, на коммутаторах ATM работает программное обеспечение MPLS, придающее им функциональность Уровня 3, и поэтому мы можем называть их маршрутизаторами. Эти P-маршрутизаторы пользуются и передающими (коммутирующими), и управляющими функциями MPLS. Передача осуществляется с помощью свопинга меток, а управление — с помощью протокола распределения меток (Label Distribution Protocol). Эти маршрутизаторы не осведомлены о существовании виртуальных частных сетей (VPN) и не участвуют в BGP-обмене, который происходит на PE-маршрутизаторах.

PE-маршрутизаторы (буквы «PE» означают периферийную часть сети провайдера) должны присваивать пакету начальную метку при его поступлении в опорную сеть MPLS (MPLS core) и удалять эту метку в момент, когда пакет покидает сеть. CE-маршрутизаторы («CE» означает периферию сети заказчика) подключаются к PE-маршрутизаторам и не требуют специальной модификации для поддержки MPLS-VPN. PE-маршрутизаторы связываются друг с другом по многопротокольному BGP для обмена информацией о подключенных VPN. Это может вызвать проблемы с масштабированием, поскольку если PE-маршрутизаторы подключаются друг к другу по принципу «каждый с каждым», то по мере появления в сети новых маршрутизаторов количество связей между ними будет нарастать в геометрической прогрессии. Главным способом сокращения связей между PE-маршрутизаторами является применение групп Route-Reflector (RR). В каждой такой RR-группе имеется одно устройство — сервер маршрутизации, которому подчиняется ряд PE-маршрутизаторов. Все подчиненные маршрутизаторы получают данные о маршрутах с этого сервера. В случае необходимости PE-маршрутизатор может одновременно входить в состав нескольких групп.

Рисунок 5. Элементы MPLS



Каждое устройство MPLS PE поддерживает по одной таблице VRF (таблица маршрутизации и передачи VPN) на каждую VPN. В таблице VRF хранятся данные обо всех маршрутах, известных этому устройству в той или иной VPN. MPLS-устройство идентифицирует маршруты, относящиеся к определенной сети VPN с помощью «различителя маршрутов» (Route Distinguisher — RD), который присваивается всем маршрутам соответствующего CE. Эти «различители» (RD) имеют значение только для PE-устройств, так как P-маршрутизаторы коммутируют ячейки или пакеты на основании информации, заключенной в метках.

Магистральная адресация, которая используется для подключения P-маршрутизаторов, полностью отделена от адресации, используемой для подключения CE-маршрутизаторов. Эти две схемы маршрутизации никак не взаимодействуют между собой. PE-маршрутизаторы сохраняют адреса опорной сети в глобальной таблице маршрутизации, которая хранится отдельно от таблиц VRF, где находятся данные обо всех маршрутах каждой VPN, к которой подключены сайты CE. Каждая таблица VRF имеет так называемую «политику импорта» (import policy), которая определяет, какие обновления PE следует принять, и «политику экспорта» (export policy), определяющую, какие маршруты следует объявлять.

Когда PE-устройство присваивает метку на границе сети MPLS, эта метка точно определяет весь маршрут, по которому будет передаваться данный пакет в этой сети. Это происходит потому, что LDP уже определил, какая входящая метка будет заменяться на соответствующую исходящую метку на каждом P-маршрутизаторе с тем, чтобы пакет был доставлен в конечный пункт назначения. Поэтому MPLS представляет собой форму маршрутизации от источника, так как только на периферии принимается решение о маршруте.

Каждый пограничный маршрутизатор заказчика должен инжектировать свои маршруты в соответствующие таблицы VRF, определенные в MPLS-сети для данной VPN. Эта задача выполняется пограничными маршрутизаторами заказчика, настроенными на передачу информации о маршрутах, необходимых другим сайтам своей же VPN. Для этой передачи может использоваться статическая маршрутизация, а также маршрутизация BGP, OSPF или RIPv2. В качестве примера на рисунке 4 показана сеть VPNA, где используются подсети сети 2.0.0.0 класса A. Сайт, находящийся в подсети 2.2.0.0, должен объявить о себе другим сайтам своей VPN. То же самое должны сделать и другие сайты. Таким образом в таблицах VRF каждого устройства PE, находящегося в этой сети, появляется информация обо всех подсетях, входящих в состав VPNA.

Из этого примера следует, что маршруты VPNA не взаимодействуют с маршрутами VPNB. Подобное разделение маршрутной информации является основным фактором, обеспечивающим отличную масштабируемость решений MPLS-VPN, поскольку не требуется поддержка единой таблицы маршрутизации, содержащей информацию о том, как добраться до любой точки сети.

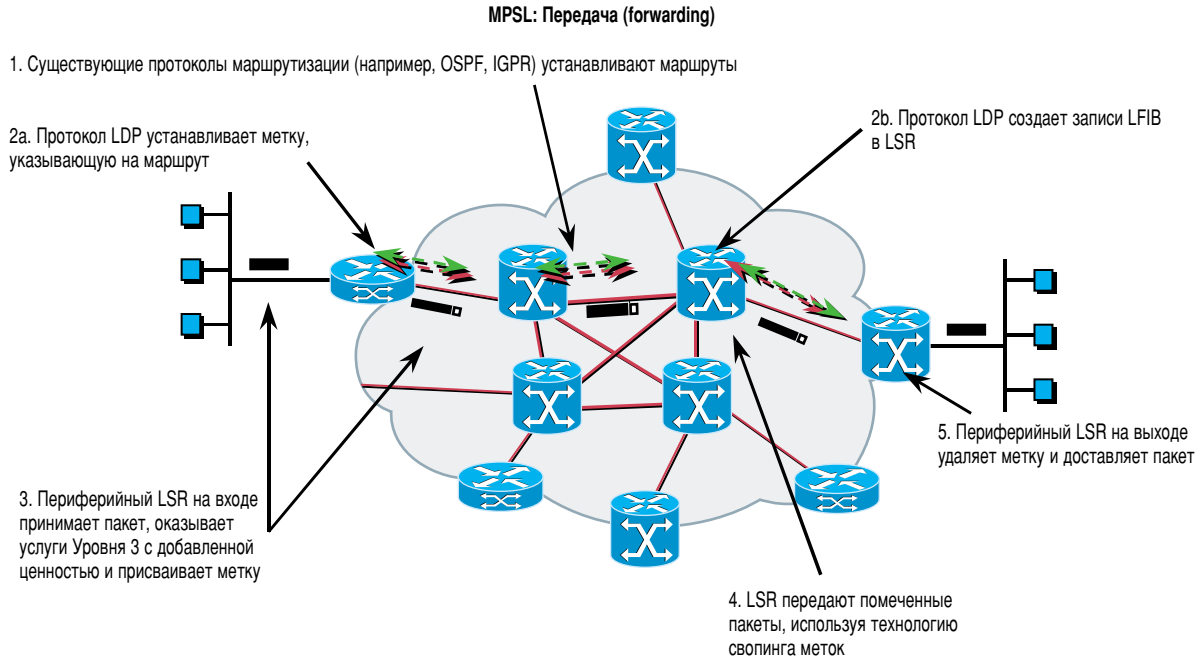
2. Обзор технологии MPLS

MPLS представляет собой своеобразный технологический «ключ», открывающий дорогу в Новый Мир услуг IP VPN. MPLS позволяет сервис-провайдерам предлагать дифференцированные, простые в настройке и управлении услуги IP VPN операторского качества как другим провайдерам, так и абонентам. С помощью MPLS сервис-провайдеры могут поддерживать услуги IP VPN в коммутируемых и в маршрутизируемых сетях, используя все современные источники дохода (такие как Frame Relay и ATM WAN) и в то же время прокладывая дорогу к новым услугам завтрашнего дня (услугам с добавленной ценностью).

MPLS — это новый стандарт Нового Мира сетевых технологий, основанный на технологии коммутации по меткам Cisco (Cisco Tag Switching). Он является перспективным проектом стандарта IETF. Сегодня он существует в качестве проекта (Internet Draft), с которым можно познакомиться на сайте http://www.ietf.org/internet-drafts/draft-ietf-mpls-arch-07.txt. Технология Cisco MPLS включает ряд полезных добавлений к стандартам MPLS. Эти добавления мы обсудим позже.

MPLS представляет собой новаторскую технологию использования метода передачи по меткам. С помощью меток определяются и маршруты, и атрибуты услуг. На периферии сети, в точке входа, происходит обработка входящих пакетов. Здесь же выбираются и присваиваются метки. Опорная сеть считывает метки, соответствующим образом обрабатывает пакеты и передает их далее в соответствии с метками. Действия, требующие больших процессорных мощностей (анализ, классификация и фильтрация), выполняются только один раз, в точке входа. После этого пакеты с метками передаются по опорной сети. Устройства опорной сети сервис-провайдера передают пакеты только основе меток и не анализи-

Рисунок 6. Функционирование MPLS



руют заголовки IP-пакетов. В точке выхода метки удаляются, и пакеты передаются в пункт назначения.

2.1. Функционирование MPLS

Чтобы понять, как функционирует сеть MPLS, давайте проследим за передачей пакета по сети сервис-провайдера, в которой реализована эта технология. Обратимся к рисунку 6.

Этап 1. Сеть автоматически формирует таблицы маршрутизации. В этом процессе участвуют маршрутизаторы или коммутаторы IP + ATM, установленные в сети сервис-провайдера. При этом используются внутренние протоколы маршрутизации, такие как OSPF или IS-IS.

Этап 2. Протокол распределения меток (Label Distribution Protocol — LDP) использует отраженную в таблицах топологию маршрутизации для определения значений меток, указывающих на соседние устройства. В результате этой операции формируются маршруты с коммутацией по меткам (Label Switched Paths — LSP) или переконфигурированный путь мапирования меток между исходной точкой и точкой назначения. Автоматическое присвоение меток MPLS выгодно отличает эту технологию от технологии частных виртуальных каналов ATM PVC, требующих ручного присвоения VCI/VPI.

Этап 3. Входящий пакет поступает на пограничный Label Switch Router (LSR), который определяет, какие услуги 3-го Уровня необходимы этому пакету (например, QoS или управление полосой пропускания). На основе учета всех требований маршрутизации и правил высокого уровня (policies), пограничный LSR выбирает и присваивает метку, которая записывается в заголовок пакета, после чего пакет передается дальше.

Этап 4. Устройство LSR, находящееся в опорной сети, считывает метки каждого пакета, заменяет старые метки новыми (новые метки определяются по локальной таблице) и передает пакет дальше. Эта операция повторяется в каждой точке передачи пакета по опорной сети.

Этап 5. На выходе пакет попадает в пограничный LSR, который удаляет метку, считывает заголовок пакета и передает его по месту назначения.

В магистральных LSR метка MPLS сравнивается с заранее рассчитанными таблицами коммутации и содержит информацию 3-го Уровня. Это позволяет каждому устройству LSR автоматически оказывать каждому пакету необходимые IP-услуги. Таблицы рассчитываются заранее, что снимает необходимость повторной обработки пакетов в каждой точке передачи. Такая схема не только позволяет разделить разные типы трафика (например, отделить неприоритетный трафик от критически важно-

го); она делает решения MPLS хорошо масштабируемыми. Поскольку для присвоения меток технология MPLS использует разные наборы правил (policy mechanisms), она отделяет передачу пакетов от содержания заголовков IP. Метки имеют только локальное значение и многократно переиспользуются в крупных сетях, поэтому исчерпать запас меток практически невозможно. В рамках предоставления корпоративных IP-услуг самое главное преимущество MPLS заключается в способности присваивать метки, имеющие специальное значение. Наборы меток определяют не только место назначения, но и тип приложения и класс обслуживания.

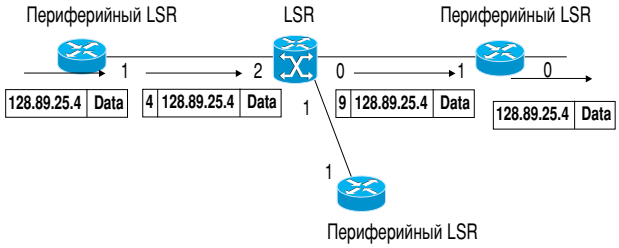
Чтобы лучше понять возможности масштабирования MPLS, обратимся к рисунку 7, где показан пример таблиц передачи (MPLS forwarding tables).

Рисунок 7. Таблицы передачи MPLS (MPLS forwarding tables)

In Lbl	Address Prefix	Out Int	Out Lbl
–	128.89	1	4
–	171.69	1	5

In Lbl	IN I/F	Address Prefix	Out Int	Out Lbl
4	2	128.89	0	9
8	1	128.89	0	10
5	2	171.69	1	7

In Lbl	IN I/F	Address Prefix	Out Int	Out Lbl
9	1	128.89	0	–
10	1	128.89	0	–



Этап 1. Входящий пакет поступает на периферийное устройство LSR, которое считывает префикс назначения, 128.89. Затем устройство LSR обращается к таблице коммутации и вставляет необходимую метку 4, а затем передает пакет на интерфейс 1.

Этап 2. Устройство LSR в опорной сети считывает метку, находит для нее соответствие в своей таблице коммутации, заменяет метку 4 на метку 9 и передает пакет на интерфейс 0.

Этап 3. Маршрутизатор в точке выхода считывает метку и находит соответствие метке 9 в своей таблице, где говорится, что эту метку нужно удалить и направить пакет на интерфейс 0. Заметим при этом, что в опорной сети маршрутная информация IP используется только для построения таблиц коммутации меток и не связана напрямую с процессом передачи.

2.2. Обзор технологии VPN

Чтобы составить правильное представление о преимуществах сетей MPLS-VPN в плане масштабирования, нужно для начала рассмотреть различные модели VPN, доступные на современном рынке. Вначале мы рассмотрим ограничения, присущие оверлейной или наложенной модели, а затем посмотрим, какие преимущества по сравнению с ней дает одноранговая модель.

2.2.1. Оверлейная модель

Сервис-провайдер предоставляет корпоративному заказчику технологию соединений между его офисами и отделениями по частной WAN IP-сети. Для этого в каждой точке подключения нужно установить маршрутизатор и связать его по какому-либо IGP-протоколу маршрутизации по крайней мере с центральным маршрутизатором. В этом случае мы говорим, что сервис-провайдер предоставляет корпоративному заказчику *частную сетевую магистраль* (private network backbone).

Если транспортная сеть и магистральные коммутаторы действительно принадлежат корпорации, это значит, что она имеет настоящую частную сеть. Однако чаще всего транспортная сеть и по крайней мере часть магистральных коммутаторов принадлежат сервис-провайдеру и совместно используются несколькими корпоративными сетями. В этом случае мы говорим, что каждая из этих корпоративных сетей является не настоящей, а *виртуальной частной сетью* (VPN).

В сети VPN с коммутацией каналов маршрутизаторы, которые находятся в разных отделениях компании, связываются между собой либо по выделенным, либо по коммутируемым линиям. В любом случае роль магистрали будет чаще всего выполнять телефонная сеть общего доступа. Сети Frame Relay и ATM основаны на технологии коммутации каналов. В этом случае маршрутизато-

ры, находящиеся в отделениях компании-заказчика, связываются между собой с помощью виртуальных каналов. Эти виртуальные каналы, подобно реальным, поддерживают соединения типа «точка — точка».

Корпоративные маршрутизаторы могут поддерживать соединения «точка — точка» и с помощью средств IP-тунелирования, например, IPSec или GRE. В таких частных или виртуальных частных сетях задачи дизайна и функционирования магистральной топологии решает сама корпорация или сервис-провайдер (если в сети предоставляются услуги по управлению). Маршрутизаторы, установленные в отделениях корпорации, связываются с соседними маршрутизаторами по каналам «точка — точка». Обмен данными о маршрутизации происходит напрямую по этим каналам.

С точки зрения магистральной сети сервис-провайдера, передаваемая маршрутная информация представляет собой обычные данные, которые обрабатываются «прозрачно», то есть так же, как и все остальные. Со своей стороны, корпоративные маршрутизаторы не имеют ни знаний, ни средств контроля над маршрутизирующими функциями магистрали. Этот домен относится к сфере, за которую отвечает сервис-провайдер.

Мы говорим, что в этом случае корпоративная IP-сеть является *оверлейной,* то есть «накладывается» поверх провайдерской магистрали. При этом корпоративную сеть можно рассматривать как сеть более высокого уровня, а магистраль — как сеть более низкого уровня. Обе сети существуют независимо друг от друга. Такой способ построения сети более высокого уровня поверх сети более низкого уровня называется *оверлейной моделью.*

2.2.1.1. Недостатки оверлейной модели

Чтобы добиться оптимальной маршрутизации в корпоративной сети, надстроенной поверх магистрали, корпоративная сеть должна иметь узловую структуру (meshed network). Это означает, что в каждом отделении корпорации должен устанавливаться маршрутизатор, соединенный с соседними маршрутизаторами, находящимися в других отделениях.

Если корпоративная сеть будет хотя бы частично отклоняться от узловой топологии (meshed), то возникнут случаи, когда трафик будет передаваться от одного корпоративного маршрутизатора в магистраль провайдера, затем поступать на корпоративный магистральный (центральный) маршрутизатор, затем передаваться обратно в провайдерскую магистраль и лишь затем поступать на оконечный (удаленный) маршрутизатор в пункте назначения. Поскольку удаленные маршрутизаторы подключаются к общей магистрали (магистрали сервис-провайдера), вариант, при котором трафик покидает магистраль, проходит через второй маршрутизатор и снова попадает в магистраль, нельзя признать эффективным.

Если сеть имеет полносвязную структуру (fully meshed), вышеуказанная ситуация не встречается, однако возникают другие проблемы. Корпорация должна платить за виртуальные каналы (а провайдер должен подкреплять их соответствующими сетевыми ресурсами), но при увеличении количества корпоративных отделений количество каналов возрастает в геометрической прогрессии. Помимо высокой стоимости проблема усугубляется тем, что алгоритмы IP-маршрутизации плохо масштабируются в случае наращивания количества прямых связей между маршрутизаторами.

2.2.2. Одноранговая модель (Peer Model)

Для того, чтобы пользоваться услугами VPN, предприятию совсем не нужно проектировать и эксплуатировать собственную магистральную сеть. Сервис-провайдер, который уже имеет магистральную сетевую инфраструктуру, вполне может взять эту задачу на себя. Одноранговая модель VPN требует только подключения маршрутизатора заказчика к одному из маршрутизаторов сервис-провайдера.

В одноранговой VPN два маршрутизатора **C** считаются одноранговыми только в том случае, когда они находятся на одном сайте. Поэтому принадлежащий заказчику маршрутизатор **C1** не имеет одноранговых (соседских) отношений с маршрутизатором **C2**, который принадлежит тому же заказчику, но установлен на другом сайте (в другом месте). Получается, что на каждом сайте заказчика имеется по крайней мере один корпоративный маршрутизатор (**CE)**, связанный одноранговыми отношениями по крайней мере с одним маршрутизатором сервис-провайдера (**PE**).

CE-маршрутизаторы не обмениваются друг с другом данными о маршрутах. Нет вообще никакой необходимости в обмене какими-либо данными между **CE**-маршрутизаторами. Данные передаются от входящего **CE**-маршрутизатора через входящий **PE**-маршрутизатор сервис-провайдера и проходят через один или несколько магистральных **P**-маршрутизаторов. В итоге они достигают исходящего **PE**-маршрутизатора сервис-провайдера и попадают на исходящий корпоративный **CE**-маршрутизатор.

Таким образом маршрутизация становится оптимальной.

Поскольку **CE**-маршрутизаторы не обмениваются друг с другом данными о маршрутах, корпорации не нужно иметь свою магистраль или управлять ею. Разумеется, корпоративный заказчик может пользоваться IP-магистралью так, как будто у него имеется сеть Frame Relay, и создавать своего рода «виртуальные каналы» между **CE**-маршрутизаторами. Обычно для этого используется одна из форм IP-туннелирования. Однако это приводит нас обратно к оверлейной модели со всеми ее проблемами. Одноранговая модель таких проблем не имеет.

2.2.2.1. Преимущества одноранговой модели

Одноранговая модель имеет целый ряд преимуществ:

В одноранговой модели количество работы, которую должен выполнить сервис-провайдер для технического обеспечения и управления VPN, *прямо пропорционально* количеству сайтов заказчика, подключенных к VPN. В оверлейной модели количество этой работы *пропорционально квадрату* сайтов заказчика, подключенных к VPN.

Одноранговая модель поддерживает оптимальную маршрутизацию пользовательского трафика по магистрали сервис-провайдера, так как в этой модели нет необходимости в транзитных **CE**-устройствах.

Корпоративному заказчику не нужно управлять собственной магистралью. Ему нужно только подключить **CE**-маршрутизатор на каждом сайте.

Таким образом, одноранговая модель выгодна и сервис-провайдеру, и заказчику. Для провайдера она означает сокращение объема работ, а для корпоративного заказчика — более ценные услуги.

2.2.2.2. Трудности реализации одноранговой модели

Хотя одноранговая модель имеет множество преимуществ по сравнению с оверлейной, на пути ее реализации также стоит ряд проблем, которые перечислены ниже:

Перегрузка P-маршрутизаторов информацией о маршрутах. Одной из основных проблем крупных IP-магистралей является большое количество ресурсов (памяти, процессорных мощностей, полосы пропускания), необходимых для хранения данных о маршрутизации. Если взять IP-магистраль и пустить по ней данные о маршрутах всех корпоративных сетей, P-маршрутизаторы никогда с ней не справятся.

Несогласованные (несмежные) адресные пространства. Обычно Интернет-сервис-провайдеры (ISP) стараются присваивать адреса осмысленно. Это значит, что адрес системы должен указывать на место, в котором эта система подключается к сети ISP. Однако многие корпоративные сети имеют адресные схемы, которые трудно совместить с магистральной топологией любого сервис-провайдера. В этих схемах адреса сайтов распределяются без какого-либо учета точки, в которой осуществляется подключение к провайдерской сети. Это сокращает возможности агрегации маршрутов и увеличивает объем данных о маршрутах, которые передаются по P-сети.

Частная адресация в C-сетях. Адреса во многих корпоративных сетях не являются уникальными. Это значит, что тот или иной адрес является уникальным только в пределах одного предприятия, но теряет уникальность при связи между предприятиями. Если IP-магистраль сервис-провайдера используется как общая магистраль для двух разных корпоративных сетей и если адреса в этих сетях не являются уникальными, P-маршрутизаторы не смогут гарантировать доставку пакетов по месту назначения.

Подслушивание. Для защиты данных нужно устанавливать шифрованные туннели «точка—точка» между каждой парой **CE**-маршрутизаторов (модель IPSec). Это решение хорошо подходит для оверлейной модели, полькольку она и без того использует туннель «точка—точка» между парами «соседних» **CE**-маршрутизаторов. Для одноранговой модели это решение подходит не столь хорошо, потому что здесь **CE**-маршрутизатор никогда не может определить, куда он будет передавать следующий пакет.

