А.Майданич
Alexander.Maydanich@rt.ru

ТЕХНИЧЕСКИЕ АСПЕКТЫ ВЗАИМОДЕЙСТВИЯ ОПЕРАТОРОВ СВЯЗИ ПРИ ПРЕДОСТАВЛЕНИИ УСЛУГ ПЕРЕДАЧИ ДАННЫХ

Компания ОАО "Ростелеком" является крупнейшим в нашей стране оператором, предоставляющим полный спектр услуг магистральной сети и объединяющим сети российских операторов в единую национальную сеть. Это также крупнейший поставщик телекоммуникационных услуг для государственных структур и ведомств, теле- и радиокомпаний, Интернет-провайдеров. В настоящей статье освещены вопросы развития сети "Ростелеком" на базе технологии IP/MPLS.

В 2006 году компания ОАО "Ростелеком" (далее "Ростелеком") начала строить федеральную сеть передачи данных на основе современных пакетных технологий. В 2007 г. сеть передачи данных IP/MPLS Ростелеком была принята в эксплуатацию. Сегодня протяженность сети составляет более 40 тыс. км. Она состоит из 10 опорных и свыше 100 региональных узлов и свыше 350 точек доступа на всей территории РФ.

РАЗВИТИЕ СЕТИ IP/MPLS РОСТЕЛЕКОМ

В сети использовано самое современное в России на сегодняшний день оборудование (к примеру, маршрутизаторы Juniper M320 производительностью до 320 Гбит/с). Пропускная способность сети в 2008 г. возросла до 20 Гбит/с. IP/MPLS Ростелеком – единственная сеть, получившая сертификат соответствия требованиям информационной безопасности ФСТЭК.

Сеть IP/MPLS Ростелеком является высокоскоростной сетью передачи данных на основе коммутации пакетов и функционирует поверх первичной транспортной сети, построенной на основе ВОЛС SDH и DWDM. Предназначена она для конвергенции услуг по передаче видео, речи и данных и призвана обеспечить возможность построения инфраструктуры интеллектуальных сетей следующего поколения. В настоящее время сеть передачи данных IP/MPLS Ростелеком присутствует на зарубежных точках обмена трафиком (Стокгольм, Франкфурт, Лондон, Амстердам, Гонконг), имеет сеть собственных региональных Дата-Центров в Москве, Екатеринбурге, Красноярске и Хабаровске, предоставляет услуги L2 VPN и VPLS (рис.1).

Сеть имеет динамическую маршрутизацию, поддерживает протоколы IPv4, IPv6, MPLS Fast Reroute и обеспечивает передачу в режиме реального времени различных типов трафика для мультимедиа, голоса, данных, видео, Интернет, с предоставлением услуг виртуальных частных сетей и различных классов обслуживания.

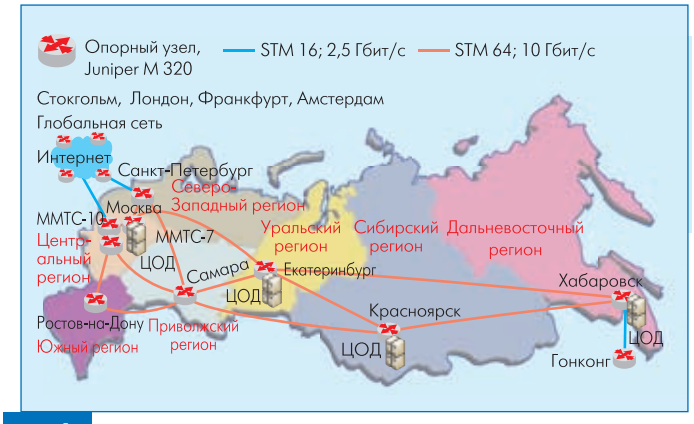

Рис. 1 Территориальное развитие сети IP/MPLS Ростелеком в 2008 г.