2.3. Обзор технологии MPLS-VPN

Чтобы экономично выделить технические ресурсы, необходимые для поддержки сетей IP VPN с богатыми функциями, сервис-провайдерам нужны средства, способные распознавать разные типы приложений, чтобы провайдер мог гарантировать определенное качество услуг (QoS) и обеспечивать безопасность данных, причем делать это нужно в сетях, которые будут менее сложными, чем оверлейные IP-туннели и узловые сети с виртуальными каналами (VC-meshed networks). Как мы уже говорили, оверлейные решения VPN, надстроенные поверх IP, требуют туннелирования или шифрования. Кроме того, поскольку IP-трафик передается по виртуальным каналам, оверлейная сеть VPN не знает, какой трафик по ней передается. Оверлейное решение сосредоточено на соединениях и не очень хорошо поддается масштабированию. Более того, оно конфликтует с бизнес-приложениями IP, которые не зависят от соединений и

ориентированы на протокол TCP/IP.

Сеть VPN должна распознавать, к какому типу приложений относится трафик (голос, SNA, видеопотоки или электронная почта). Она должна уметь быстро отделять трафик одного приложения от другого. Далее, сеть должна быть VPN-осведомленной (VPN-aware), чтобы сервис-провайдер мог легко группировать пользователей и услуги, в сетях интранет и экстранет. MPLS — это та технология, которая придает коммутирующим и маршрутизирующим сетям VPN-осведомленность. Она дает возможность сервис-провайдерам быстро и экономично создавать защищенные сети VPN любого размера — в единой инфраструктуре.

В отличие от оверлейных решений, сеть MPLS может разделять трафик и обеспечивать его защиту без шифрования и туннелирования. Технология MPLS поддерживает безопасность в каждой отдельной сети, точно так же, как сети Frame Relay и ATM поддерживают ее для каждого отдельного соединения. Если традиционная сеть VPN предоставляет базовые услуги сетевого транспорта, то сеть с технологией MPLS — это масштабируемые услуги VPN, допускающие поддержку IP-приложений с добавленной ценностью поверх базовой транспортной сети VPN. Этот сценарий отражает переход сервис-провайдеров от транспортно-ориентированной модели бизнеса к модели, ориентированной на услуги.

MPLS-VPN — это настоящая одноранговая VPN, которая разделяет трафик на Уровне 3 с помощью раздельных IP VPN таблиц передачи. MPLS-VPN может отделить трафик одного заказчика от другого, потому что каждой сети VPN каждого заказчика присваивается уникальный идентификатор (VPN ID). Это создает такие же условия безопасности, как в сетях ATM и Frame Relay, потому что пользователь сети VPN не может видеть трафик, передающийся за пределами этой сети.

Еще раз кратко перечислим **характеристики сетей MPLS-VPN:**

- Использование многопротокольных расширений BGP для преобразования префиксов адреса IPv4 в уникальные VPN-IPv4 NLRI.

- С каждым маршрутом заказчика связана определенная метка MPLS. Ее присваивает PE-маршрутизатор, стоящий в начале маршрута. Эта метка используется для того, чтобы направить пакет данных к нужному оконечному PE-маршрутизатору.

- В процессе передачи пакета данных по магистрали используются две метки. Верхняя метка направляет пакет к нужному оконечному PE-маршрутизатору. Вторая метка показывает, куда этот PE-маршрутизатор должен направить пакет.

- В каналах связи между PE-маршрутизаторами и CE-маршрутизаторами используются стандартные схемы передачи (IP forwarding). PE связывает каждый CE с таблицей передачи (forwarding table), в которой хранятся только те маршруты, которые доступны данному CE-маршрутизатору.

2.3.1. MPLS-VPN — настоящая одноранговая модель

В MPLS-VPN MPLS используется для передачи пакетов по магистрали, а BGP — для распространения по магистрали маршрутной информации. Главная цель этого метода состоит в том, чтобы поддержать аутсорсинг магистральных IP-услуг для корпоративных сетей. Для предприятий эта схема выглядит очень просто, а для сервис-провайдера она является гибкой и масштабируемой. Кроме того, она позволяет сервис-провайдеру оказывать услуги с добавленной ценностью. Боле того, эта схема может использоваться для создания VPN предоставления IP-услуг заказчикам.

CE-маршрутизатор является одноранговым устройством для PE-маршрутизатора (или маршрутизаторов), к которому он подключен, но не является одноранговым устройством для других CE-маршрутизаторов, установленных на других сайтах. Маршрутизаторы, расположенные на разных сайтах, не только не обмениваются информацией друг с другом, но в принципе вообще могут не знать о существовании других устройств CE (за исключением ситуации, когда это необходимо по требованиям безопасности). В результате провайдер может легко поддерживать очень крупные сети VPN (т.е. VPN с очень большим количеством сайтов), при этом настройка маршрутизации на каждом сайте также сильно упрощается.

Настоящая одноранговая модель поддерживает необходимые административные границы между C-сетью и P-сетью. Только сервис-провайдер может администрировать PE-маршрутизаторы и P-маршрутизаторы. Его заказчики никогда не должны получать доступ к этим устройствам на правах администратора. С другой стороны, только заказчик должен администрировать устройства CE (если только он не передал эти функции на аут-

сорсинг сервис-провайдеру).

В настоящей одноранговой модели каждый сайт той или иной С-сети моделируется как Автономная Система; CE-маршрутизаторы, находящиеся на одном сайте, используют, например, External BGP для обмена данными маршрутной информации с PE-маршрутизаторами этого сайта. Альтернативами EBGP являются OSPF, RIP II и статическая маршрутизация. Внутренний протокол маршрутизации С-сети (IGP) работает независимо на каждом отдельном сайте и не работает в Р-сети. Другими словами, парадигма настоящей одноранговой модели рассматривает каждую VPN как «малый Интернет» со своей магистралью и Р-сетями, которые соединяют сайты между собой.

2.3.2. Поддержка нового семейства адресов с помощью MBGP

PE-маршрутизаторы мапируют адреса IPv4 конкретной С-сети с новым семейством адресов VPN-IPv4. Адрес VPN-IPv4 состоит из 12 байтов. Первые 8 байтов называются «различителями маршрута» (Route Dis-tinguisher — RD). Остальные 4 байта занимают оригинальный адрес IPv4.

Если к одной Р-сети подключены две С-сети и если тот или иной IP-адрес используется в обеих С-сетях, PE-маршрутизаторы, подключенные к этим С-сетям, преобразуют одинаковые IPv4 адреса в два разных адреса VPN-IPv4 (с помощью использования разных RD). Таким образом, даже если в двух С-сетях используются одни и те же адреса IPv4, соответствующие им адреса VPN-IPv4 будут отличаться друг от друга. В Р-сети маршруты, ведущие к адресам, находящимся в С-сетях, определяются по адресам VPN-IPv4.

Таким образом, совпадения адресов в двух С-сетях не ведут к неопределенности адресации в Р-сети. С другой стороны, если конечная система имеет адрес, который является уникальным в пределах сети VPN, к которой эта система принадлежит, ей совершенно не нужно знать о своем VPN-IPv4 адресе.

Многие сервис-провайдеры используют полные IP-префиксы Интернет-маршрутов. Поэтому, когда сервис-провайдер передает данные об этих маршрутах через BGP4 по магистрали, все IBGP-устройства должны получить полную маршрутную информацию. Это вызывает проблемы с масштабированием, поскольку количество маршрутов становится чересчур большим. Однако иерархическая коммутация по меткам содержит механизм передачи, позволяющий хранить данные о внешних маршрутах только на пограничных маршрутизаторах. И хотя для распространения данных о маршрутах VPN по-прежнему используется BGP, он не требует передачи данных о маршрутах, связанных с адресами VPN-IPv4, внутренним магистральным маршрутизаторам.

В MPLS-VPN сетях пограничными маршрутизаторами являются PE-маршрутизаторы. При поддержке множества сетей VPN в одной совместно используемой магистрали совершенно не нужно и даже не рекомендуется обеспечивать полную доступность сетей. Полная доступность должна обеспечиваться только между системами, которые принадлежат к одной и той же VPN. Данные о маршрутах VPN-IPv4 для конкретной С-сети передаются (с помощью BGP) только PE-маршрутизаторам, подключенным к этой С-сети. PE-маршрутизаторы, не подключенные к С-сети, не получают данных о ее маршрутах. В результате объем информации о маршрутах, который хранится на PE-маршрутизаторе, не пропорционален общему количеству сетей VPN, поддерживаемых в данной Р-сети. Этот объем пропорционален только количеству сетей VPN, к которым напрямую подключен данный PE-маршрутизатор.

2.3.3. Множество инстанций маршрутизации/передачи

В MPLS-VPN входящий PE-маршрутизатор должен поддерживать отдельную таблицу (forwarding table) для каждой С-сети, к которой он подключен. Эта таблица заполняется данными о маршрутах, относящихся только к этой конкретной С-сети. Данные о маршрутах собираются через IBGP с других узлов PE, подключенных к той же С-сети.

Входящий PE-маршрутизатор получает «нормальные» IP-пакеты от своего CE-маршрутизатора. Далее он ищет «наилучшее совпадение» в VPN B FIB, находит iBGP для следующего устройства (PE2) и присваивает пакету стек меток: Внешняя метка + Внутренняя метка.

Все последующие Р-маршрутизаторы коммутируют этот пакет только на основании Внешней метки. Оконечный PE-маршрутизатор удаляет Внешнюю метку и с помощью Внутренней метки определяет, в какую сеть VPN/CE передать пакет. После этого Внешняя метка тоже удаляется, и пакет передается на подключенный CE-маршрутизатор.

Маршрут, по которому пакет передается от входящего до оконечного PE-маршрутизатора, обычно включает один или несколько промежуточных Р-маршрутизато-

ров. Промежуточные P-маршрутизаторы не хранят данные о маршрутах VPN и не могут доставить пакет к конечному IP-адресу. Правильное прохождение пакета по P-сети достигается с помощью коммутации по меткам. Если для пакета определен оконечный PE-маршрутизатор, коммутация по меткам направляет пакет именно к этому маршрутизатору. Входящий PE-маршрутизатор присваивает пакету заголовок для коммутации по меткам (Внешнюю метку), которая указывает маршрут (по P-сети) к оконечному PE-маршрутизатору. Промежуточные P-маршрутизаторы направляют пакет по этой метке, а не по IP-адресу. Поэтому промежуточные P-маршрутизаторы и не должны ничего знать о маршрутизации в C-сети. Они также ничего не должны знать об адресах VPN-IPv4. В принципе, P-маршрутизаторы могут одновременно поддерживать сети MPLS-VPN и оконечные устройства LSR, не имеющие к этим сетям никакого отношения.

Внешняя метка, которая используется для маршрутизации пакета по P-сети, указывает на маршрут к оконечному PE-маршрутизатору. Внутренняя метка, которой пользуется оконечный PE-маршрутизатор, определяет конечный исходящий порт (или подинтерфейс), через который необходимо передать пакет. Поэтому оконечному PE-маршрутизатору также не нужно знать IP-адрес, по которому передается пакет.

Настоящая одноранговая модель MPLS-VPN дает возможность P-сети поддерживать любое количество VPN без непомерного увеличения объема данных о маршрутах, которые должны храниться на P-маршрутизаторах. Эта модель исключает случайную передачу трафика между сетями VPN, так как каждая сеть VPN пользуется своей собственной маршрутной информацией. Кроме того, эта модель не требует уникальности адресов, которые используются в разных сетях VPN. Это позволяет избегать проблем, характерных для оверлейной модели, а также проблем виртуальной одноранговой модели.

В настоящей одноранговой модели каждая корпоративная сеть становится «маленьким Интернетом», где P-сеть играет роль провайдерской магистрали.

2.3.4. Таблицы VRF

Каждый PE-маршрутизатор поддерживает одну или несколько таблиц маршрутов и передачи (route/forwarding tables — VRF). Такая таблица поддерживается для каждого сайта, подключенного к PE-маршрутизатору. Если IP-адрес пакета указывает на то, что его нужно передать в сайт A, его ищут в таблице (forwarding table) сайта A только в том случае, когда пакет прибывает из сайта, ассоциированного с таблицей (forwarding table) сайта A.

Если сайт связан с несколькими сетями VPN, его таблица VRF может включать данные о маршрутах всех этих сетей. К примеру, сайт CE1 принадлежит к сетям VPNA и VPNB. В этом случае таблица VRF устройства PE1 будет содержать информацию о маршрутах сети VPNA и VPNB. Другими словами, на устройстве PE1 не будет двух отдельных таблиц VRF. Обычно на устройстве PE поддерживается по одной таблице VRF на сайт, даже если с этим сайтом у данного устройства имеется несколько соединений. Кроме того, если разные сайты пользуются одним и тем же набором маршрутов, они также будут объединяться в одну таблицу VRF.

Таблицы VRF на устройствах PE используются ТОЛЬКО для пакетов, поступающих из сайта, напрямую подключенного к данному устройству PE. Они не используются для маршрутизации пакетов, поступающих с других маршрутизаторов, установленных в магистрали сервис-провайдера. В результате к одному и тому же адресу в сети могут вести несколько маршрутов, потому что маршрут для передачи каждого пакета определяется в точке, через которую пакет попадает в магистраль. Так, например, один маршрут может использоваться для передачи пакетов из сети экстранет (где установлен межсетевой экран), а другой маршрут — для передачи пакетов по тому же адресу из сети интранет.

2.3.5 Отношения между PE- и P-маршрутизацией

P-маршрутизаторы подключаются к другим P-маршрутизаторам и к PE-маршрутизаторам. P-маршрутизаторы выполняют функции коммутации по меткам. При этом пакеты передаются только по меткам MPLS. В сетях MPLS-VPN для P-маршрутизаторов используется двухуровневый стек меток, с помощью которого пакеты передаются по магистрали из одного сайта VPN в другой. Обычно P-маршрутизаторы связываются друг с другом с помощью IGP-протокола маршрутизации (например, IS-IS или OSPF) и не имеют никакой информации о других маршрутах, кроме маршрутов, ведущих к PE-маршрутизаторам.

PE-маршрутизаторы вводят префиксы своих IP-адресов/32 в магистральные таблицы маршрутизации IGP. Это позволяет MPLS на каждом узле магистральной сети присваивать метки, указывающие на маршрут, ведущий к тому или иному PE-маршрутизатору.

Когда устройство PE получает пакет от устройства CE, оно выбирает определенную таблицу VRF для поиска адреса назначения для этого пакета. Если такой адрес найден

и если пакет предназначен для устройства CE, подключенного к данному PE-маршрутизатору, пакет направляется прямо на устройство CE и не передается в магистраль.

Если же пакет не предназначен для устройства CE, подключенного к данному устройству PE, для него находится следующий узел (BGP Next Hop), а также метка, которую этот узел BGP next-hop присвоил адресу назначения. Эта метка записывается в стек меток данного пакета и становится его Внутренней меткой.

Если следующий узел IGP (IBGP или OSPF) отличается от следующего узла BGP, в стек записывается дополнительная метка. Эта метка, указывающая на следующий узел BGP, становится Внешней меткой. (Если следующий узел BGP совпадает со следующим узлом IGP, вторая метка может не присваиваться).

После этого MPLS доставляет пакет по магистрали до соответствующего устройства CE в соответствии с Внешней меткой MPLS. Это значит, что все решения P-маршрутизаторов и PE-маршрутизаторов принимаются на основе данных MPLS, а IP-заголовок пакета не рассматривается, пока пакет не поступит на оконечный PE-маршрутизатор.

P-маршрутизатор (или PE-маршрутизатор), находящийся перед оконечным PE-маршрутизатором, удаляет Внешнюю метку из стека MPLS и направляет пакет оконечному PE-маршрутизатору. Оконечный PE-маршрутизатор просматривает Внутреннюю метку и отправляет пакет соответствующему устройству CE. Таким образом, до устройства CE доходит обычный IP-пакет, который не несет на себе никаких следов MPLS.

Чтобы изолировать сети VPN друг от друга, нужно сделать так, чтобы ни один магистральный маршрутизатор не принимал никаких пакетов с метками от соседних немагистральных устройств, кроме следующих случаев:

- когда Внешняя метка в стеке меток была сообщена P-маршрутизатором (магистральным маршрутизатором) немагистральному устройству;

- когда P-маршрутизатор (магистральный маршрутизатор) определяет, что в результате использования данной метки пакет покинет магистраль до считывания Внутренней метки в сетке и до считывания заголовка IP.

Эти ограничения необходимы для того, чтобы исключить передачу в VPN пакетов, которые для нее не предназначены.

2.4. Варианты топологии сетей MPLS-VPN

Существуют два варианта топологии, которые используются в сетях MPLS-VPN. Первый вариант мы рассматривали в разделе, посвященном одноранговой сетевой топологии. Второй вариант называется топологией Hub-and-Spoke (букв. — *«колесо и спицы»*).

2.4.1. Топология одноранговой сети MPLS-VPN

Общая топология одноранговых сетей MPLS-VPN состоит из сетей заказчиков, включающих множество сайтов и сетей VPN, CE-маршрутизаторов и PE-маршрутизаторов (пограничных устройств LSR), и из сети провайдера, в которой установлены P-маршрутизаторы (устройства LSR). На рисунке 8 показана общая топология сети MPLS-VPN.

На рисунке 8 CE-маршрутизаторы соединяют сеть за-

Рисунок 8. Топология одноранговой сети MPLS-VPN

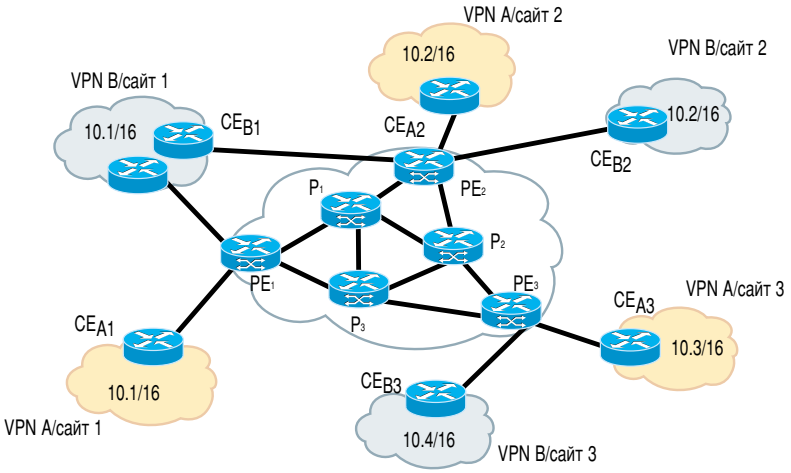
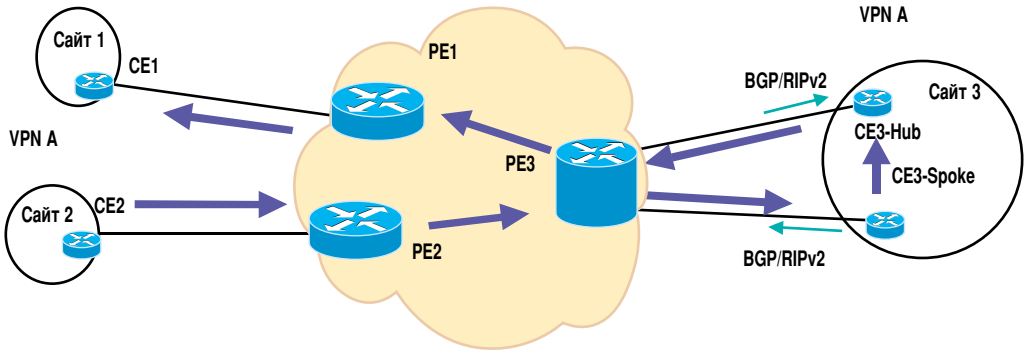


Рисунок 9. Сетевая топология MLS-VPN Hub-and-Spoke



казчика с сетью сервис-провайдера. CE-маршрутизаторы находятся под контролем заказчика. Они являются одноранговыми устройствами для PE-маршрутизаторов сервис-провайдера и обмениваются с ними данными о маршрутизации EBGP. CEA1 подключается к PE1 и является для него одноранговым устройством. CEA1 и PE1 пользуются одной и той же глобальной информацией о маршрутах (стандартной информацией об IP-маршрутах, к которой мы все привыкли). PE-маршрутизаторы и устройства CE общаются между собой с помощью EBGP, OSPF, RIPv2 или статических маршрутов.

Пограничное устройство LSR (PE-маршрутизатор) может подключаться к одному или нескольким CE-маршрутизаторам, поддерживать одну или несколько сетей VPN и подключаться к одному или нескольким сайтам в переделах одной VPN. К примеру, на рисунке 8, PE2 подключен к VPNA/Site 2 (CEA2), а также к VPNB/Site 1 и Site 2 (CEB1 и CEB2). Поэтому PE2 добавляет метки MPLS для сетей VPN A и B и создает адреса VPN-Ipv4 и таблицы VRF для обеих сетей.

В одноранговой сети MPLS-VPN магистраль имеет частичную или полную узловую топологию (meshed topology). Если CEA1 хочет отправить данные для VPN A/Site 3, пакет поступает на устройство PE1. PE1 добавляет к пакету необходимую метку и передает его устройству P3. P3 передает данные на устройство PE3. PE3 удаляет метку MPLS, просматривает IP-адрес и передает пакет устройству CEA3. CEA3 отправляет пакет конечному адресату, находящемуся в данном сайте.

А сейчас мы перейдем к другому варианту топологии, где маршрут, по которому проходит пакет, сильно отличается от маршрута, характерного для одноранговых сетей.

2.4.2. Сетевая топология MPLS-VPN Hub-and-Spoke

Другим вариантом топологии сетей MPLS-VPN является Hub-and-Spoke. Хотя одним из главных преимуществ сети MPLS-VPN является полная одноранговость, некоторые заказчики предпочитают отходить от нее и выбирают топологию Hub-and-Spoke. В этом сценарии все сайты (spokes) должны отправлять свой трафик через концентратор (hub). Эта топология является более сложной, потому что концентратор должен знать все другие сайты VPN и служить центральным транзитным пунктом для передачи трафика между ними. Топология Hub-and-Spoke для сетей MPLS-VPN показана на рисунке 9.

В этом сценарии весь трафик между сайтами должен проходить через центральный маршрутизатор CE3-Hub. Если, например, сайт 2 хочет отправить информацию сайту 1, то этот трафик пройдет через сеть сервис-провайдера, поступит на маршрутизатор CE3-Hub, затем опять попадет в сеть сервис-провайдера и лишь после этого попадет на сайт 1. В одноранговой топологии такой трафик проходит от CE2 к PE2, затем к PE1 и затем на сайт 1.

На рисунке 9 показана упрощенная версия топологии Hub-and-Spoke. Представьте себе сеть VPN с сотней сайтов, и все они подключены к единственному центральному маршрутизатору. Добавьте сюда еще один уровень сложности и представьте, что сервис-провайдер должен поддерживать сто сетей по сто сайтов в каждой, и в каждой из них используется топология Hub-and-Spoke. В этом случае для успешной поддержки всех сетей логическая сеть провайдера должна быть очень тщательно спроектирована и сконфигурирована.

Две перечисленные топологии — одноранговая и Hub-and-Spoke — лежат в основе любых сетей MPLS-VPN.

2.5. Безопасность в сетях MPLS-VPN

Из того, что было сказано выше, ясно, что функциональность MPLS-VPN поддерживает уровень безопасности, эквивалентный безопасности оверлейных виртуальных каналов в сетях Frame Relay и ATM. Безопасность в сетях MPLS-VPN поддерживается с помощью сочетания

протокола BGP и системы разрешения IP-адресов.

BGP-протокол отвечает за распространение информации о маршрутах. Он определяет, кто и с кем может связываться с помощью многопротокольных расширений и атрибутов community. Членство в VPN зависит от логических портов, которые объединяются в сеть VPN и которым BGP присваивает уникальный параметр Route Distinguisher (RD). Параметры RD неизвестны конечным пользователям, и поэтому они не могут получить доступ к этой сети через другой порт и перехватить чужой поток данных. В состав VPN входят только определенные назначенные порты. В сети VPN с функциями MPLS протокол BGP распространяет таблицы FIB (Forwarding Information Base) с информацией о VPN только участникам данной VPN, обеспечивая таким образом безопасность передачи данных с помощью логического разделения трафика.

Именно провайдер, а не заказчик присваивает порты определенной VPN во время ее формирования. В сети провайдера каждый пакет ассоциирован с RD, и поэтому попытки перехвата пакета или потока трафика не могут привести к прорыву хакера в VPN. Пользователи могут работать в сети интранет или экстранет, только если они связаны с нужным физическим или логическим портом и имеют нужный параметр RD. Эта схема придает сетям Cisco MPLS-VPN очень высокий уровень защищенности.

В опорной сети информация о маршрутах передается с помощью стандартного протокола Interior Gateway Protocol (IGP), такого как OSPF или IS-IS. Пограничные устройства PE в сети провайдера устанавливают между собой связи-пути, используя LDP для назначения меток. Назначения меток для внешних (пользовательских) маршрутов распространяется между PE-маршрутизаторами не через LDP, а через многопротокольные расширения BGP. Атрибут Community BGP ограничивает рамки информации о доступности сетей и позволяет поддерживать очень крупные сети, не перегружая их информацией об изменениях маршрутной информации. BGP не обновляет информацию на всех периферийных устройствах PE, находящихся в провайдерской сети, а приводит в соответствие таблицы FIB только тех PE, которые принадлежат к конкретной VPN.

Если виртуальные каналы создаются при оверлейной модели, исходящий интерфейс любого индивидуального пакета данных является функцией только входящего интерфейса. Это означает, что IP-адрес пакета не определяет маршрута его передачи по магистральной сети. Это позволяет предотвратить попадание несанкционированного трафика в сеть VPN и передачу несанкционированного трафика из нее.

В сетях MPLS-VPN пакет, поступающий в магистраль, в первую очередь ассоциируется с конкретной сетью VPN на основании того, по какому интерфейсу (подинтерфейсу) пакет поступил на PE-маршрутизатор. Затем IP-адрес пакета сверяется с таблицей передачи (forwarding table) данной VPN. Указанные в таблице маршруты относятся только к VPN принятого пакета. Таким образом, входящий интерфейс определяет набор возможных исходящих интерфейсов. Эта процедура также предотвращает как попадание несанкционированного трафика в сеть VPN, так и передачу несанкционированного трафика из нее.

3. Описание услуг и целей решения

В этом разделе описана базовая топология сетей MPLS-VPN и различные услуги MPLS-VPN, которые сервис-провайдер может предложить своим заказчикам. Архитектура MPLS-VPN отличается большой гибкостью и позволяет с помощью нескольких общих сценариев поддерживать огромное количество услуг.

В этом разделе мы расскажем о следующих услугах:

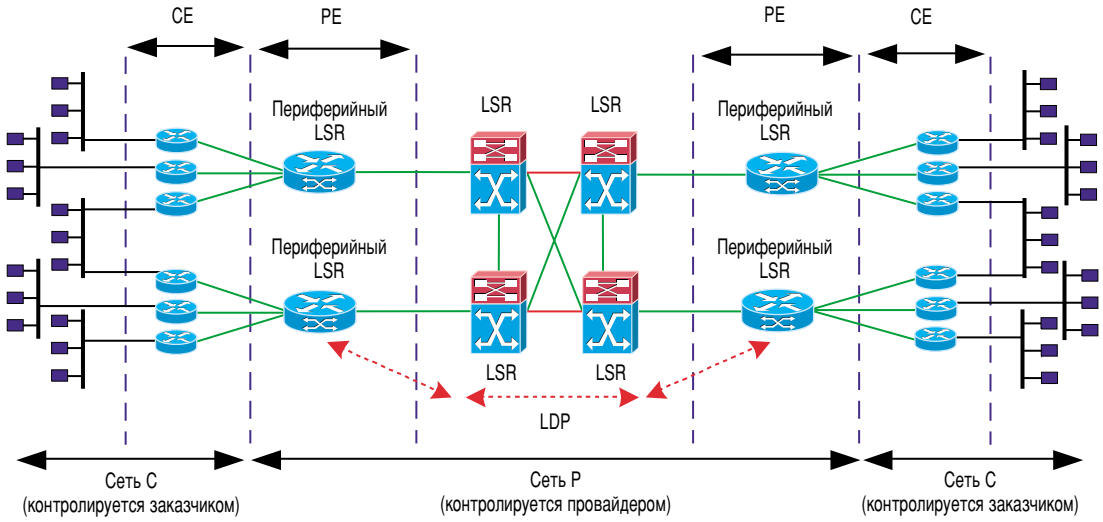
- **Intranet VPN** — как связать в единую корпоративную сеть все офисы и отделения заказчика.
- **Extranet VPN** — как создать общую межкорпоративную сеть для разных заказчиков.
- **VPN сетевого управления** — как обеспечить доступ для управления к маршрутизаторам CE, P и PE.
- **Доступ к внешним услугам** — как поддержать услуги третьих сторон в сетях интранет.
- **Доступ в Интернет** — как обеспечить доступ к Интернет-услугам.
- **Качество услуг (QoS)** — как поддержать дифференцированные услуги с разным уровнем качества.
- **Инжиниринг трафика** — как наиболее эффективно передавать трафик по сети.

3.1. Блок-схемы сети / решения

Типичная структура сети MPLS, реализованной в провайдерской инфраструктуре (т.е. в сети оператора связи или Интернет-провайдера), показана на рисунке 10. Сеть MPLS состоит из пограничных коммутирующих маршрутизаторов (Edge LSR), расположенных вокруг опорной сети с коммутирующими маршрутизаторами (Core LSR). Устройства LSR могут работать с ячейками ATM или с фреймами.

На рисунке 10 показана типичная сетевая инфра-

Рисунок 10. Сетевая топология MPLS-VPN



структура MPLS-VPN. Сети заказчиков подключаются к провайдерской сети MPLS с помощью CE-маршрутизаторов (пограничных маршрутизаторов заказчика). В терминологии MPLS-VPN пограничное устройство Edge LSR, поддерживающее услуги VPN-MPLS, называется устройством PE. Пограничный маршрутизатор заказчика (CE-маршрутизатор) выполняет обычные операции IP-передачи (статической или динамической) и, как правило, не поддерживает MPLS. Важно заметить, что устройства PE не являются частью сети заказчика. Они принадлежат сервис-провайдеру, который и осуществляет их эксплуатацию.

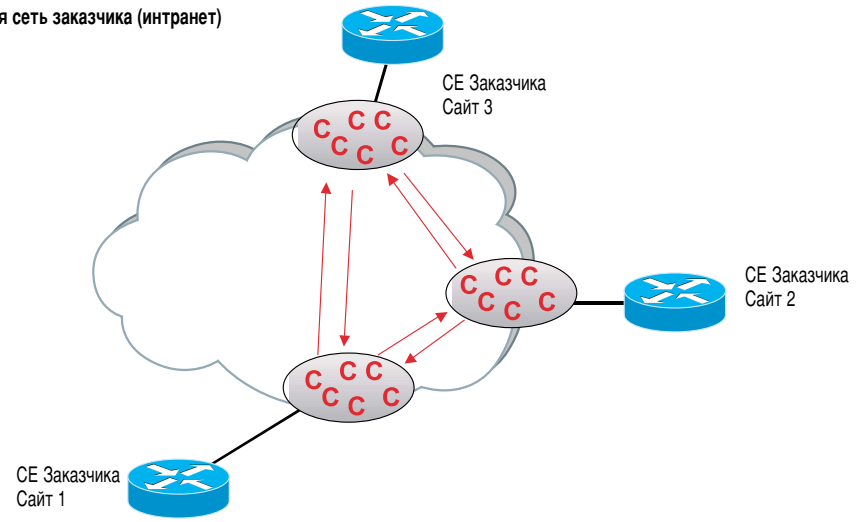
Устройство PE подключается к LSR. В терминологии MPLS-VPN устройство LSR называется P-маршрутизатором. P-маршрутизатор осуществсвляет коммутацию по меткам и входит в состав опорной сети сервис-провайдера.

3.2. Услуга интранет VPN

Intranet VPN является самым простым вариантом реализации сети VPN с функциями MPLS. Она включает все сайты данного заказчика. Эти сайты являются равноправными (одноранговыми). С точки зрения заказчика, все его сайты находятся на расстоянии одного сетевого перехода друг от друга. В реальности IP-пакет заказчика может передаваться не через один, а через несколько сетевых узлов, но заказчик этого не увидит.

На рисунке 11 показан заказчик с тремя сайтами. Каждый из них напрямую обменивается маршрутной информацией (VPN Route/Forwarding — VRF) с подключенными

Рисунок 11. Корпоративная сеть заказчика (интранет)



к нему одноранговыми сайтами. Заметим, что при этом передаются данные только о тех маршрутах, которые *порождаются* данной таблицей VRF. В результате на каждом PE-маршрутизаторе формируются идентичные маршрутные таблицы VFR данного заказчика, и каждый маршрут заказчика становится доступным через следующий PE-маршрутизатор.

3.3. Услуга экстранет VPN

3.3.1. Заказчики с уникальными адресами

Создание межкорпоративной сети (экстранет) требует импорта/экспорта данных о маршрутах между таблицами VRF нескольких заказчиков. Если у этих заказчиков нет совпадающих IP-адресов, то есть все их IP-адреса являются уникальными, то маршруты могут напрямую импортироваться в таблицы VRF.

На рисунке 12 показаны два заказчика, **Заказчик 1** и **Заказчик 2,** каждый из которых имеет по два сайта, **Сайт А** и **Сайт В**. Эти заказчики создают общую сеть экстранет, но она включает только два сайта: **Заказчик 1 Сайт А** и **Заказчик 2 Сайт В**. Все другие сайты этих заказчиков не будут подключены к сети экстранет до тех пор, пока их таблицы VRF не будут специально настроены для этого.

В таблице VRF на сайте **Заказчик** 1 **Сайт А** хранятся данные о маршрутах для всех сайтов **С1** (C1a, C1b E). Точно так же в таблице VRF на сайте **Заказчик 2 Сайт В** хранятся данные о маршрутах для всех сайтов **С2** (C2a, C2b).

Кроме этого, в таблицы VRF обоих сайтов дополнительно импортируются/экспортируются маршруты, используя параметр route-target. Таким образом, в таблице VRF сайта **Заказчик 1 Сайт А** содержатся данные обо всех маршрутах **C2b** сайта **Заказчик 2 Сайт В**, а в таблице VRF сайта **Заказчик 2 Сайт В** содержатся данные обо всех маршрутах **C1a** сайта **Заказчик 1 Сайт А**.

3.3.2. Заказчики с совпадающими (неуникальными) адресами

Если заказчики, желающие сформировать сеть экстранет, имеют пересекающееся адресное пространство или если появление новых членов сети экстранет может вызвать проблемы адресации, возникает необходимость в преобразовании (трансляции) адресов, прежде чем трафик попадет в сеть экстранет.

На рисунке 13 заказчики имеют совпадающее адрес-

Рисунок 12. Межкорпоративные сети экстранет

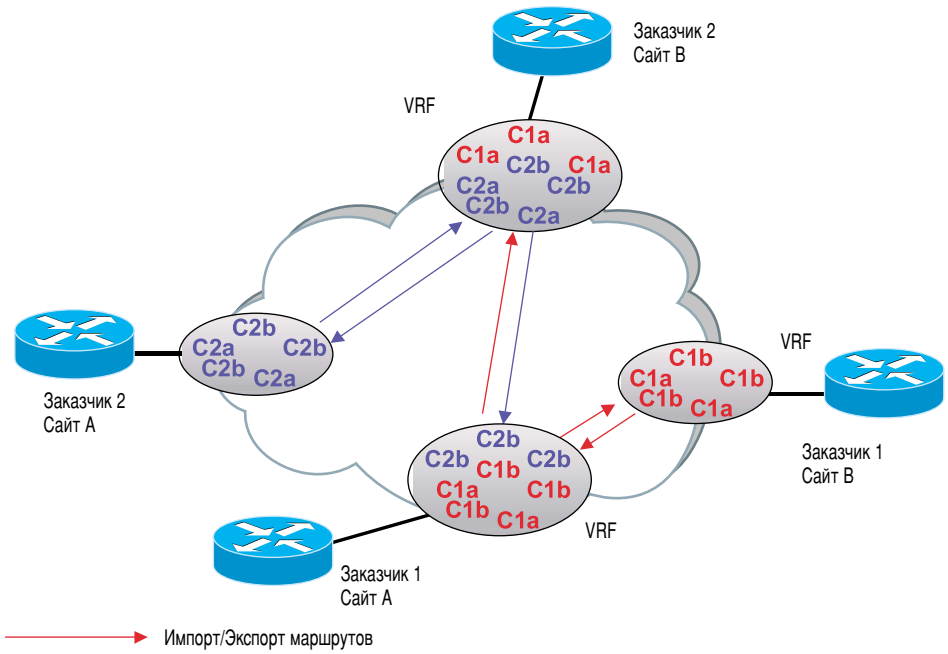
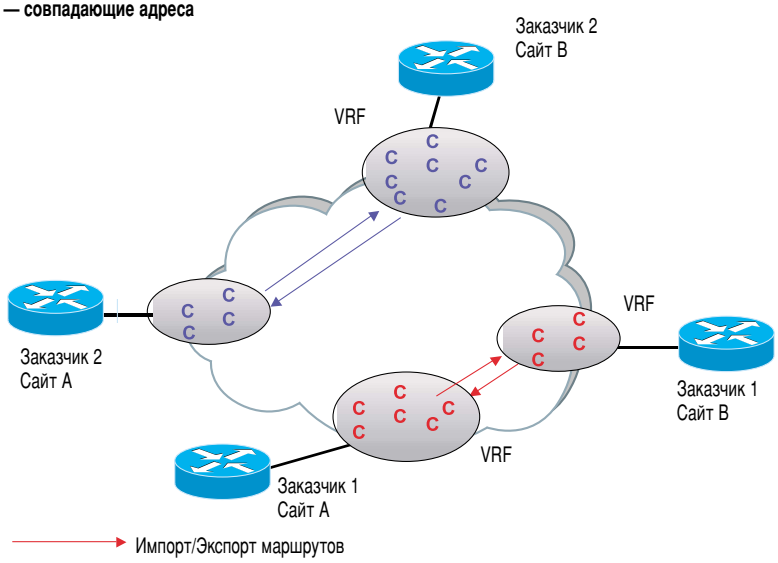


Рисунок 13. Межкорпоративные сети экстранет — совпадающие адреса



ное пространство **C**. Чтобы сайт **Заказчик 1 Сайт A** смог обмениваться данными о маршрутах с сайтом **Заказчик 2 Сайт B**, необходимо преобразование адресов (NAT), позволяющее сайту C1A передавать трафик в C2B и наоборот.

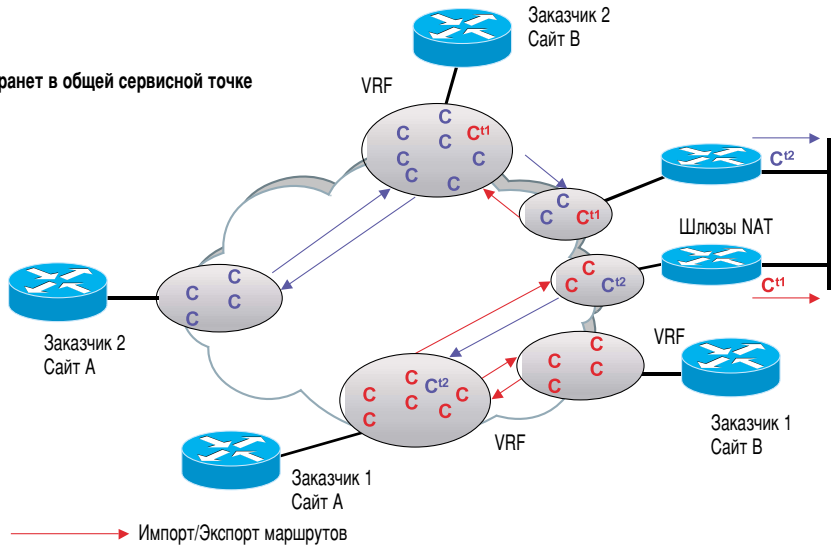
Текущая версия MPLS не позволяет PE-маршрутизатору напрямую преобразовывать адреса в таблицах VRF, и поэтому данная операция должна происходить за его пределами (либо в общей сервисной точке, либо на CE-маршрутизаторе).

3.3.3. Преобразование адресов экстранет в общей сервисной точке

На рисунке 14 показана трансляция адресов в центральной сервисной точке. Каждый заказчик будет иметь отдельный шлюз преобразования адресов (NAT gateway), который подключается к VRF в соответствующей сети Intranet VPN. Таблица VRF, подключенная к шлюзу NAT, будет включать данные о введенных в нее маршрутах преобразованных адресов другого заказчика. Поэтому C^{t1} инжектируется в таблицу VRF сайта **Заказчик 2 Сайт B**, а C^{t2} инжектируется в таблицу VRF сайта **Заказчик 1 Сайт A**. Каждый заказчик может работать в сети интранет с помощью двух шлюзов NAT. В качестве шлюзов NAT могут использоваться межсетевые экраны с функцией NAT. Это позволит дополнительно повысить безопасность при межсетевом взаимодействии заказчиков, включенных в один экстранет.

3.3.4. Преобразование адресов экстранет на границе

Рисунок 14. Преобразование адресов экстранет в общей сервисной точке



сети заказчика

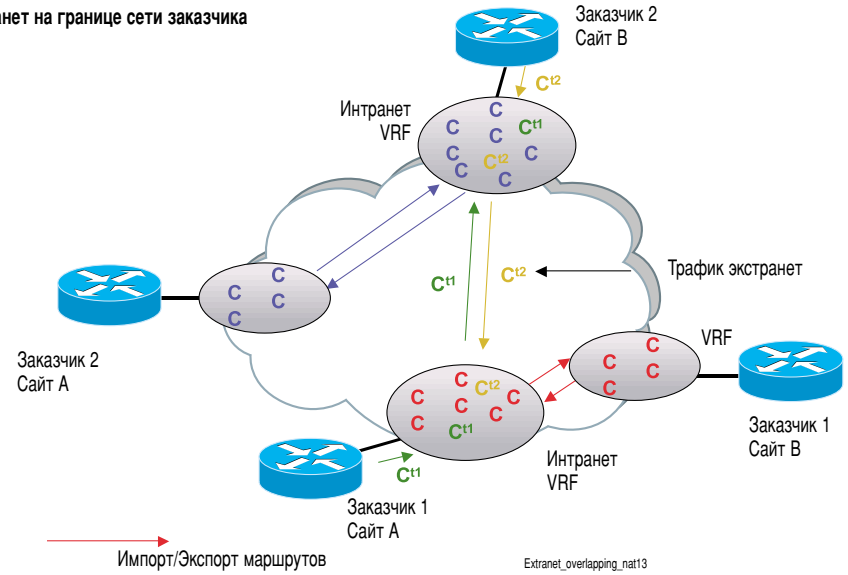
На рисунке 15 показана трансляция адресов на границе сети заказчика. Трафик Extranet/NAT и Intranet/non-NAT передается через один и тот же интерфейс, что позволяет экономить аппаратные ресурсы PE-маршрутизаторов.

Если CE-маршрутизаторы принадлежат заказчику, именно он несет ответственность за преобразование адресов на интерфейсах, выходящих на экстранет VRF, и за согласование используемых адресов. Сервис-провайдер берет на себя ответственность за создание таблиц

В таблицах VRF обоих заказчиков будут храниться введенные в них преобразованные адреса, которые позволят направлять пакеты в сеть экстранет. Специальная карта маршрутов и виртуальный интерфейс, которые имеются на каждом маршрутизаторе CE NAT, предотвращают преобразование адресов трафика, предназначенного для внутренних сетей интранет. К трафику интранет будет относиться любой пакет с адресом назначения, относящимся к адресному пространству **C**.

Поскольку трансляция адресов в экстранет происходит с обеих сторон, то для каждого адреса хоста, требующего взаимодействия через экстранет, требуется статическое

Рисунок 15. Преобразование адресов экстранет на границе сети заказчика



VRF и инжектирование в них данных о маршрутах с преобразованными адресами (в случае, когда используется статическая маршрутизация).

Более благоприятная ситуация возникает, когда сервис-провайдер предлагает заказчику услугу по управлению маршрутизаторами. В этом случае сервис-провайдер контролирует весь маршрут до CE-маршрутизатора и может поддерживать между CE-маршрутизаторами сквозное (end-to-end) управление NAT.

На рисунке 15 показаны два заказчика: **Заказчик 1 Сайт A (C1A)** и **Заказчик 2 Сайт B (C2B)**, которые работают в сети экстранет с преобразованием адресов (NAT). Когда **C1A** хочет установить связь с **C2B**, он транслирует свой адрес источника, заменив его на адрес из пула $\mathbf{C^{t1}}$, с помощью процедур динамической или статической трансляции. **C2B** поступает точно так же, но он заменяет адрес трафика, предназначенного для **C1A** , на адрес из пула $\mathbf{C^{t2}}$.

преобразование. Если преобразование будет динамическим, мы никогда не сможем определить, какой NAT-адрес был присвоен каждому из внутренних хостов.

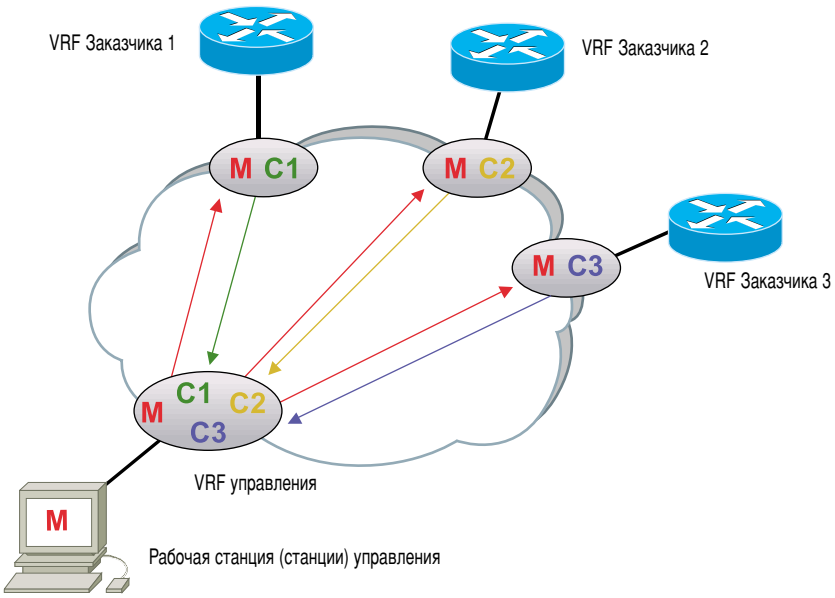
3.4. Услуга сетевого управления MPLS-VPN

3.4.1. Управление CE-маршрутизаторами

Сервис-провайдер может предоставлять заказчикам услугу по управлению их маршрутизаторами, позволяющую как минимум определять доступность того или иного устройства. Это особенно важно, если сервис-провайдер владеет устройствами CE, хотя в принципе все устройства CE (в том числе принадлежащие заказчику) должны включаться в общую систему управления. Ниже описан один из способов решения этой задачи.

В таблице сетевого управления VRF, которая называется **VPN_Network_Management**, содержатся адреса

Рисунок 16. Таблица VRF для управления устройствами CE



всех CE-маршрутизаторов. Имеющаяся у сервис-провайдера станция сетевого управления (или несколько станций) использует в своей работе именно эту таблицу VRF. С другой стороны, таблица VRF каждого заказчика должна содержать адрес станции управления сервис-провайдера (или нескольких станций), чтобы поддержать двустороннюю связь между станцией сетевого управления и CE-маршрутизатором.

Создание VRF сетевого управления позволяет управлять всеми CE-маршрутизаторами из единой точки. При этом гарантируется разделение маршрутизации между CE-маршрутизаторами. На рисунке 16 показаны процедуры импорта и экспорта маршрутов в таблице VRF.

Все CE-маршрутизаторы легко идентифицируются, так как пользуются адресами из единого адресного пространства, находящегося под управлением сервис-провайдера.

3.4.2. Управление маршрутизаторами MPLS опорной сети (P + PE)

Управление опорной сети необходимо как для мониторинга ее состояния и производительности, так и для поддержки конфигурирования P- и PE-устройств с помощью VPN Solutions Center.

Конфигурация управления маршрутизаторами опорной сети несколько отличается от управления CE-маршрутизаторами, поскольку адреса PE-маршрутизаторов находятся не в таблице VRF, а в глобальной таблице маршрутизации (Global Routing Table). Существует несколько способов управления устройствами PE. Первый состоит в управлении P-маршрутизаторами и PE-маршрутизаторами с помощью таблицы VRF, а другой — в управлении ими с помощью глобальной таблицы.

3.4.2.1. Управление устройствами P и PE с помощью таблицы VRF

Управление P-маршрутизаторами и PE-маршрутизаторами с помощью таблицы VRF показано на рисунке 17.

Адреса loopback'ов P и PE находятся в глобальной таблице маршрутизации, но адрес рабочей станции сетевого управления находится в таблице VRF. Чтобы обеспе-

Рисунок 17. Таблица VRF для управления устройствами PE

чить связь между опорной сетью MPLS и рабочей станцией управления, необходимо инжектировать в таблицу VRF глобальный статический маршрут, указывающий на адреса сети MPLS, а в глобальную таблицу маршрутизации нужно инжектировать статический маршрут, указывающий на адрес рабочей станции.

3.4.2.2. Управление устройствами P и PE с помощью глобальной таблицы

Другим способом управления опорной сетью является прямое подключение сети управления к интерфейсу, определенному в глобальной таблице маршрутизации. Другими словами, у нее не будет ассоциаций с таблицей VRF. Это самый простой и прямой способ управления опорной сетью. Он показан на рисунке 18.

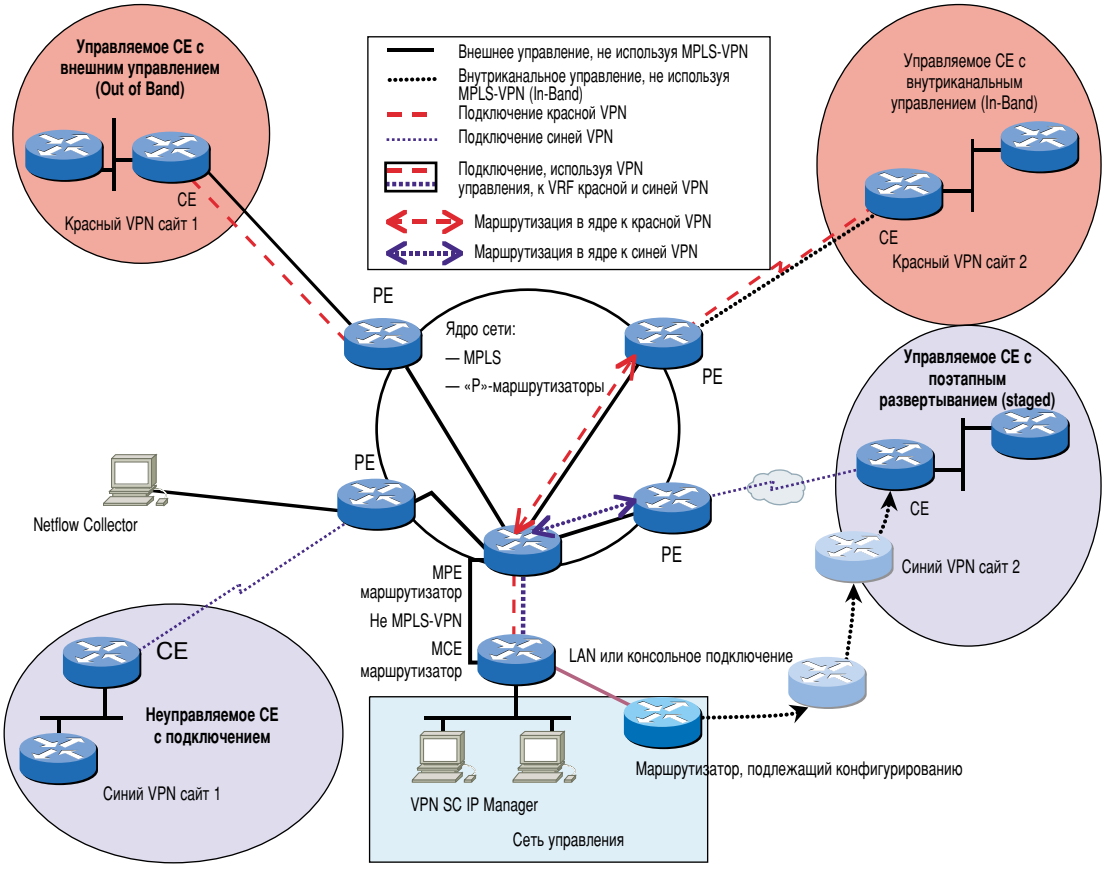
Рисунок 18. Управление PE-маршрутизаторами с помощью глобальной таблицы маршрутизации (Global Routing Table)

3.4.3. Подсеть сетевого управления: Extranet Multiple VPN

Для управления типа Extranet Multiple VPN (другое название — Rainbow Management) необходимо рабочие станции VPN Solutions Center и элемент-менеджеры подключить к единой локальной сети и к маршрутизатору управления (management router — MCE). На рисунке 19 подробно показана подсеть управления, подключенная к MPE.

Маршрутизатор MCE, подключаемый к PE-маршрутизатору, должен подключаться к non-MPLS-VPN и MPLS-VPN через два разных интерфейса. Соединение MPLS-VPN называется Extranet Multiple VPN. Эта сеть VPN будет импортировать в таблицы VRF информацию о маршрутах для связи со всеми управляемыми устройствами

Рисунок 19. Центр VPN Solutions Center: метод управления Extranet Multiple VPN



CE, которые разрешено конфигурировать центру VPN Solutions Center. Соединение non-MPLS-VPN будет использоваться маршрутизатором MCE для связи с Netflow Collector и PE-маршрутизаторами. Неуправляемым CE-маршрутизаторам не нужны Extranet Multiple VPN, и канал non-MPLS-VPN link может использоваться для поддержки устройств PE. Для связи между устройствами MCE и MPE в сетях MPLS-VPN рекомендуется использовать динамическую маршрутизацию. Статический маршрут будет в этом случае опционным, и маршрут по умолчанию будет использоваться для связи с Интернет. С помощью VPN Solutions Center пользователь должен определять ресурсы, необходимые для поддержки связи между маршрутизаторами MCE, а PE-маршрутизаторы должны соединять между собой все сети VPN в случае наличия необходимых ресурсов.

VPN Solutions Center поддерживает управление сетями VPN с помощью экстранет на PE, поэтому устройства CE реально подключаются к сети управления (Management VPN) и сети заказчика (VPN). Оператор, выполняющий инсталляцию, должен пользоваться списками доступа (access-lists) и экспортировать карты маршрутов на устройства PE, чтобы для управления CE-маршрутизаторами использовалась только одна подсеть адреса хоста. В этой системе устройство CE будет считаться «спицей» (spoke) VPN управления, поэтому весь трафик управления в целях безопасности будет направляться на маршрутизатор MCE. В результате конечный пользователь не сможет проникнуть в другие сети VPN через VPN управления.

3.5. Доступ к внешним услугам

Одно из преимуществ MPLS-VPN состоит в том, что заказчики могут пользоваться единой IP-инфраструктурой с частными адресами, которые не обязательно должны быть уникальными для опорной сети сервис-провайдера. Уникальность этих адресов должна соблюдаться только в пределах внутрикорпоративной сети интранет.

Проблемы с уникальностью адресации возникают только в случае соединений с абонентами, которые находятся за пределами сети VPN заказчика. К таким соединениям относятся:

- соединения с другим заказчиком или группой заказчиков (экстранет), которые могут иметь совпадающие адреса;
- подключения к услугам общего доступа (DNS, web-кэширование, web-хостинг, электронная почта или Интернет);
- подключение к провайдерам информационного наполнения (например, к финансовым учреждениям).

3.5.1. Заказчики с зарегистрированными адресами

Если у заказчика уже есть зарегистрированное адресное пространство IP, то глобальная уникальность его адресов не представляет никакой проблемы. Любые услуги общего доступа и сети экстранет, к которым получает доступ этот заказчик, могут напрямую инжектировать свои префиксы в его таблицы VRF. В этом случае заказчик сам решает, как контролировать доступ к этим услугам. Собственно говоря, так он поступает и без MPLS-VPN, используя межсетевые экраны, прокси-устройства и средства контроля доступа на маршрутизаторах.

Нет никаких препятствий, мешающих заказчику с зарегистрированными Интернет-адресами пользоваться системой доступа к услугам, которые будут описаны в следующих разделах. С точки зрения сервис-провайдера, легче пользоваться единым подходом к предоставлению услуг, независимо от типа адресных пространств тех или иных пользователей. Единственная разница в этом случае будет состоять в том, что описанный в следующих разделах этап преобразования адресов (NAT) не будет обязательным для заказчиков с зарегистрированным адресным пространством.

3.5.2. Заказчики с частными адресами

Большинство заказчиков будет скорее всего использовать частные адреса (RFC 1918), и поэтому для связи между сетью VPN заказчика и услугами общего доступа и сетями экстранет нужно будет применять какую-то систему трансляции адресов. Если этого не сделать, то вы не сможете точно определить адрес-источник в сети заказчика, так как часть адресов обязательно будет совпадать.

В следующих разделах описываются два способа связи с абонентами, которые находятся за пределами частной сети VPN заказчика (это может быть Интернет или экстранет с преобразованием адресов). В обоих случаях используется функция преобразования адресов CISCO (Network Address Translation — NAT), которая поддерживается операционной системой IOS™. Разница между ними заключается в месте, где происходит преобразование. Эти способы доступа к услугам называются:

- доступ к услугам на устройстве CE (Service Access at the CE);
- доступ к услугам на шлюзе (Service Access at a Gateway) сервис-провайдера.

3.5.2.1. Доступ к услугам на устройстве CE

Для доступа устройств CE к услугам NAT лучше, когда эти устройства принадлежат сервис-провайдеру, который ими и управляет. Такая схема позволяет просто и легко предоставлять услуги NAT устройствам CE.

На рисунке 20 показаны услуги NAT, предоставляемые устройствам CE для связи с сетями общего доступа и для связи с собственной сетью интранет через тот же физический канал. В принципе, это вариант экстранет-доступа (заказчик – заказчик), хотя здесь чаще используется динамическое, а не статическое преобразование адресов. Заметим, что «сетью общего доступа» здесь может быть все что угодно — от серверной фермы до сети Интернет-провайдера (ISP) или провайдера прикладных услуг (ASP).

У заказчика в таблице VRF содержатся все адреса **C**, которые импортируются и экспортируются между всеми другими таблицами VRF, принадлежащими к сети интранет этого заказчика. Все таблицы VRF, действующие на всех сайтах данного заказчика, определяют адресное пространство его сети Intranet VPN.

В этой таблице VRF также содержится преобразованное зарегистрированное адресное пространство **C**^{T}. На рисунке видно, что этот заказчик подписался на две услуги — **P1** и **P3** — и импортировал в свою таблицу VRF все маршруты, относящиеся к этим услугам.

Кроме того, адресное пространство CT также экспортируется в каждую таблицу VRF, относящуюся к услугам, чтобы обеспечить двустороннюю связь между провайдером приложений (ASP) и заказчиком.

Карты маршрутов, виртуальные интерфейсы и списки доступа настраиваются таким образом, чтобы пакет с адресом назначения из пространства C мог общаться с другим хостом интранет VPN без преобразований адресов, поскольку CE-маршрутизатор будет и без этого (в «родном» режиме) направлять IP-пакет на устройство PE.

Если заказчик с исходным адресом C1 отправляет запрос хост-системе с адресом P1, CE-маршутизатор преобразует C1 в C1^{T}, и PE-маршрутизатор, согласно таблице VRF, направит пакет к P1.

Недостаток этого дизайна в том, что каждое устройство CE должно иметь пул зарегистрированных адресов. Эту проблему можно смягчить, если одно устройство CE будет выступать в качестве концентратора доступа к услугам для данного заказчика, как в топологии Hub-and-Spoke. Подход Hub-and-Spoke обычно будет использоваться для Интернет-доступа, когда трафик проходит через прокси-серверы и межсетевые экраны, установленные в информационном центре заказчика.

3.5.2.2. Доступ к услугам через шлюз (с ориентацией на заказчика)

Сервис-провайдер также может предоставить доступ к услугам своей внутренней сети. Ниже описан подход к доступу через шлюз с ориентацией на заказчика. Это означает, что каждый заказчик будет идентифицироваться на шлюзе с помощью отдельного подинтерфейса. Преимущество этого подхода заключается в точной идентификации заказчиков, четком определении необходимых им услуг и простоте управления. Любое изменение кон-

Рисунок 20. Доступ к услугам и преобразование адресов на устройстве CE

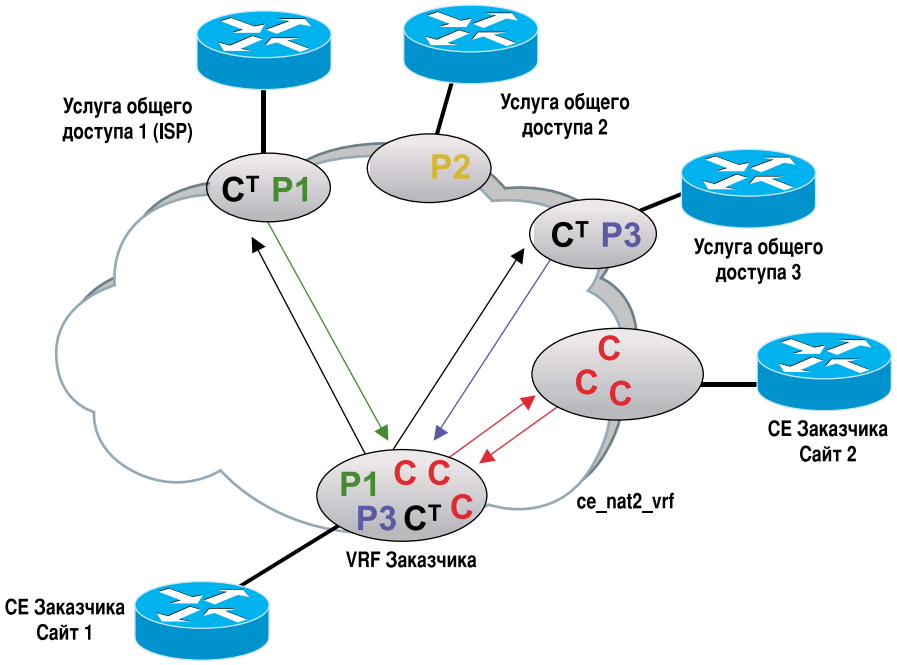
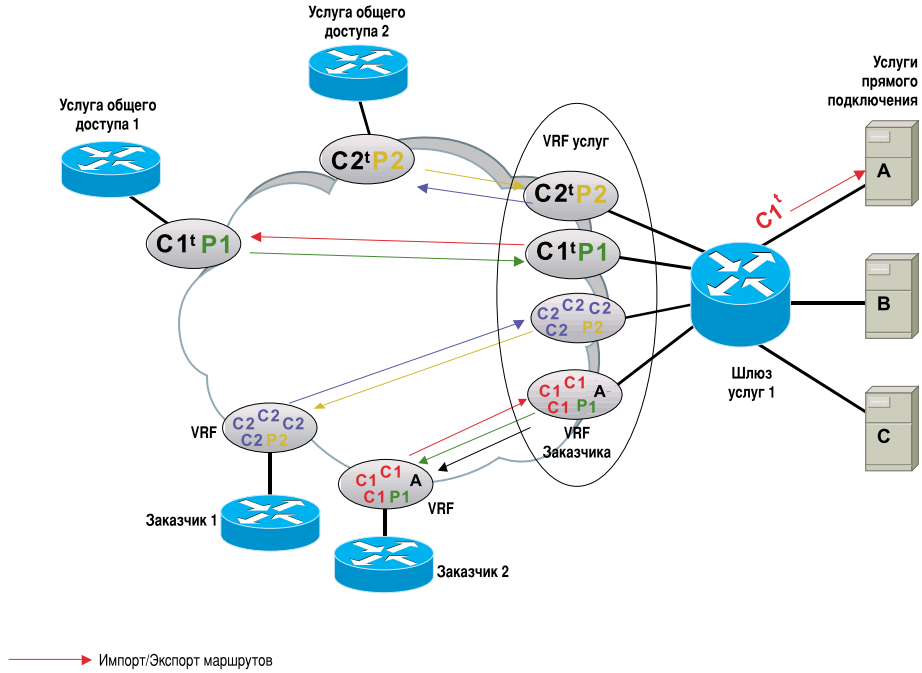


Рисунок 21. Услуги и преобразование адресов на шлюзе (с ориентацией на заказчика)



фигурации связывается только с данным заказчиком (таблицей VRF и подинтерфейсом), что ограничивает влияние конфигурационных ошибок на других заказчиков. Небольшой недостаток состоит в том, что для каждого заказчика нужно определять отдельный интерфейс и таблицу VRF, что увеличивает объем конфигурации и требует большего объема памяти на шлюзе и PE-маршрутизаторах в точке предоставления услуг.

В этом сценарии весь трафик, предназначенный для доступа к внешним услугам, должен проходить через шлюз (service gateway router). Этот шлюз транслирует адреса и отправляет пакет к следующей VRF или непосредственно к подключенному хосту. Кроме этого, шлюз выполняет функции межсетевого экрана, повышая общий уровень безопасности. Преимущество шлюза состоит в том, что его пул адресов может использоваться всеми заказчиками. Таким образом повышается эффективность использования адресов.

На рисунке 21 показаны два заказчика, пользующиеся услугами, которые предоставляются через шлюз Service Gateway 1. Этот шлюз настроен на предоставление пяти разных услуг. Три из них предоставляются по прямым каналам связи со шлюзом (**A, B, C**), а две другие предоставляются в других местах, и доступ к ним осуществляется с помощью индивидуальных таблиц VRF (Public Service 1 и Public Service 2). Эти таблицы определяются на PE-маршрутизаторе. Все услуги должны иметь зарегистрированные IP-адреса.

Каждый заказчик должен иметь на шлюзе свой отдельный подинтерфейс. Шлюз подключается к соответствующему PE-маршрутизатору, который имеет таблицу VRF данного заказчика, определенную на каждом подинтерфейсе, ведущем к шлюзу.

3.5.2.3 Доступ к услугам через шлюз (с ориентацией на услуги)

Описанную выше схему можно изменить, сориентировав ее не на заказчиков, а на услуги. Каждая услуга на шлюзе (service gateway) будет иметь связанную с ней таблицу VRF и подинтерфейс. Эти таблицы VRF определяются в той части сети, где действуют непреобразованные адреса. Другими словами, в большинстве случаев в этих таблицах будет отражаться частное адресное пространство заказчика. Из этого вытекает, что адреса любого заказчика, который пользуется шлюзом (service gateway), не должны совпадать с адресами других заказчиков, которые пользуются тем же шлюзом (такое же правило действует и в предыдущем сценарии, ориентированном на заказчиков).

Любой заказчик, подписывающийся на данную услугу, должен импортировать данные о маршрутах (route-target), которые экспортируются из сервисной таблицы VRF. И наоборот, каждая сервисная таблица VRF должна импортировать маршруты заказчиков для поддержки двусторонней связи. В этом примере единая таблица VRF для всех услуг создается в той части сети, где используются преобразованные адреса. Это упрощает задачи настройки конфигурации, но затрудняет точный

контроль над доступом.

На рисунке 22 показан тот же шлюз (*service gateway*), который был описан в сценарии, ориентированном на заказчика, но у него имеется пять таблиц VRF, определенных на стороне с непреобразованными адресами, и одна таблица VRF для всех услуг на стороне с преобразованными адресами. **Заказчик 2** подписывается на услугу **P2**, импортируя маршрут к **P2 (route-target). Заказчик 1** подписывается на услуги **P1** и **A**, импортируя маршрут к **P1** и маршрут к **A**.

С той стороны шлюза (service gateway), где действуют преобразованнные адреса, располагается единая таблица VRF со статическим маршрутом для всех преобразованных адресов **Cx**^{t} . Этот маршрут ведет обратно к шлюзу. Пул преобразованных адресов **Cx**^{t} также импортируется в каждую сервисную таблицу VRF (**P1** и **P2**), чтобы трафик мог вернуться к шлюзу.

Таблицы VRF с преобразованными адресами на PE-маршрутизаторе PE-I импоритруют маршруты каждой услуги (**P1** и **P2**), к которой предоставляется доступ. Услуги **A**, **B** и **C** являются локальными для домена маршрутизации шлюза и поэтому не требуют специальной конфигурации MPLS-VPN.

3.6. Услуга Интернет-доступа

3.6.1. Простой совместный Интернет-доступ (трансляция адресов на множестве общих шлюзов)

Структура совместного доступа к Интернет предназначена для заказчиков, которым нужен простой способ выхода в Интернет без установки собственных средств кэширования и межсетевых экранов. Этот способ хорошо подходит в основном для малых предприятий, не имеющих собственной информационно-технологической инфраструктуры. Преобразование адресов выполняется сервис-провайдером на общем шлюзе (или шлюзах). В редких случаях вся сеть заказчика пользуется зарегистрированными IP-адресами, и тогда трансляции адресов (NAT) не требуется, а трафик проходит этап NAT без обработки.

Главное преимущество преобразования адресов в центральной точке состоит в экономии зарегистрированного адресного пространства, так как все заказчики совместно пользуются адресами из единого пула. На рисунке 23 показан общий шлюз для доступа в Интернет. Используемый по умолчанию маршрут **I** импортируется в таб-

Рисунок 22. Доступ к услугам через шлюз (с ориентацией на услуги)

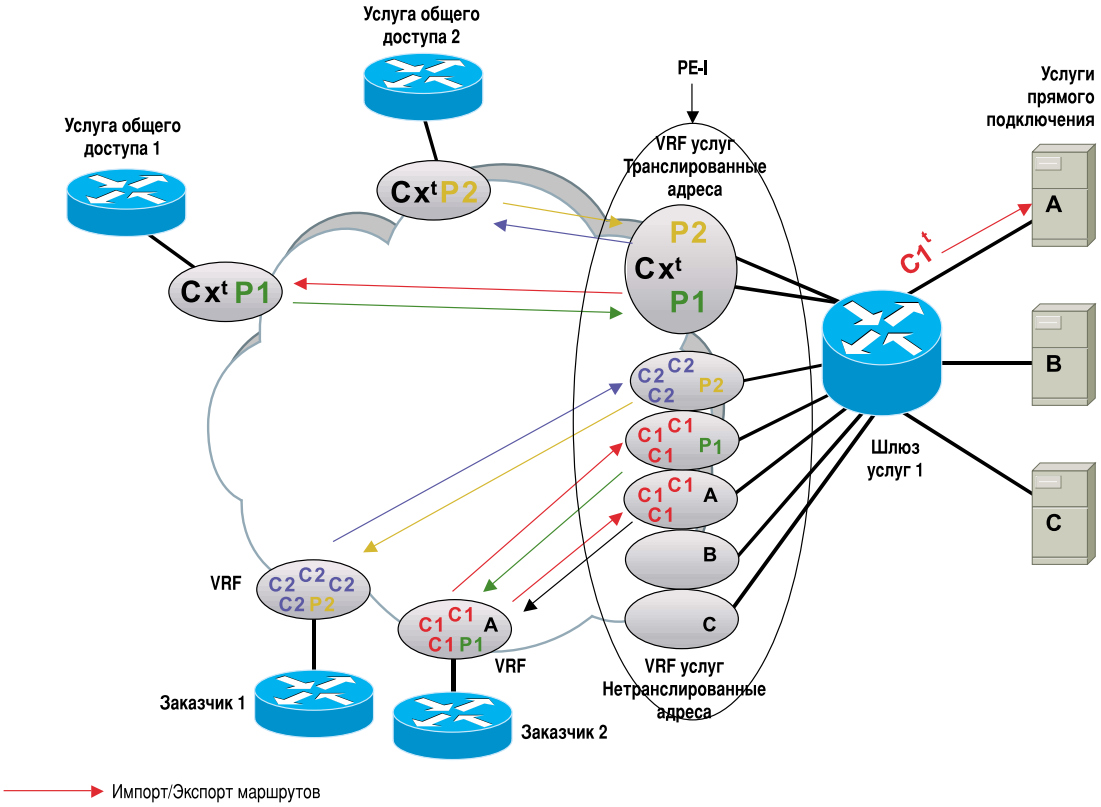
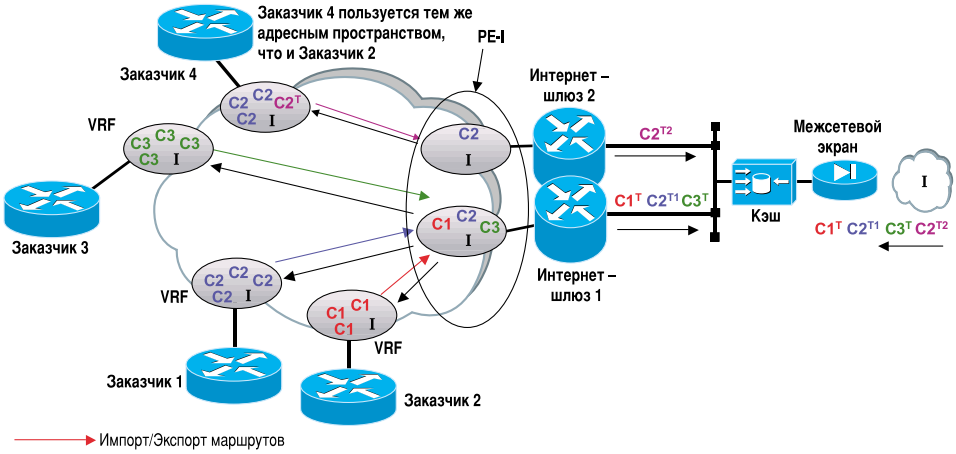


Рисунок 23. Совместный Интернет-доступ — множество шлюзов NAT



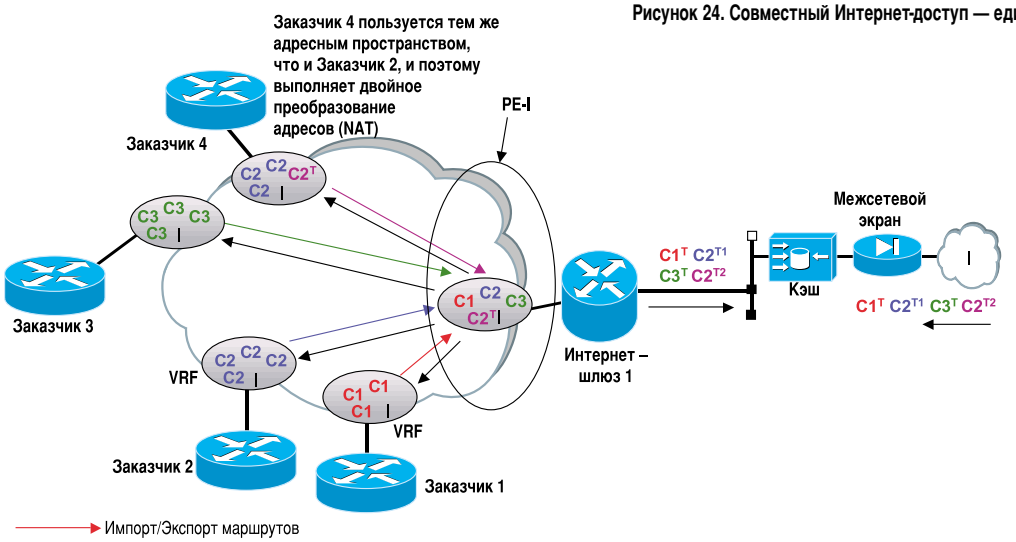
лицы VRF каждого заказчика, и поэтому любой трафик от заказчика, местонахождение которого явно не указывается, передается на маршрутизатор **Internet Gateway**. Соответствующие маршруты заказчиков импортируются в таблицы Интернет VRF и на PE-маршрутизатор PE-I. Маршрутизатор **Internet Gateway** будет преобразовывать адрес заказчика в зарегистрированный IP-адрес, взятый из доступного пула (**Cx -> Cx**^{t}), и затем передавать пакет через механизм кэширования и межсетевой экран в Интернет. Преобразование адресов может выполняться и на межсетевом экране.

Проблема с этим дизайном, как и с любым дизайном, включающим центральный шлюз, заключается в том, что единый шлюз может преобразовывать адреса только для заказчиков, адреса которых не совпадают. Если заказчики пользуются единым адресным пространством, они должны иметь отдельный шлюз, выполняющий преобразование адресов для каждого заказчика, работающего в общем адресном пространстве. Множество Интернет-шлюзов могут, однако, иметь общий доступ к единому межсетевому экрану, как показано на рисунке 23.

3.6.2. Простой совместный Интернет-доступ (трансляция адресов на одном общем шлюзе)

Если используется единый Интернет-шлюз (т.е. все преобразования адресов выполняются единым устройством) и если этим устройством пользуются заказчики с совпадающими адресами, трансляция адресов выполняется в два этапа. Этот процесс называется «двойной трансляцией» (double NAT). Первая трансляция выполняется на CE-маршрутизаторе с помощью незарегистрированных адресов, чтобы не тратить ограниченных ресурсов зарегистрированного пула. Это преобразование позволяет шлюзу уникально идентифицировать заказчиков с совпадающими адресами и затем производить вторую трансляцию (присвоение зарегистрированных адресов) для доступа в Интернет. Этот пример показан

Рисунок 24. Совместный Интернет-доступ — единый шлюз NAT



на рисунке 24.

Заказчик 4 пользуется тем же адресным пространством, что и Заказчик 2, поэтому общий шлюз (Internet NAT Gateway) не может их различить. Это значит, что Заказчик 4 должен преобразовать свой адрес, сделав его уникальным. Для этого используется пул незарегистрированных адресов C2T. Этот уникальный пул может предоставляться и контролироваться сервис-провайдером. После того, как пакет поступает на общий шлюз (NAT Gateway), C2T распознается как уникальный адрес Заказчик 4 и преобразуется в зарегистрированный адрес, который далее будет обрабатываться в обычном порядке.

3.6.3. Интернет-доступ с использованием глобальной таблицы маршрутизации

Все перечисленные схемы предоставляли доступ в Интернет с помощью таблицы VRF, в которой содержался используемый по умолчанию маршрут к шлюзу (Internet Gateway). Другой метод опирается на доступ к шлюзу с помощью глобальной таблицы маршрутизации. Его можно описать следующим образом:

- К сети MPLS подключается маршрутизатор, имеющий выход в Интернет. Этот маршрутизатор может инжектировать или не инжектировать маршруты BGP в глобальную таблицу маршрутизации. Заметим, что с протоколом BGP работают только PE-маршрутизаторы. P-маршрутизаторы не работают с BGP.
- Заказчик, которому нужен доступ в Интернет, получит для использования маршрут по умолчанию, который будет инжектирован в его таблицу VRF. Этот маршрут будет указывать на loopback-адрес маршрутизатора Internet Gateway. Этот адрес находится в глобальной таблице маршрутизации, и поэтому в конце команды статического маршрута необходимо добавить метку «global». Эта метка заставит систему обратиться к глобальной таблице маршрутизации.
- Статический маршрут для сети заказчика также должен вводиться в глобальную таблицу маршрутизации, чтобы указывать обратный маршрут к CE. Этот статический маршрут может быть объявлен в сеть Интернет с помощью BGP.

Главное условие для этого сценария состоит в том, что заказчик должен пользоваться зарегистрированными адресами, которые могут записываться в глобальную таблицу маршрутизации, имеющуюся у сервис-провайдера.

3.7. Качество услуг (QoS)

QoS — это сетевая архитектура, позволяющая администраторам контролировать такие параметры передачи трафика, как задержка, колебания задержки и потери пакетов в сети. QoS на Уровне 3 необходима для поддержки приложений, имеющих критически важное значение для бизнеса. Кроме того, QoS помогает провайдерам поддерживать разные виды трафика (данные, голос и видео) в единой сетевой архитектуре и предлагать услуги IP VPN корпоративного качества, а также подписывать с заказчиками соглашения о гарантированном качестве услуг (Service Level Agreements — SLA).

MPLS позволяет поддерживать и наращивать QoS в очень крупных сетях, поскольку провайдеры могут присваивать трафику разные наборы меток, соответствующие разным классам услуг. Класс услуг в потоках MPLS можно указывать двумя способами. Первый из них предназначен для маршрутизируемых опорных сетей, где используются методы IP Precedence, Type-of-Service (ToS) или DiffServ. Второй предназначен для поддержки усовершенствованных методов QoS в сетях Cisco IP + ATM MPLS. Конкретные способы поддержки QoS определяются в конкретном контексте каждой сетевой архитектуры. QoS поддерживается не отдельными устройствами, а всей системной архитектурой в целом. В данном разделе описываются основы технологий QoS, которые взаимодействуют с MPLS для поддержки операторского качества услуг в сетях VPN.

В операторских сетях VPN не рекомендуется поддерживать QoS в каждом отдельном потоке из-за слишком большого числа IP-потоков в таких сетях. Главной задачей QoS в крупных сетях VPN является поддержка множества классов услуг (Layer 3 CoS). К примеру, сеть сервис-провайдера может поддерживать три класса услуг: класс высокой приоритетности «premium» с низкой задержкой, класс «mission-critical» с гарантированной доставкой и, наконец, низкоприоритетный класс «best-effort». Каждый класс по-своему тарифицируется, и абоненты могут приобретать те услуги, которые отвечают их потребностям. Так, например, абонент может подписаться на услугу с гарантированной доставкой и низкой задержкой для голосовых приложений и видеоконференций и на низкоприоритетную услугу для трафика электронной почты.

Практическая реализация QoS в сети требует разделения труда, которое помогает добиться высокой эффективности. Поскольку задачи QoS требуют интенсивной обработки, в модели Cisco они распределяются между пограничными LSR и LSR опорной сети. Эта схема добивается оптимальной эффективности и масштабируемости, рабо-

тая с менее скоростной сетевой периферией и более скоростной опорной сетью. Измерения трафика, необходимые для поддержки дифференцированных классов услуг, требуют проведения четырех процедур. Во-первых, сервис-провайдер устанавливает пороговые значения для входящего трафика на пограничных устройствах LSR (PE), а также иные параметры, определяющие класс входящего трафика. Все задачи, требующие интенсивной работы процессоров, выполняются на пограничных устройствах, которые распознают приложения и классифицируют пакеты в соответствии с уникальными правилами, действующими у того или иного заказчика. Кроме того, пограничные устройства обеспечивают управление полосой пропускания. Во-вторых, устройства, установленные в опорной сети, поддерживают класс услуг (CoS), определенный пограничными устройствами. В-третьих, выходные устройства, так же как и входные, имеют наборы пороговых значений. Пороговые значения скорости передачи на входе и выходе предотвращают переполнение сети и потерю трафика. Эта модель хорошо масштабируется и подходит для использования в операторских сетях VPN.

Операционная система Cisco IOS™ включает несколько функций поддержки QoS на Уровне 3, которые особенно хорошо подходят для поддержки и управления VPN. Сети с функциональностью MPLS используют следующие возможности Cisco IOS™ для поддержки сквозной архитектуры QoS:

- IP Precedence
- Committed Access Rate (CAR)
- Weighted Random Early Detection (WRED)
- Weighted Fair Queuing (WFQ)
- Class-Based Weighted Fair Queuing (CBWFQ)
- Modified Deficit Round Robin (M-DRR)

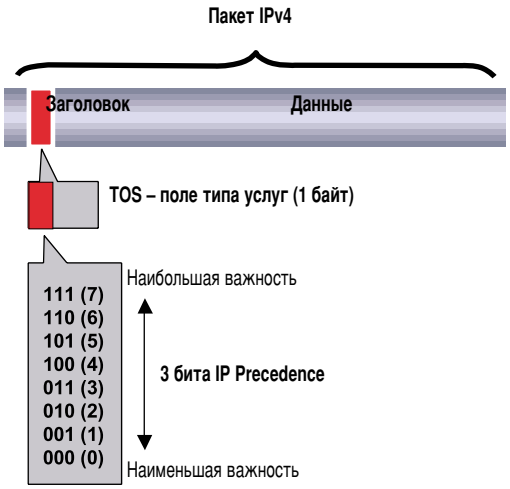
3.7.1. IP Precedence

IP Precedence использует три бита приоритетности (precedence bits) в заголовке IPv4. Это поле типа услуги (Type-of-Service), которое указывает на класс услуг (CoS) для каждого пакета, как показано на рисунке 25. Эти величины устанавливаются на периферии сети MPLS-VPN и поддерживаются в опорной сети. С помощью битов приоритетности трафик можно разделить на шесть классов (еще два класса резервируются для внутрисетевого использования).

В таблице 1 показан пример соотношения между услугами и битами IP Precedence.

В каждом классе для дополнительной дифференциации можно определить множество битов приоритетности. В методе Weighted Random Early Detect используется приоритетность отбрасывания (drop precedence), которая показывает, какие пакеты можно сбрасывать, чтобы избежать переполнения (этот метод описывается ниже). Трафик с самым низким уровнем приоритетности (IP Precedence) будет сбрасываться первым, а трафик с самым высоким уровнем приоритетности — последним.

Рисунок 25. Биты IP Precedence



3.7.2. Committed Access Rate (CAR)

Committed Access Rate представляет собой средство

Таблица 1. Классы услуг, приложения и IP Precedence

Класс		Биты IP Precedence
Золотой	Высшая приоритетность, критически важные приложения, голос поверх IP (VoIP), видеопотоки	4 5
Серебряный	Приложения клиент/сервер	2,3
Бронзовый	Просмотр web-страниц/передача IP-трафика по возможности	0,1

Cisco, предназначенное для поддержки QoS в сетевой периферии (edge). CAR позволяет определить контракт для передачи трафика в маршрутизируемых сетях. Вы можете классифицировать трафик и применять к нему определенные правила (policies) на входном интерфейсе, а также устанавливать правила обработки трафика, превышающего лимит полосы пропускания.

CAR можно использовать для установки приоритетов на основе расширенного списка классификации. Это создает большую гибкость распределения приоритетов, включая присвоение приоритетов приложениям, портам, адресам источника/назначения и т.д. CAR — это механизм, работающий на основе правил. Он классифицирует трафик на основе гибких правил, включая правила приоритетности (IP Precedence), контрольные списки IP-доступа (IP access control lists), входящие интерфейсы и MAC-адреса. CAR ограничивает скорость передачи на входе определенным пороговым уровнем, что помогает избежать переполнения опорной сети.

В ситуациях, когда для подключения заказчиков используются частные виртуальные каналы (PVC) Frame Relay или ATM, функции этих технологий, связанные с правилами (CIR, PCR и т д.), будут ограничивать скорость входящего трафика той скоростью, на которую подписан абонент. Таким образом, CAR не обязательно используется для ограничения скорости передачи, но всегда применяется для классификации пакетов.

Технология Ethernet не имеет встроенных средств, связанных с правилами или формированием трафика (policing/shaping), так как за ограничение скорости передачи отвечают устройства, работающие на уровнях выше Уровня 2. Если заказчик подключен к сети через интерфейс доступа 10Мбит Ethernet, но подписан на скорость 512 кбит/с, то скорость для него нужно ограничить или подчинить определенным правилам доступа. То же самое относится к любым заказчикам, использующим для доступа технологию DSL. Технология кабельных модемов позволяет ограничивать скорость на самом кабельном модеме (CE) с помощью конфигурационного файла DOCSIS.

В случае необходимости ограничение скорости может происходить в одной из двух точек:

- на входном или выходном устройстве CE (на входе/выходе PE);
- на входном или выходном устройстве PE (на входе/выходе заказчика, где может быть установлен или не установлен CE-маршрутизатор).

Настоятельно рекомендуется при малейшей возможности ограничивать скорость передачи на устройствах CE, чтобы не перегружать процессор PE-маршрутизатора. Выполнение функций CAR на устройстве CE распределяет нагрузку на процессоры, так как каждое устройство CE отвечает только за одного заказчика, тогда как устройство PE должно поддерживать множество заказчиков.

Базовая функциональность CAR требует соблюдения следующих критериев:

- **Направление пакетов**, входящие или исходящие.
- **Средняя скорость** (в битах в секунду) определяется длительными замерами средней скорости передачи. Трафик, передающийся с более низкой скоростью, всегда удовлетворяет этот критерий.
- **Нормальный пиковый уровень (normal burst size)**, в байтах, показывает допускаемую величину, которую может иметь пик трафика, прежде чем система зарегистрирует превышение лимита.
- **Чрезмерный пиковый уровень**, в байтах.

Вероятность того, что трафик, находящийся между нормальным и чрезмерным пиковым уровнем, превысит допустимые лимиты, повышается по мере повышения размеров пика. CAR передает пиковый трафик. Эта функция не занимается выравниванием пиков и формированием трафика.

Для вычисления скорости (в битах в секунду) CAR использует все данные о соединении. Сюда входят не только пользовательские данные, но и данные протоколов Уровня 2 и Уровня 3.

3.7.3. Weighted Random Early Detection (WRED)

Технология WRED предназначена для профилактики сетевых переполнений, прежде чем они превратятся в серьезную проблему. Для этого используются средства протокола TCP, предназначенные для мониторинга потоков. WRED производит мониторинг трафика в разных точках сети и сбрасывает пакеты в случае угрозы переполнения. В результате источник трафика замечает потерю пакетов и замедляет скорость передачи. WRED сочетается с другими средствами, которые, как правило, действуют «постфактум», т.е. когда переполнение уже возникло.

При приеме пакета WRED выполняет следующие действия:

- рассчитывает средний размер очереди;
- если размер очереди меньше минимальной пороговой величины, пакет ставится в очередь;
- если размер очереди находится между минимальной и максимальной пороговой величиной, пакет либо отбрасывается, либо ставится в очередь в зависимости от класса обслуживания данного типа трафика;
- если средний размер очереди превышает максимальную пороговую величину, пакет отбрасыва-

ется.

Для каждого класса определяется политика (правила обслуживания). Каждый класс получает определенный процент полосы пропускания. К примеру, Бронзовый класс получает минимум 10% полосы пропускания, Серебряный — 25% и Золотой — 40%. Заметим, что это минимальные величины, и если какому-то классу нужна дополнительная пропускная способность, он может воспользоваться свободными ресурсами другого класса. Выделенная полоса пропускания должна быть достаточна для передачи служебной информации Уровня 2.

Вы можете установить правила для любого количества классов, которые может поддержать маршрутизатор (максимум 64 класса). Однако общее количество полосы пропускания, выделенной для всех классов, не должно превышать 75% общей полосы пропускания на данном интерфейсе. Остальные 25% используются для контрольного трафика и трафика, связанного с маршрутизацией. Если полоса пропускания распределена не полностью, то остающаяся ее часть распределяется по классам пропорционально выделенной для них полосе пропускания.

Параметры WRED устанавливаются для каждого класса и определяют вероятность сбрасывания пакетов для каждого из них. Чем выше класс, тем ниже вероятность сбрасывания пакетов. Эти параметры определяют поведение WRED в каждой очереди. Когда средневзвешенная длина очереди находится ниже минимальной пороговой величины, никакие пакеты не отбрасываются. Когда эта средняя длина находится между минимальной и максимальной пороговыми величинами, вероятность сброса пакетов рассчитывается по прямой линии, соединяющей минимальную величину (вероятность = 0) и максимальную величину (вероятность равна единице, деленной на показатель приоритетности). Вероятность сброса пакетов системой WRED показана на рисунке 26.

При подходе к максимальной пороговой величине (1292 пакета) все очереди сбрасывают пакеты с вероятностью 10%. При этом вероятность сброса трафика с нулевой приоритетностью выше, чем трафика с приоритетностью номер 5. Это значит, что при увеличении длины очередей (что свидетельствует об угрозе переполнения) трафик нулевой приоритетности будет сбрасываться в первую очередь, увеличивая вероятность нормальной передачи трафика высокой приоритетности.

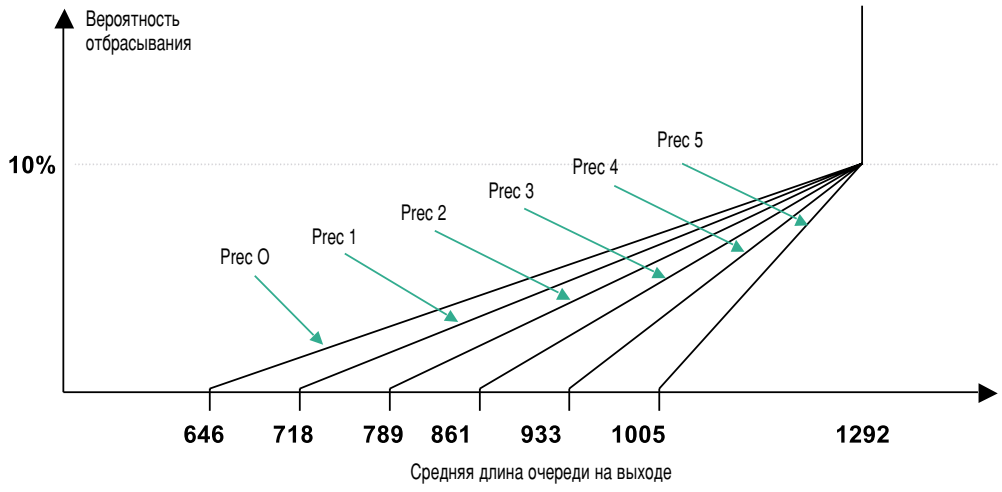
Величины, показанные в этом примере, использованы для иллюстрации. Для окончательного отлаживания и настройки параметров в производственной сети необходимо тщательное тестирование и мониторинг.

3.7.4. Weighted Fair Queuing (WFQ)

Метод «взвешенной справедливой очередности» (WFQ) предназначен для ситуаций, когда необходимо поддержать разумное время реагирования для интенсивных и неинтенсивных пользователей, не накладывая излишней нагрузки на полосу пропускания. WFQ представляет собой алгоритм очередности для потоков трафика, который одновременно выполняет две задачи: ставит интерактивный трафик в начало очереди, чтобы сократить время реагирования, и справедливо распределяет оставшуюся полосу пропускания между потоками трафика с более низким уровнем приоритетности.

WFQ гарантирует, что очереди не останутся без поло-

Рисунок 26. Профиль WRED



сы пропускания и что трафик будет передаваться с предсказуемой скоростью. При этом трафик, имеющий критически важное значение для бизнеса, будет иметь самую высокую приоритетность с гарантированной доставкой и низкой задержкой. Остающаяся полоса пропускания будет равномерно распределяться между потоками низкоприоритетного трафика.

Метод WFQ предназначен для максимального облегчения настройки конфигурации. Он автоматически настраивается на меняющиеся условия передачи трафика. В целом WFQ работает настолько хорошо, что многие приложения используют его по умолчанию в качестве основного средства управления очередями на большинстве последовательных интерфейсов, работающих на скоростях E1 (2,048 Мбит/с) и ниже.

Если высокоприоритетный трафик отсутствует, WFQ эффективно использует свободную полосу пропускания для передачи низкоприоритетного трафика. Это выгодно отличает WFQ от технологии мультиплексирования с временным разделением (TDM), которая выделяет полосу пропускания разным типам трафика и не использует ее, если трафик какого-либо типа отсутствует. WFQ взаимодействует с методом QoS IP Precedence и вместе с ним поддерживает дифференцированные и гарантированные уровни качества услуг (QoS).

Кроме этого, алгоритм WFQ помогает решать проблему колебаний задержки. Если WFQ используется в сети, где одновременно поддерживается множество широкополосных сеансов связи, скорость передачи и общее время задержки для этих сеансов становятся гораздо более предсказуемыми. WFQ резко оптимизирует работу таких алгоритмов, как алгоритм TCP для контроля над переполнением и алгоритмы «медленного старта» (slow-start features). Результатом использования WFQ всегда является предсказуемая пропускная способность и предсказуемое время реагирования в каждом активном потоке.

3.7.5. Class Based Weighted Fair Queuing (CBWFQ)

Метод «взвешенной справедливой очередности с учетом классов» (CBWFQ) дает возможность перераспределения пакетов и управления задержкой на сетевой периферии и в опорной сети. Присваивая каждому классу обслуживания определенный «вес», CBWFQ позволяет коммутатору или маршрутизатору управлять буферизацией и полосой пропускания каждого класса. Поскольку «вес» является относительной, а не абсолютной величиной, свободные ресурсы могут распределяться между классами, что позволяет использовать полосу пропускания с максимальной эффективностью.

CBWFQ позволяет накладывать класс обслуживания

Рисунок 27. Class Based Weighted Fair Queuing

на часть сетевого канала. К примеру, определенный класс QoS может настраиваться таким образом, чтобы занимать максимум 35% канала OC3. На рисунке 27 показан пример трех классов обслуживания, определенных с помощью CBWFQ:

- Золотой — с гарантированной доставкой и временем задержки;
- Серебряный — с гарантированной доставкой;
- Бронзовый — с доставкой по мере возможности.

Разделяя управление полосой пропускания и буферизацией, сервис-провайдер может настроить каждый класс на определенные потребности заказчиков. Так, например, сервис-провайдер может предложить Золотой класс для голосового трафика. В этом случае широкая полоса пропускания обеспечит передачу всех ячеек, а умеренная величина буфера будет достаточна для ограничения задержки. Поскольку доля полосы пропускания зависит от относительного «веса», присвоенного тому или иному классу, присвоение высокого (Золотого) веса голосовому трафику гарантирует соблюдение минимальных требований. Если ресурсы Золотого класса не будут использоваться, они будут распределяться между остальными классами пропорционально их весу. Таким образом обеспечивается максимальная эффективность передачи трафика при наличии свободной полосы пропускания.

3.7.6. Взаимодействие между WFQ и IP Precedence

Метод WFQ взаимодействует с методом IP Precedence. Это значит, что он может распознавать приоритетные пакеты по меткам в битах IP-приоритетности и отправлять их быстрее, обеспечивая более короткое время реагирования для этого трафика. По мере роста величины приоритетности этот алгоритм выделяет данному сеансу связи все более широкую полосу пропускания, чтобы обеспечить более качественное обслуживание этого трафика в случае переполнения. WFQ присваивает вес каждому потоку, и этот вес определяет порядок передачи пакетов в очередях. Он создает возможность перераспределения пакетов и управления латентностью на сетевой периферии и в опорной сети. Присвоение разных весов разным классам обслуживания позволяет коммутатору управлять буферизацией и полосой пропускания каждо-

го класса. Этот механизм ограничивает колебания задержки для трафика, чувствительного ко времени (т.е., для голоса и видео).

3.7.7. Modified Deficit Round Robin (MDRR) — GSR

Устройства GSR поддерживают механизм управления очередностью с учетом классов, который получил название Modified Deficit Round Robin (MDRR). Он работает примерно так же, как описанный выше механизм CBWFQ.

При использовании MDRR пакеты помещаются в очереди с учетом битов CoS/приоритетности в заголовке метки MPLS. Другими словами, биты IP Precedence просматриваются в устройстве PE и, в случае необходимости, модифицируются, а затем копируются в поле CoS, которое имеется в метках MPLS. Функция CoS Transparency (прозрачность CoS) обеспечивает возможность независимого заполнения поля MPLS CoS. Это значит, что биты IP Precedence в пакете заказчика остаются нетронутыми. В этом случае IP-пакет заказчика можно передавать по сети с соблюдением установленного CoS на всем протяжении канала связи.

Очереди обслуживаются по принципу Round Robin, то есть каждая очередь имеет свой относительный вес. Этот вес определяет количество данных, которые будут выведены из очереди за один цикл. GSR имеет семь обычных очередей MDRR (с номерами от 0 до 6) и одну очередь низкой задержки. Каждая очередь MDRR имеет свой относительный вес, и поэтому распределение полосы пропускания соответствует классам обслуживания (CoS). Алгоритм MDRR выводит данные из очередей (если в них есть данные) в следующей очередности: 0-1-2-3-4-5-6-0-1-2-3-4-5-6 ... Если в сети сервис-провайдера из-за установленных правил очередности заполняются только первые три очереди, то сканироваться будут все равно все семь очередей, несмотря на то, что очереди 3 – 6 всегда будут пустыми. Это будет продолжаться до тех пор, пока не поменяются правила.

Одна из очередей называется очередью высокой приоритетности, и отношение к ней отличается от отношения к другим очередям. Она обрабатывается по принципу строгой приоритетности или по принципу альтернативной приоритетности.

В режиме строгой приоритетности очередь обслуживается немедленно каждый раз, когда в ней появляются какие-либо данные. Так гарантируется наименьшее время задержки для трафика данного типа. Однако это может негативно повлиять на все остальные очереди, поскольку очередь высокой приоритетности может забирать себе слишком широкую полосу пропускания.

В режиме альтернативной приоритетности очереди обслуживаются одна за другой: вначале приоритетная, затем одна из неприоритетных, затем снова приоритетная и за ней другая неприоритетная и так далее. Этот способ обработки используется по умолчанию.

Каждый раз при обработке той или иной очереди из нее передается то количество данных, которое определяется ее относительным весом. Вес 1 означает вес, равный MTU. Для интерфейса OC3/STM-1 это будет 4470 байт. Для каждой последующей единицы веса добавляется по 512 байт. В таблице 2 показан пример относительных весов и объемов данных, передаваемых из очереди за каждый цикл обработки.

3.8. Инжиниринг трафика

В этом разделе описывается инжиниринг трафика в сетях MPLS. Функция MPLS Traffic Engineering (TE) позволяет сети сервис-провайдера эмулировать возможности инжиниринга трафика, существующие в сетях Уровня 2, таких как Frame Relay и ATM. Инжиниринг трафика на Уровне 3 создает возможность контролировать отдельные сетевые маршруты, снижая вероятность переполнения и повышая экономичность передачи IP-трафи-

Таблица 2. Относительные веса MDRR

Класс	Процент	Вес	Байты выхода из очереди
Бронзовый	20,00%	1	4470
Серебряный	30,00%	5	6705
Золотой	50,00%	14	11175

ка в маршрутизируемых сетях. Цель инжиниринга трафика на Уровне 3 заключается в том, чтобы максимально задействовать в работе все сетевые ресурсы. Обычно в сетях IP есть много альтернативных маршрутов, по которым трафик передается к месту назначения. Если полагаться только на протоколы маршрутизации, то некоторые маршруты окажутся переполненными, в то время как другие будут простаивать.

Инжиниринг трафика MPLS:

- создает единый подход к инжинирингу трафика. С помощью MPLS возможности инжиниринга трафика вводятся на 3-й Уровень, что позволяет оптимизировать маршрутизацию IP-трафика с учетом ограничений, накладываемых емкостью и топологией сетевой магистрали;
- маршрутизирует потоки трафика по сети с учетом доступных сетевых ресурсов;
- использует «маршрутизацию с учетом ограничений», т.е. выбирает для передачи трафика наиболее короткий маршрут, отвечающий требованиям (ограничениям) данного потока. В MPLS TE у трафика существуют требования к полосе пропускания, требования к среде передачи, требования приоритетности и т.д.;
- распознает сетевые сбои и отказы, меняющие топологию сети, и приспосабливается к новому набору ограничений.

Инжиниринг трафика позволяет сервис-провайдеру предложить своим пользователям лучшие услуги с контролируемой пропускной способностью и временем задержки. Это достигается за счет классификации данных и передачи этих данных по туннелям, отвечающим требованиям данного трафика.

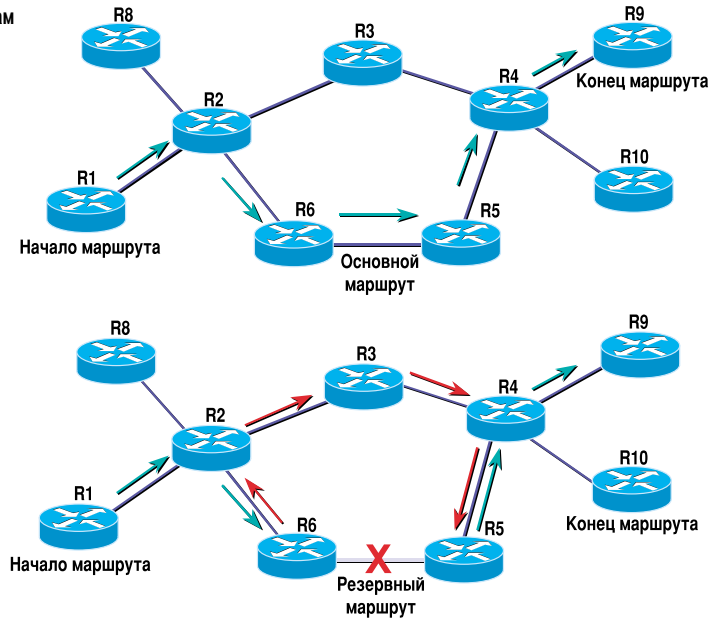
Инжиниринг трафика MPLS снимает необходимость в ручной настройке сетевых устройств на поддержку определенных маршрутов. Вместо этого вы можете воспользоваться функциональностью MPLS Traffic Engineering, которая распознает топологию сети и установит динамические маршруты с помощью автоматической сигнализации. При определении маршрутов в сетевой магистрали эта функция учитывает полосу пропускания и объем потока трафика. И наконец, MPLS Traffic Engineering имеет механизм динамической адаптации, который повышает отказоустойчивость магистрали.

Далее мы рассмотрим вопросы, связанные с восстановлением услуг с помощью инжиниринга трафика (Traffic Engineering Service Restoration), а затем поговорим о маршрутизации MPLS с целью резервирования ресурсов (MPLS Routing for Resource Reservation — RRR) в маршрутизируемой опорной сети MPLS. Следует заметить, что инжиниринг трафика работает только с протоколами Link State Routing Protocols (IS-IS, OSPF) и не работает с протоколами Distance Vector Routing Protocols (RIP, EIGRP).

3.8.1. Восстановление услуг с помощью инжиниринга трафика

В MPLS TE существует метод восстанавления услуг. Это достигается с помощью функции защиты каналов или быстрой перемаршрутизации (Link Protection или Fast ReRoute).

Рисунок 28. Защищенный канал с коммутацией по меткам



Новой функцией инжиниринга трафика является «быстрая перемаршрутизация» или Fast ReRoute (FRR). Функция FRR может защитить от сбоя индивидуальный канал. Время коммутации защищенных каналов FRR подобрано таким образом, чтобы отвечать стандартам SONET/SDH (около 50 мсек).

Это означает, что каждый канал LSP может быть защищен с помощью резервного маршрута, который начинает работать *с момента отказа канала,* независимо от главного маршрутизатора (head-end-router). Эта технология отличается от простой защиты канала, когда именно главный маршрутизатор активизирует работу резервного канала.

Если вы используете FRR, главный маршрутизатор даже не будет знать об отказе. С точки зрения этого маршрутизатора, туннель TE будет действовать как обычно.

На рисунке 28 показан процесс Fast ReRoute. Канал между **R6** и **R5** защищен с помощью Fast ReRoute. В случае сбоя **R6** определит, что канал не работает, и сразу же передаст все данные в резервный туннель TE через **{R2,R3,R4}** к **R5**. Важно помнить, что данные или трафик с метками, передаваемый по резервному каналу, обязательно должен попадать на маршрутизатор, подключенный к другому концу защищаемого канала.

В приведенном примере трафик передается по резервному каналу очень длинным путем. Это не столь важно, поскольку механизм защиты канала уже запущен, трафик передается, сеть знает о сбое и принимает меры к поиску более оптимального маршрута. После восстановления канала с помощью таймеров оптимизации маршрута будет восстановлен и первоначальный LSP.

3.8.2. Инжиниринг трафика MPLS с учетом Diff-Serv (инжиниринг трафика с гарантированной полосой пропускания — GB TE)

Туннель TE имеет возможность учитывать требования Diff-Serv. Возникает возможность создания с помощью MPLS Traffic Engineering гарантированного туннеля «точка—точка» и отправления избранного трафика по этому туннелю. В текущей версии поддерживаются два пула полосы пропускания. При этом используются проекты (drafts) стандарта IETF:

a) требования к поддержке Diff-Serv-Aware Traffic Engineering;

b) дополнения к RSVP-TE и CR-LDP для поддержки Diff-Serv-Aware Traffic Engineering;

c) дополнения к OSPF для поддержки Diff-Serv-Aware Traffic Engineering;

d) дополнения к IS-IS для поддержки Diff-Serv-Aware Traffic Engineering.

В маршрутизируемых опорных сетях Cisco технология MPLS позволяет поддерживать элегантный механизм инжиниринга трафика. MPLS позволяет менеджерам накладывать потоки трафика на специально сконфигурированные маршруты и отправлять избранный трафик по заранее просчитанным маршрутам, настроенным на поддержку определенных параметров для определенных заказчиков.

MPLS Diff-Serv-Aware Traffic Engineering позволяет сетевым операторам применять «определенную» маршрутизацию (explicit routing), которая заменяет собой традиционный механизм передачи IP и автоматизирует процессы оптимизации использования сетевых ресурсов. При этом создается один или несколько «определенных» маршрутов с гарантированной полосой пропускания для каждого транка. Принимаются во внимание правила и ограничения для транков, а также наличие физических сетевых ресурсов и сетевая топология. Таким образом, маршруты передачи пакетов зависят не только от адреса пункта назначения, но и от наличия сетевых ресурсов и установленных правил.

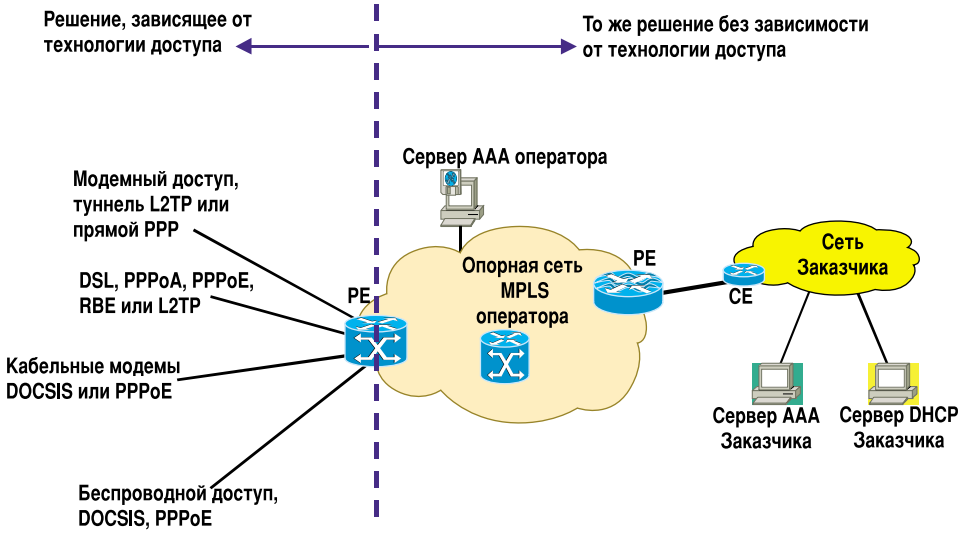
MPLS Diff-Serv-Aware Traffic Engineering пользуется несколькими базовыми технологиями: MPLS, OSPF, IS-IS и Resource Reservation Protocol (RSVP). Использование RSVP для инжиниринга трафика отличается от первоначальных задач, для которых был разработан протокол RSVP. В этом случае RSVP используется только пограничными маршрутизаторами (edge routers) для поддержки потоков unicast, определенных отправителем. Для поддержки высокой масштабируемости сессии RSVP создаются отдельно для каждого трафика

транка.

4. Топология сети доступа MPLS-VPN

Решения Cisco VPN не зависят от типа доступа. Это значит, что какая-то особая технология доступа для них не требуется. В этом разделе мы расскажем о разных технологиях доступа и соответствующих PE-маршрутизаторах, способных поддержать требования MPLS-VPN для этих

Рисунок 29. Удаленный доступ к решениям MPLS-VPN



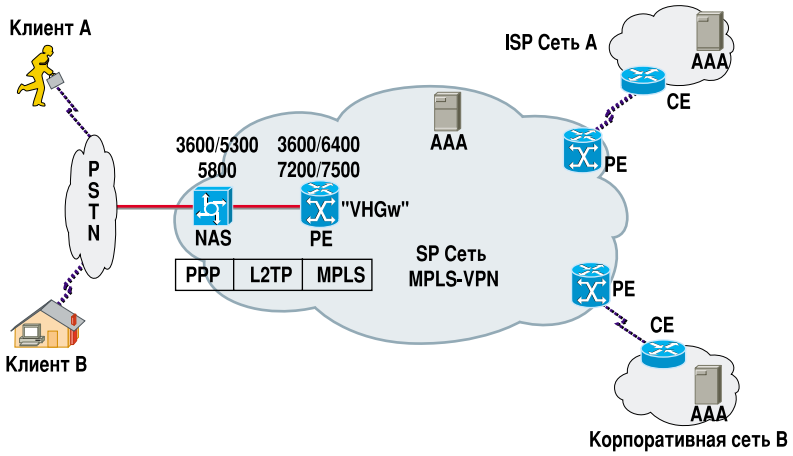
технологий. Кроме этого, мы обсудим протоколы маршрутизации PE-CE, которые используются в сетях MPLS-VPN.

4.1. Коммутируемый доступ (по аналоговым каналам или каналам ISDN)

С помощью протокола PPP клиентские устройства могут подключаться к провайдерской точке присутствия POP и связываться с сетями MPLS-VPN. Этот процесс является полностью прозрачным для клиента PPP, который может пользоваться любым устройством доступа (например, персональным компьютером с модемом или домашним маршрутизатором ISDN).

Этот процесс начинается, когда клиент PPP связыва-

Рисунок 30. Удаленный доступ к MPLS L2TP



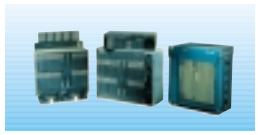
ется с узлом доступа (NAS) сервис-провайдера. Терминация этого вызова происходит в обычном порядке. Используя имя домена, обнаруженное в ходе аутентификации PPP, или набранный номер (DNIS), предоставленный коммутатором ТфОП, маршрутизатор NAS создает туннель с помощью протокола туннелирования 2-го Уровня (Layer 2 Tunneling Protocol — L2TP). После создания туннеля сессия PPP передается PE-маршрутизатору.

После терминации сессии PPP на PE-маршрутизаторе она привязывается к интерфейсу, который ассоциируется с конкретной сетью VPN. Интерфейсы группируются в отдельные сети VPN на основании имени домена или номера DNIS. Входящая сессия PPP докладывает имя домена или номер DNIS PE-маршрутизатору и привязывается к соответствующему интерфейсу. В ходе сессии, как обычно, используется средство аутентификации и учета RADIUS. После этого сессия PPP полностью принадлежит данной сети VPN и может направлять пакеты к месту назначения. При этом может использоваться любой узел доступа, поддерживающий L2TP.

4.2. DSL

Цифровые абонентские линии (DSL) поддерживают широкую полосу пропускания на существующих витых медных парах, проложенных по всему миру. Надомные работники, малые предприятия и отделения крупных корпораций могут пользоваться технологией DSL для удаленного доступа и выделенного доступа к сетям VPN.

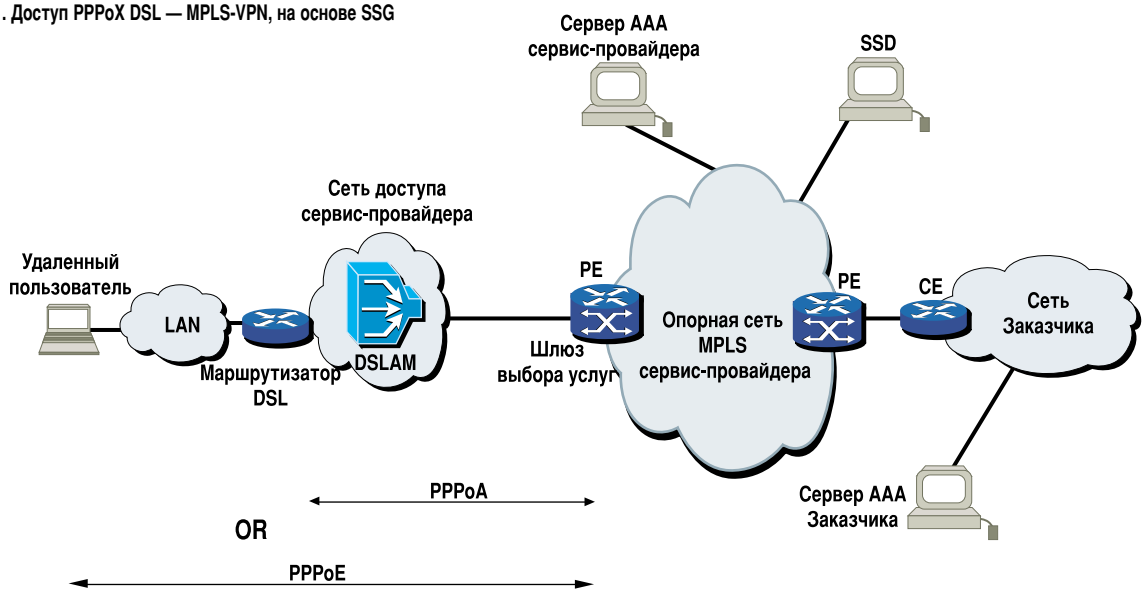
В среде DSL оборудование, установленное у заказчика (CPE), работает и как мост, и как маршрутизатор. Кроме того, оно может поддерживать PPP поверх Ethernet или PPP поверх ATM. Устройство Cisco 6400 выполняет функции концентратора доступа и PE-маршрутизатора. Опорная сеть MPLS полностью прозрачна для CPE. Маршрутизируемый или «мостовой» (bridged) трафик на CPE может статически конфигурироваться на устройстве Cisco 6400 и направляться согласно MPLS RD. Функции статической конфигурации выполняют идентификаторы VCI/VPI. Входящие идентификаторы статически привязаны к MPLS RD.



Провайдеры могут также поддержать выбор услуг через клиента PPP или через web-браузер и информационную панель (dashboard). Если используется клиент PPP, пользователь вводит в соответствующее поле имя (username). UAC анализирует имя услуги, просматривает ее определение в локально или удаленно хранящемся профиле, где имеется идентификатор MPLS-VPN, и выдает инструкции по аутентификации. После аутентификации пользователя Cisco 6400 UAC динамически связывает абонента с нужной сетью VPN.

В случае с web-браузером для выбора услуг используется программный образ, имеющийся на устройстве Cisco 6400 UAC, и сервер информационной панели (web dashboard server). Когда пользователь с помощью браузера получает доступ к адресу URL информационной панели, на его экран выводится меню услуг. Эти услуги могут быть связаны с разными сетями MPLS-VPN. Когда пользователь щелкает мышкой по кнопке информационной панели, на экране может появиться подсказка, требую-

Рисунок 31. Доступ PPPoX DSL — MPLS-VPN, на основе SSG

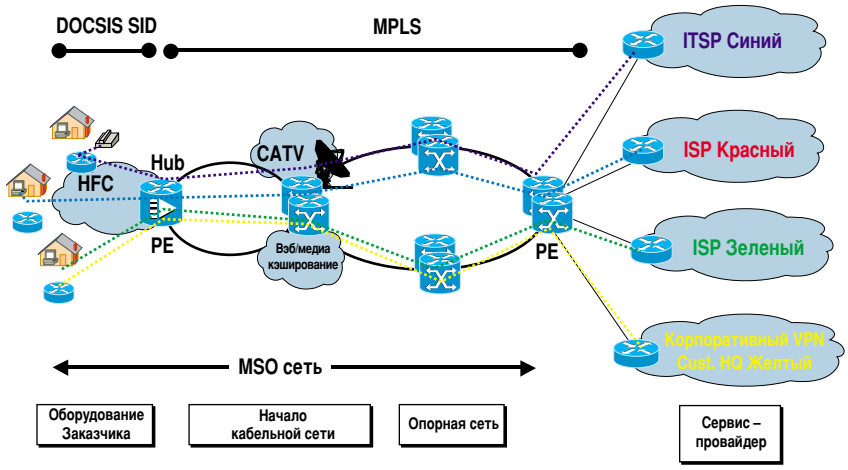


щая аутентификации. После успешной аутентификации пользователь динамически связывается с соответствующей сетью MPLS-VPN.

4.3. Кабельные модемы

Кабельные модемы предоставляют широкополосный доступ по существующим гибридным оптическим/коаксиальным сетям (HFC), которые используются для кабельного телевидения. В этом случае uBR7200 выступает в роли PE-маршрутизатора.

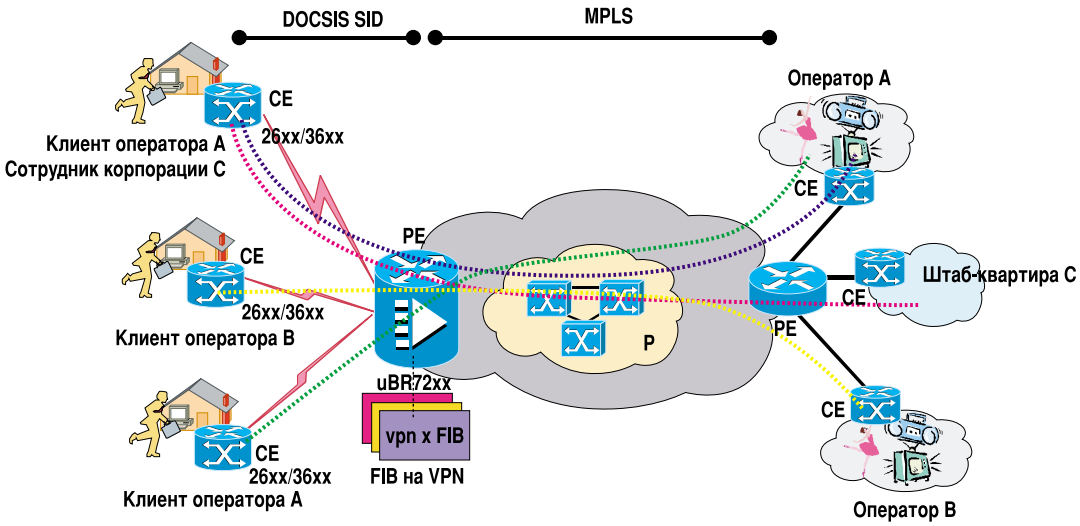
Рисунок 32. MPLS-VPN в сетях кабельного телевидения



4.4. Широкополосный фиксированный беспроводной доступ (BBFW)

На рисунке 33 показана топология решения с интеграцией BBFW в сеть MPLS-VPN. Главный маршрутизатор (Cisco uBR72xx/VXR с беспроводным модулем) действует как PE-маршрутизатор в магистрали MPLS-VPN. Беспроводной абонентский блок (CPE, маршрутизатор Cisco 26xx/36xx с модулем BBFW), установленный в клиентской сети, выступает в качестве CE-маршрутизтора, подключенного к PE. Трафик с клиентских ПК, поступающий из клиентской сети, которая находится за абонентским блоком, будет передаваться в сети VPN с уче-

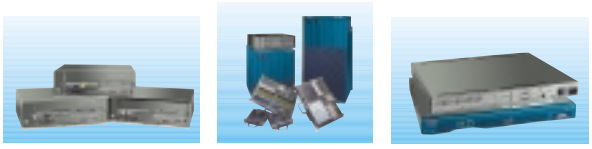
Рисунок 33. Интеграция DOCSIS SID => MPLS-VPN



том идентификаторов услуг (Service Identifiers — SID), находящихся в соответствующих фреймах DOCSIS. Каждый CPE может поддерживать множество идентификаторов SID.

4.5. Frame Relay/ATM

Технологии Frame Relay и ATM широко распространены и хорошо известны. Они поддерживают надежную защиту каналов связи с классификацией и приоритизацией трафика на Уровне 2. В качестве PE-маршрутизаторов в сетях Frame Relay и ATM используются стандартные периферийные устройства Cisco,



например, маршрутизаторы серий Cisco 7200 и Cisco 7500. В небольших офисах в качестве PE-маршрутизатора хорошо работают маршрутизаторы серии Cisco 3600.

4.6. Поддержка классов обслуживания и качества услуг CoS/QoS на устройствах PE

На рисунке 34 показана поддержка CoS/QoS на PE-маршрутизаторе с помощью описанных выше механизмов CoS.

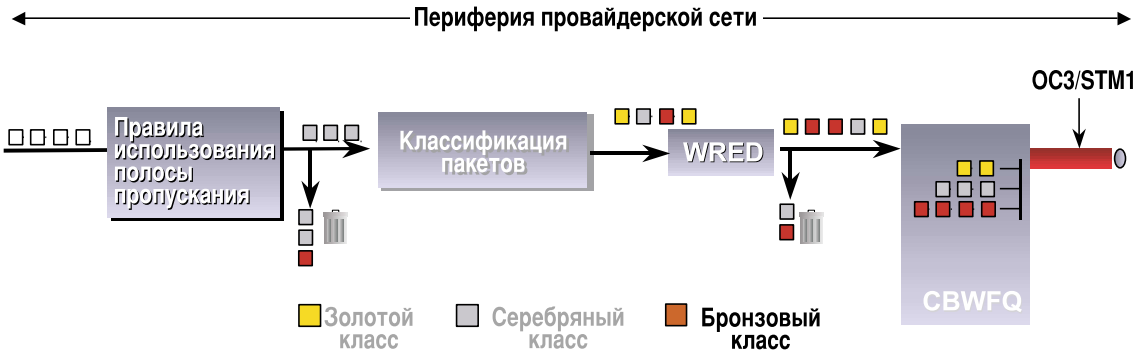
Обычная процедура поддержки CoS на PE-маршрутизаторе включает следующие шаги:

- на входе PE к трафику заказчика применяются правила, связанные с полосой пропускания;
- в зависимости от условий контракта, подписанного с заказчиком, выполняются некоторые действия, такие как отбрасывание пакетов или установка определенного значения в битах приоритетности;
- каждый интерфейс PE может поддерживать разные скорости передачи для разных типов трафика в зависимости от установленной классификации (трафик заказчиков может подразделяться на разные классы обслуживания: Золотой, Серебряный, Бронзовый и т.д.);
- после классификации пакета он передается для постановки в очередь;
- применяется метод WRED для борьбы с переполнением;
- если пакет успешно проходит фильтры WRED, он помещается в очередь соответствующего класса.

4.7. Маршрутизация от границы сети заказчика до границы сети провайдера (CE — PE)

Если устройство CE является маршрутизатором, то

Рисунок 34. Поддержка CoS/QoS на PE-маршрутизаторах серии 7500/7200



для передачи трафика между CE и PE необходим только протокол маршрутизации. В ситуациях, когда пограничным устройством заказчика является концентратор или коммутатор, устройство PE должно напрямую взаимодействовать с сетью заказчика.

Каждый CE-интерфейс на устройстве PE имеет свою таблицу маршрутизации и передачи VPN (VPN Routing and Forwarding table — VRF), в которой содержится информация о маршрутах данного сайта. Чтобы заполнить таблицу PE данными о маршрутах заказчика, необходим протокол маршутизации PE/CE.

В сети MPLS между областями CE и PE могут использоваться следующие протоколы маршрутизации:

- статический;
- RIPv2;
- eBGP;
- OSPF.

Все перечисленные протоколы модифицированы для поддержки таблиц VRF. Для этого используется новая функция, которая называется address families (семейства адресов). Семейства адресов определяют контексты таблиц VRF, с которыми работает протокол маршрутизации.

Заметим, что протокол маршрутизации, действующий между PE и CE, не зависит от протокола IGP, действующего в сети заказчика. Маршруты, которые обнаруживает IGP заказчика, передаются в протокол маршрутизации PE/CE и вводятся в таблицу VRF. Поэтому заказчик может пользоваться протоколом EIGRP в своей частной глобальной сети (WAN) и переходить к протоколу RIPv2 в области PE/CE, чтобы заполнить таблицу VRF.

Важно понять, что на периферии сети заказчика (Customer Edge) нет необходимости в каких-либо специальных конфигурациях MPLS. Требуются только стандартные команды маршрутизации IOS. Периферия сети заказчика ничего не знает о сети MPLS, к которой она подключена. Ей необходима только конфигурация соответствующего протокола PE/CE и (при необходимости) команды, перенаправляющие трафик на IGP заказчика.

Статическая маршрутизация

Статическая маршрутизация предназначена для малых предприятий и отдельных сайтов (stub site), где адресация IP-устройств вряд ли будет меняться. Сюда входят все заказчики, подключенные к сети через концентратор или коммутатор. CE-маршрутизатор будет иметь маршрут по умолчанию, указывающий на сеть MPLS. PE-маршрутизатор также должен иметь аналогичный статический маршрут в соответствующей таблице VRF, связанной с подинтерфейсом заказчика.

В случае, когда устройство PE напрямую подключено к концентратору или коммутатору заказчика, поддержка статического маршрута будет необязательна, поскольку маршрут будет определяться по IP-адресу на интерфейсе PE LAN. Однако если заказчик имеет маршруты, скрытые за локальной сетью (LAN), то статический маршрут все же нужно вводить в таблицу PE VRF.

Маршрутизация RIPv2

Протокол RIPv2 рекомендуется для сайтов заказчика, где топология маршрутизации может изменяться. В этом случае все изменения топологии будут автоматически включаться в таблицу MPLS VRF. Кроме того, RIPv2 поддерживает CIDR маски подсетей переменной длины, что позволяет лучше использовать доступное пространство IP-адресов (протокол RIPv1 не имеет таких возможностей).

RIPv2 — это дистанционно-векторный протокол маршрутизации, поэтому под управлением RIPv2 конвергенция будет происходить медленнее, чем в случае использования протоколов, использующих состояние канала (link state), таких как OSPF.

4.8. Магистральные протоколы маршрутизации

Для связи PE-PE и P-P требуются иные протоколы маршрутизации, поскольку здесь к маршрутизации применяются иные требования.

Для связи P-P рекомендуется протокол IS-IS или OSPF. Для связи PE-PE рекомендуется протокол MP-BGP.

Протоколы IS-IS и OSPF в магистрали

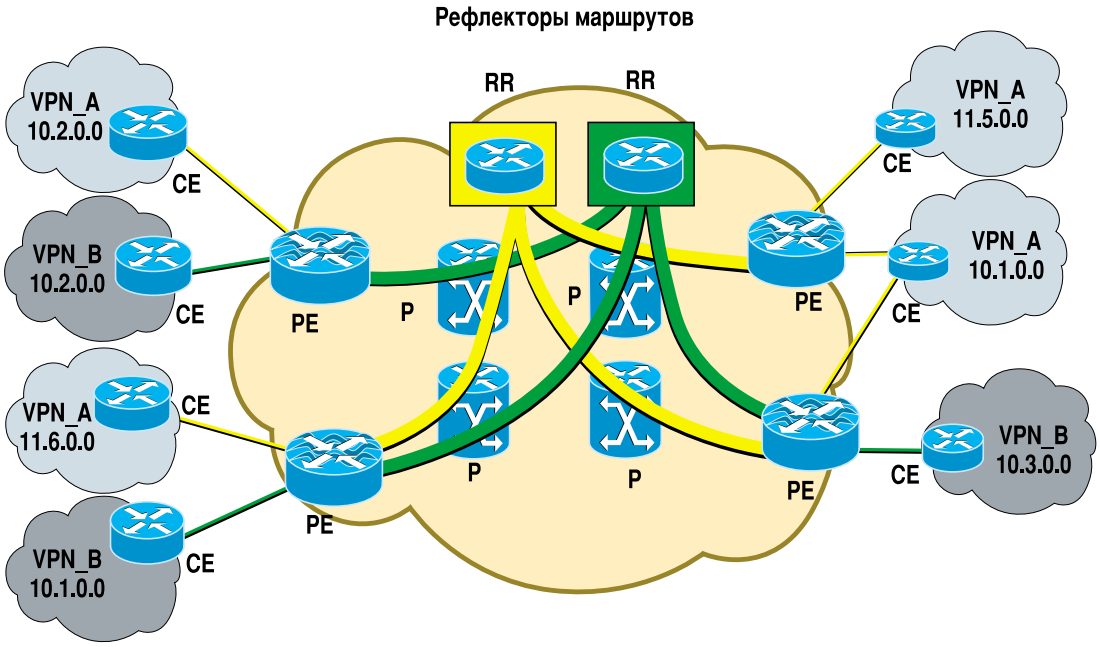
Протоколы IS-IS/OSPF действуют как IGP, обеспечивая IP-связь для всех устройств LSR (P и PE). Этот протокол маршрутизации должен действовать до распределения данных о маршрутах LDP и VPN (BGP4).

Рекомендуется использовать IS-IS или OSPF в качестве IGP для глобальной таблицы маршрутизации между магистральными маршрутизаторами. Протоколы IS-IS и OSPF работают на основе учета состояния каналов (link state) и могут поддерживать RRR. Дистанционно-векторные протоколы, такие как EIRGP, не могут поддерживать RRR.

Глобальная таблица маршрутизации

Глобальная таблица маршрутизации (global routing table — GRT) имеется на всех P-маршрутизаторах и PE-маршрутизаторах. В ней содержатся данные обо всех

Рисунок 35. Рефлекторы маршрутов BGP



маршрутах, которые не принадлежат к VPN. Сюда включаются loopback адреса и адреса каналов. Таблица GRT содержит информацию, которая позволяет маршрутизировать трафик в сети P/PE.

Маршруты заказчиков хранятся в таблицах VRF. Обычно маршруты глобальной таблицы недоступны для маршрутов из таблиц VRF, если их специально не сконфигурирует для этого сервис-провайдер с помощью команды «global».

MP-BGP4 (многопротокольный BGP)

Для распространения информации о маршрутах VPN используется протокол BGP. В сети MPLS каждая сеть VPN, определенная сервис-провайдером, состоит из таблиц VRF, связанных с интерфейсами заказчиков. Поскольку в таблицах VRF используются не адреса IPv4, а адреса VPN-IPv4, BGP поддерживает многопротокольные расширения, позволяющие распространять данные об этих маршрутах VPN-IPv4.

Эти расширения используются для передачи информации только между PE-маршрутизаторами. Информация для данной VPN передается только членам этой VPN. Многопротокольные расширения BGP определяют законных получателей маршрутизационной информации VPN. Все члены данной VPN получают маршруты других членов этой сети.

Рефлекторы маршрутов BGP (BGP Route Reflectors)

Рефлекторы маршрутов BGP не имеют критически важного значения для функционирования сети MPLS, однако они позволяют значительно повысить ее эффективность.

Если рефлекторы маршрутов отсутствуют, то в случае подключения нового устройства PE каждое устройство PE в сети сервис-провайдера должно получить дополнительную команду (BGP neighbor command), указывающую на новое устройство. BGP требует, чтобы обновления, принятые одноранговым устройством в зоне того же сервера доступа (AS), не передавались дальше в той же зоне. Поэтому сеть BGP должна иметь полностью уз-

ловую структуру (fully meshed), в которой одноранговые устройства должны рассматриваться как соседи, между которыми передаются обновления маршрутов BGP.

Если количество устройств PE слишком сильно возрастает, что делает непрактичной процедуру добавления команды каждому PE, необходимо использовать рефлекторы маршрутов BGP. Рефлекторы маршрутов сокращают необходимость связи каждого одноранговой устройства BGP со всеми остальными и позволяют не добавлять новые команды каждому устройству PE.

В сети, где используются рефлекторы маршрутов, устройствам PE нужны только те соседи, которые определены для каждого рефлектора. Все обновления, включая информацию для таблиц VRF, будут передаваться только рефлекторам маршрутов. В свою очередь, рефлекторы распространяют информацию, полученную от PE, всем другим устройствам PE.

4.9. Оборудование заказчика (Customer Equipment — CE)

Оборудование, которое использует заказчик в сетях non-MPLS-VPN, сохраняется и для сетей MPLS-VPN. Это оборудование не распознает технологию MPLS-VPN. Заказчик пользуется им для подключения к сетям интранет/экстранет/Интернет и выбирает оборудование в зависимости от требуемой скорости передачи и объема трафика.

5. VPN Solutions Center (центр решения VPN)

Эксплуатация, учет, обслуживание, поддержка и управление (Operations, Accounting, Maintentance, Provisioning and Management — OAM&P) играют важную роль в решении MPLS-VPN. Для поддержки этих функций Cisco предлагает сервис-провайдеру центр решения VPN (VPN Solutions Center — VPNSC). Этот центр дает сервис-провайдеру следующие преимущества: сокращение сроков внедрения услуг VPN, гладкое и безошибочное внедрение и сокращение оперативных расходов, связанных с оказанием услуг VPN в сети MPLS. Центр позволяет управлять всеми услугами IP VPN на всем протяжении их жизненного цикла, включая техническое обеспечение и активацию услуг, аудит, поддержку соглашений о гарантированном качестве обслуживания (SLA) и мониторинг объемов трафика.

5.1. Описание услуги

Cisco VPN Solutions Center представляет собой решение для сети MPLS и соглашений SLA, позволяющее сервис-провайдеру эффективно внедрять услуги MPLS-VPN и управлять ими.

Cisco VPN Solutions Center включает полный интегрированный набор функций управления услугами MPLS-VPN на всем протяжении их жизненного цикла. Возможности этого центра включают техническое обеспечение и активацию услуг, аудит услуг, мониторинг соглашений о гарантированном качестве обслуживания (SLA), а также сбор данных о пользовании и составление отчетов. Cisco VPN Solutions Center поддерживает богатый набор интерфейсов прикладного программирования (API). Он изначально приспособлен для работы с большинством модулей управления услугами Cisco (Cisco Service Management — CSM). Сервис-провайдер, приобретающий другие приложения CSM, увеличивает ценность Cisco VPN Solutions Center и дает модулям CSM возможность работать с сетями VPN. Решения с добавленной ценностью, такие как Cisco Provisioning Center и Cisco Info Center, расширяют возможности работы Cisco VPN Solutions Center в разнородой среде, состоящей из оборудования множества производителей. Cisco VPN Solutions Center можно использовать в автономном режиме (standalone) для того, чтобы помочь сервис-провайдерам сократить сроки внедрения новых услуг, обеспечить безошибочное внедрение и сократить оперативные расходы, связанные с оказанием услуг VPN.

5.2. Основные характеристики решения

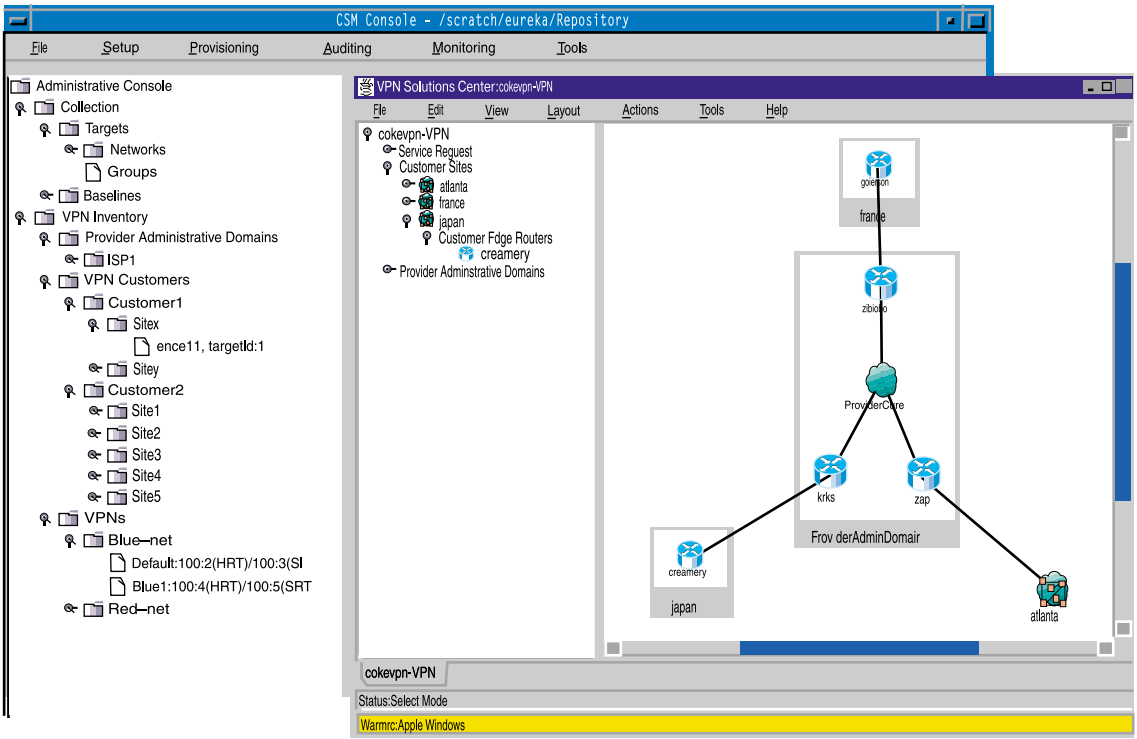
- Поддержка подсистем, необходимых для оказания услуг MPLS-VPN.
- Поддержка параметров QoS для эффективного внедрения правил и дифференцированных классов обслуживания.
- Ввод запросов на оказание услуг с помощью шаблонов (wizards), что упрощает работу операторов.
- Планировщик (scheduler) для технического обеспечения с учетом времени.
- Полный просмотр топологий VPN (hub-and-spoke и full-mesh).
- Аудит конфигурации услуг IP-VPN и обеспечение целостности сети.
- Подсистема учета для сбора данных о пользовании и составления отчетов, включающих особенности VPN и классов обслуживания.
- Подсистема соглашений о гарантированном качестве обслуживания (SLA) для мониторинга соглашеий SLA с учетом требований VPN.
- Открытые интерфейсы API для технического обеспечения, учета и поддержки производительности, позволяющие применять приложения третьих сторон и интегрировать системы OSS (Operations Support Systems).

- Поддержка маршрутизаторов, коммутаторов и гигабитных коммутирующих маршрутизаторов (GSR) Cisco.
- Поддержка операционной системы Cisco IOS и ее богатой функциональности.

5.3. Основные преимущества

- Простота настройки и управления сетями VPN и участниками сетей VPN с помощью интерактивных шаблонов (wizards).
- Уверенное внедрение VPN с тестированием до и после активации.
- Поддержка web-доступа к данным о производительности в режиме, приближенном к реальному времени.
- Сокращение количества ошибок в процессе настройки и проверка данных на непротиворечивость.
- Унифицированный контроль, отслеживание и управление в течение всего жизненного цикла услуги.
- Сокращение общей стоимости эксплуатации и управления.
- Быстрая доставка услуг VPN и повышение конкурентоспособности провайдера.
- Создание дифференцированных услуг VPN за счет поддержки QoS.

Рисунок 36. Директория VPN



5.4. Основные функции

Техническое обеспечение (Provisioning). Cisco VPN Solutions Center позволяет постепенно, шаг за шагом заполнять предоставляемые шаблоны. Операторы могут добавлять, удалять и модифицировать сети VPN заказчиков. Кроме того, они могут легко устанавливать отношения экстранет. В этом случае шаблоны превращаются в соответствующие команды Cisco IOS, которые затем по определенному графику загружаются в сеть.

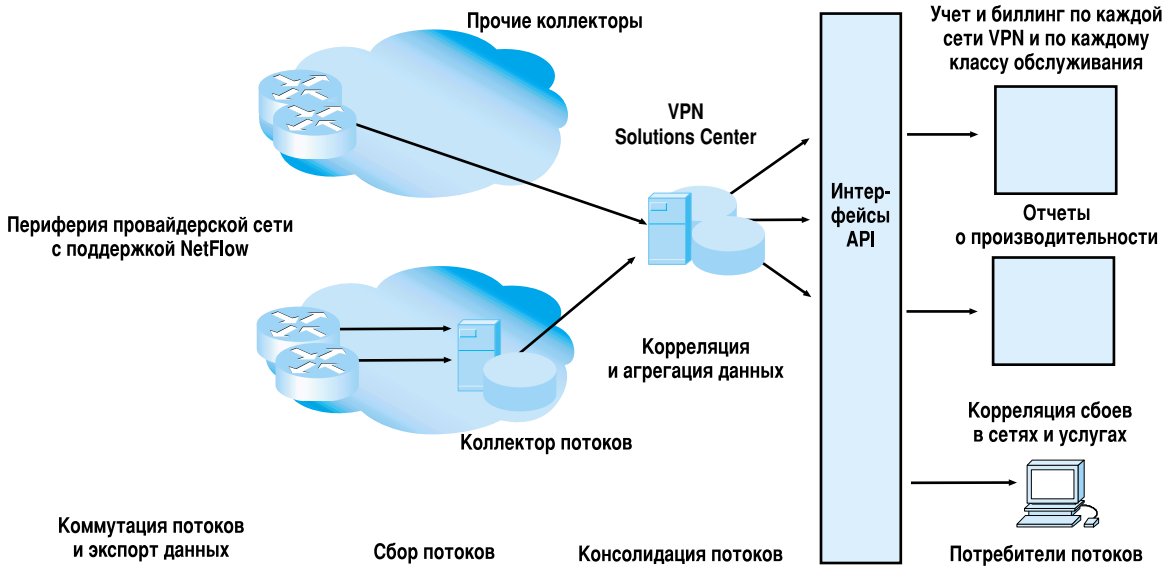
Планировка (Scheduling). При внедрении новой или изменении старой услуги пользователи могут распланировать время активации услуги, позволяя сервис-провайдеру получить нужные аппаратные средства или предприять другие меры, необходимые для активации.

Активация (Activation). Изменения услуг активизируются в сети с помощью надежной доставки соответствующим сетевым элементам команд Cisco IOS. Сетевые элементы тестируются, чтобы обеспечить успешную доставку команд.

Пост-активационное тестирование (Post-activation testing). После активации услуг эти услуги тестируются, чтобы обеспечить их успешное функционирование. Так, например, тестирование связи между сайтами по методу «запрос — ответ» (site-to-site ping test) обеспечивает корректную активацию нового сайта для существующей услуги VPN.

Аудит услуг (Service auditing). VPN Solutions Center может генерировать отчеты о состоянии запросов на предоставление услуг (запрос может быть отложенным «pending» или удовлетворенным «deployed»). В запланированный момент эта функция считывает текущие конфигурационные файлы маршрутизаторов, анализирует историю запросов на предоставление услуг и генерирует отчет о текущем состоянии системы.

Рисунок 37: Архитектура сбора данных



Отчеты о пользовании (Usage). С помощью технологии Cisco NetFlow, VPN Solutions Center генерирует отчеты о производительности каждой сети VPN интранет и экстранет. NetFlow записывает множество статистических данных, включая информацию по каждому порту приложений и IP-адресу заказчика. Информация, которая содержится в этих отчетах, помогает заказчикам оценивать потребление своих внутренних ресурсов.

Мониторинг соглашений SLA и составление отчетов по ним. VPN Solutions Center осуществляет мониторинг таикх параметров соглашений SLA, как общее время передачи (round-trip time), доступность и использование агентов в существующих маршрутизаторах Cisco. Здесь можно устанавливать пороговые значения и отслеживать их нарушение.

Техническое обеспечение и измерение параметров QoS. VPN Solutions Center поддерживает QoS и дает возможность сервис-провайдеру предлагать заказчикам

разные классы обслуживания. VPN Solutions Center генерирует конфигурацию маршрутизатора, распределяет полосу пропускания по разным классам обслуживания и следит за соблюдением условий SLA с помощью агента (Response Time Reporter — RTR), который входит в состав Cisco IOS™.

5.5. Архитектура

VPN Solutions Center поддерживает открытые интерфейсы API и интегрируется в большинство модулей CSM. Кроме того, интерфейсы API могут использоваться другими приложениями, например, приложениями для биллинга (Belle Systems IMS), мониторинга сбоев (Cisco Info Center) и отчетности (Concord eHealth). К примеру, Info Center может использовать эти интерфейсы для того, чтобы определить, какие услуги пострадали в результате того или иного сетевого сбоя. Эта задача выполняется с помощью запроса, направляемого в хранилище данных VPN Solutions Center с использованием открытых интерфейсов API.

5.6. Интеграция приложений

5.6.1. Управление сбоями (Fault Management)

Функция управления сбоями VPN Solutions Center поддерживается интеграционным модулем Cisco Info Center (CIC). Интеграционный модуль CIC поддерживает управление сбоями в VPN с помощью корреляции системных ловушек с информационной моделью VPN в репозитории VPN Solutions Center.

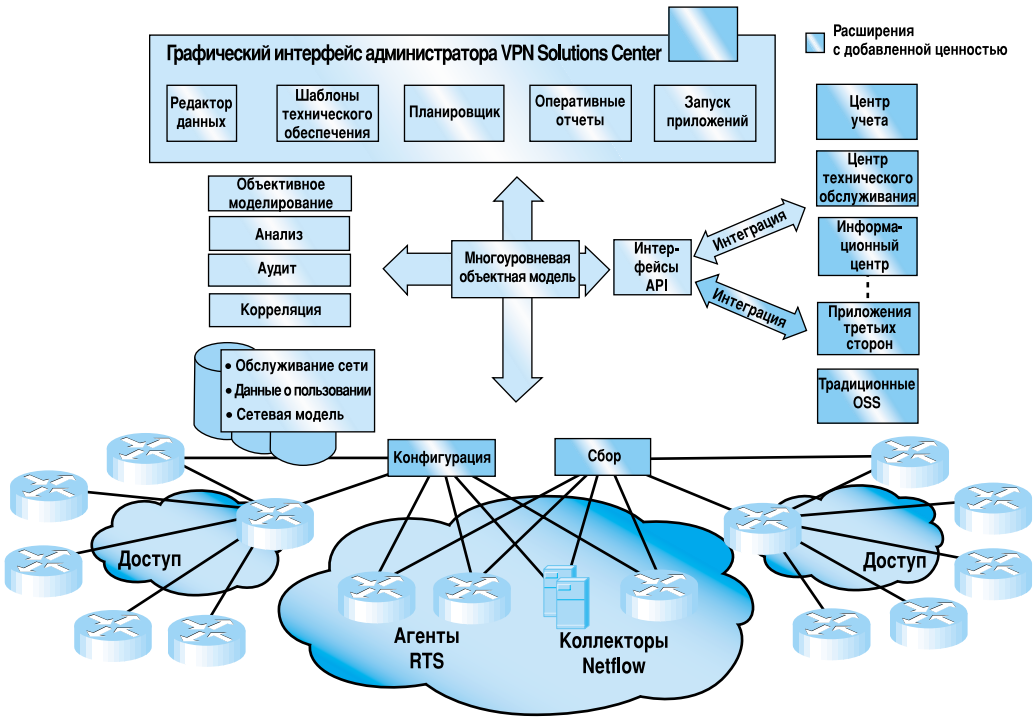
5.6.2. Управление производительностью

VPN Solutions Center позволяет создавать и отслеживать метрику производительности, которая необходима для оценки доступности услуг, среднего времени наработки на отказ, времени реагирования, колебаний задержки, потери пакетов и т.д. Кроме сбора данных о производительности, VPN Solutions Center коррелирует эти данные с классом обслуживания в каждой сети VPN. Для более продвинутых оценок тенденций, услуг и общего «состояния здоровья сети» VPN Solutions Center интегрируется с пакетом приложений Concord eHealth.

5.6.3. Управление учетом

VPN Solutions Center поддерживает интерфейс CORBA API для сбора данных о пользовании услугами VPN с помощью коллекторов Netflow. Модули интеграции биллинга Portal and Belle System IMS для VPN Solutions Center используют данные, полученные с помощью этого интерфейса для предоставления заказчикам детальной информации о биллинге.

Рисунок 38: Архитектура VPN Solutions Center



Приложение А. Терминология MPLS

Border Router (пограничный маршрутизатор)	Поддерживает связь с сетью другого провайдера. С помощью IBGP пограничный маршрутизатор PE связывается с одногранговыми устройствами PE и с одноранговым устройством EBGP для подключения к Интернет-маршрутизатору общего доступа.
CEF	Cisco Express Forwarding — технология коммутации на 3-м Уровне. Для поддержки сетей MPLS-VPN необходимо использовать CEF.
CE-маршрутизатор	Периферийный маршрутизатор сети заказчика. Часть сети заказчика. Связан с периферийным маршрутизатором сети провайдера (PE-маршрутизатором) и является для него одноранговым устройством.
Customer Network (C-Network)	Сеть заказчика.
Customer Premise Equipment (CPE)	Оборудование, которое принадлежит заказчику и контролируется им.
Edge LSR	Периферийное устройство, на котором присваивается первая метка. Устройство LSR, имеющее соседей, не относящихся к сети MPLS, считается устройством Edge LSR.
Global Routing Table (глобальная таблица маршрутизации)	Стандартная таблица IP-маршрутизации Cisco IOS. Для доступа к глобальной таблице маршрутизации используется команда «show ip route».
Label (метка)	Заголовок, используемый коммутирующим маршрутизатором LSR для передачи пакетов. В сети MPLS метки имеют локальное значение и используются только для передачи пакетов.
Label Switching (коммутация по меткам)	Использование для коммутации меток (labels или tags). Для передачи пакета следующему устройству устройство MPLS использует входящую метку (incoming label) и исходящую метку (outgoing label).
Протокол LDP	Протокол распределения меток (Label Distribution Protocol), определенный стандартом *draft-ietf-mpls-ldp-05*.
Label switched path (LSP) (маршрут для коммутации по меткам)	Маршрут, определенный всеми метками, присвоенными устройствами на всем протяжении канала связи. Маршрут LSP может быть статическим или динамическим.
LSR: Label Switch Router (коммутирующий маршрутизатор для коммутации по меткам)	Маршрутизатор, который выполняет процедуры распределения меток и передает пакеты по меткам.
MPLS	Многопротокольная коммутация по меткам (Multi-Protocol Label Switching).
NLRI	Информация о доступности сетевого уровня (Network Layer Reachability Information). В этом поле находится префикс адреса VPN-IPv4 с меткой. Формат поля: <label, length, prefix> (метка, длина, префикс).
P-маршрутизатор	Маршрутизатор провайдера, т.е. магистральный маршрутизатор MPLS-VPN. P-маршрутизатор выполняет задачи коммутации по меткам и является одноранговым для других P-маршрутизаторов. Кроме того, P-маршрутизатор может напрямую подключаться к PE-маршрутизатору. P-маршрутизаторы также называются устройствами LSR.

PE-маршрутизатор	Периферийный маршрутизатор провайдера. Часть провайдерской сети. Связывается с CE-маршрутизатором и является для него одноранговым. PE-маршрутизаторы преобразуют адреса Ipv4 в 12-байтовые адреса VPN-Ipv4. PE-маршрутизаторы также называются Edge LSR.
Provider Network (P-Network) (сеть провайдера)	Сеть сервис-провайдера, состоящая из P-маршрутизаторов.
Route Distinguisher (RD) (распознаватель маршрутов)	Атрибут каждого маршрута, используемый для уникальной идентификации префиксов в сетях VPN (64 бита). Во избежание конфликтов между RD каждый сервис-провайдер управляет своим собственным «номерным пространством».
VPN (Vitural Private Network)	Виртуальная частная сеть. Сеть заказчика. Состоит из множества сайтов и опирается на физическую инфраструктуру совместного пользования (т.е. сеть сервис-провайдера), но имеет свои правила и работает как частная сеть.
VPN Aware Network	Магистраль провайдера, поддерживающая технологию MPLS-VPN.
Адреса VPN-IPV4	12-байтовые IP-адреса. Первые 8 байт — это «различитель маршрутов» (RD), а последние 4 байта — это IP-адрес.
VRF (VPN Routing & Forwarding)	Таблица маршрутизации и передачи, связанная с одним или несколькими подключенными сайтами. Инстанция VRF состоит из таблицы IP-маршрутизации, производной таблицы передачи, набора интерфейсов, которые используют таблицу маршрутизации, и набора правил и протоколов маршрутизации, которые определяют, какую информацию поместить в таблицу передачи. С одним (под)интерфейсом может быть связана только одна таблица VRF.
VRF ForwardingTable (таблица передачи VRF)	Содержит маршруты, которые могут использоваться в определенной группе сайтов. Использует технологию CEF. Для поддержки VPN необходимо внедрить и активизировать CEF.
VRF Routing Table (таблица маршрутизации VRF)	Таблица, в которой содержатся маршруты, которые должны быть доступны определенной группе сайтов. Аналогична стандартным таблицам IP-маршрутизации. Для просмотра таблицы VRF Routing Table используется команда «show ip route vrf *vrf_name*».

Составитель:
Михаил Захватов — CCIE,
системный инженер-консультант

Московский офис
Cisco Systems
113054 Москва, Россия
Риверсайд Тауэрз
Космодамианская наб., 52
Стр. 1, 4-й этаж
тел.: +7 (095) 961 14 10
факс: +7 (095) 961 14 69
World Wide Web: www.cisco.com
World Wide Web: www.cisco.ru

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the **Cisco Connection Online Web site at http://www.cisco.com.**
//www.cisco.ru.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxemburg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania •Russia • Saudi Arabia • Singapore • Slovakia • Slovenia •South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • United Kingdom • United States • Venezuela