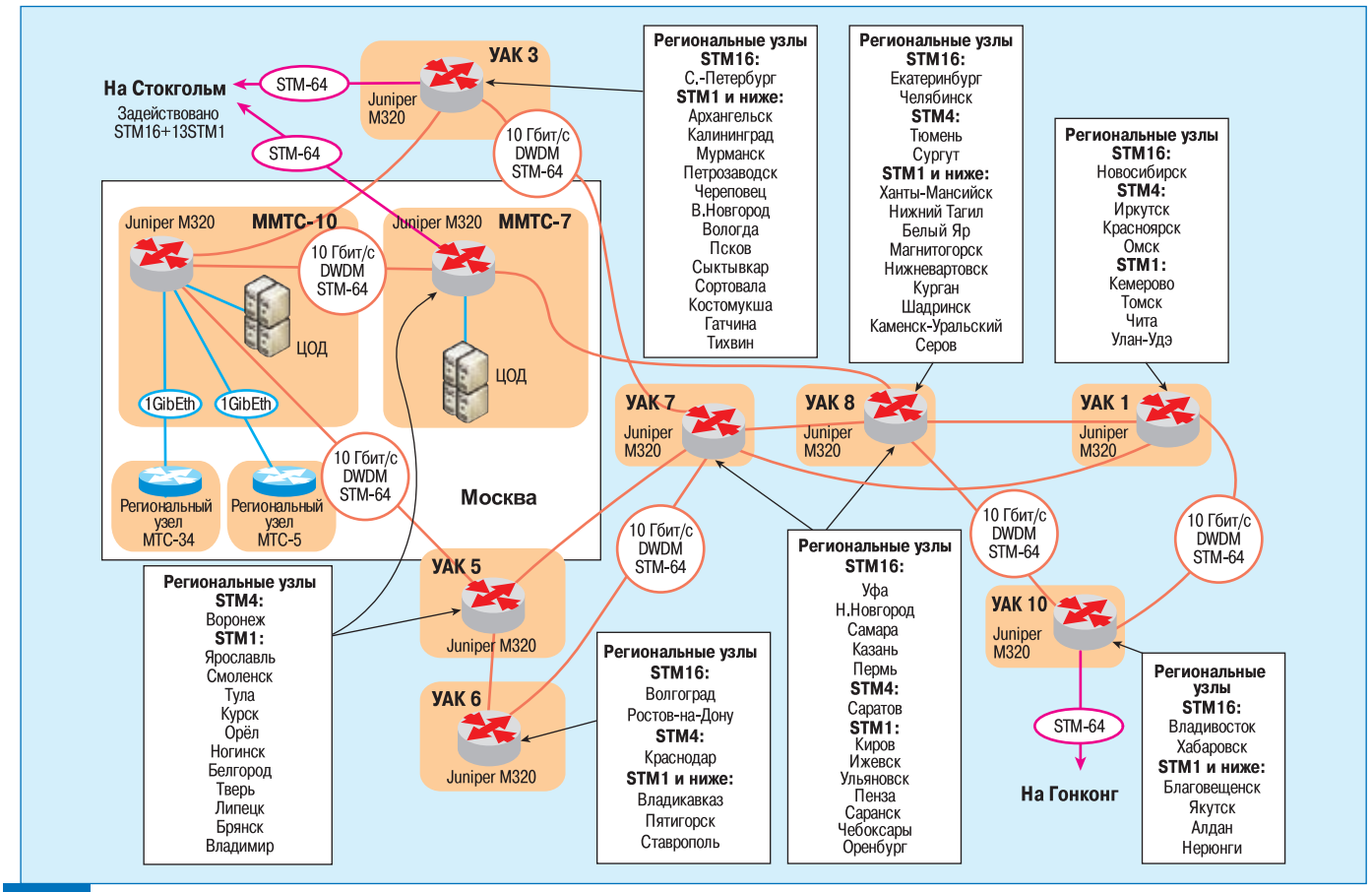

Рис.2 Схема сети передачи данных IP/MPLS Ростелеком на начало 2008 года

Вместе с тем, дальнейшее развитие услуг передачи данных на основе виртуальных частных сетей IP/MPLS для крупных корпоративных клиентов и государственных структур федерального уровня потребовало организации взаимодействия с сетями других операторов и выявило ряд проблем, без решения которых невозможно предоставлять услуги IP/MPLS VPN на географически протяженных территориях.

СХЕМА СЕТИ ПЕРЕДАЧИ ДАННЫХ IP/MPLS РОСТЕЛЕКОМ НА НАЧАЛО 2008 ГОДА

В соответствии с общей архитектурой сети, все ее сервисы (исключая доступ в Интернет) и клиентские подключения, а также подключение внутренних технологических сетей осуществляются в рамках какой-либо виртуальной частной сети. Такая схема позволяет обеспечить безопасность, изолированность и независимость по адресному пространству для сетей, принадлежащих разным клиентам (рис.2).

Пропускная способность сети составляет (по трафикам):

- Интернет – 1000 Тбайт в месяц,
- телефония (Voice over IP) – 700 млн. мин в месяц,
- данные VPN – 1000 Тбайт в месяц,
- потоковое видео – 200 телевизионных программ.

Надежность ядра сети соответствует уровню 99,999% (максимальное время простоя менее 5,2 мин в год). В сети обеспечено резервирование по электропитанию всего оборудования.

УСЛУГА INTERAS VPN

Развернутые в настоящее время операторами связи MPLS VPN-сети (Virtual Private Network) принадлежат к одной автономной системе (AS), а потребности Заказчика (например, транзит голосового трафика или подключение удаленных филиалов) требуют распространения виртуальной частной сети Заказчика через MPLS-сети нескольких операторов с пересечением ряда автономных систем.

В свою очередь, взаимное соединение MPLS-сетей представляет самостоятельный интерес и для операторов связи, так как позволяет получить дополнительные конкурентные преимущества – быстро расширить географическую зону покрытия сети и существенно увеличить клиентскую базу для оказания услуг. При этом соединение MPLS-сетей должно сохранять параметры надежности, безопасности и уровня обслуживания и обеспечивать полную прозрачность услуги VPN для Заказчика.

Сложности взаимного соединения VPN IP/MPLS-сетей разных операторов вызваны тремя основными причинами. Первая – распределение MPLS-меток между устройствами выполняется на основе внутренней таблицы маршрутов ав-

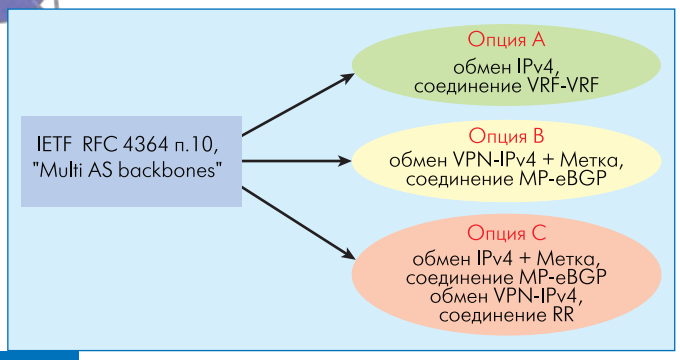

Рис.3 Методы взаимного соединения IP/MPLS VPN

тономной системы, в которой отсутствуют маршруты к узлам сети другого оператора. Таким образом, если выходной маршрутизатор VPN находится в другой AS, то путь MPLS к нему не может быть построен. Вторая – идентификаторы уникальности VPN, такие как "Разделитель маршрутов" (Route Distinguisher), "Назначение маршрутов" (Route Target) содержат в своей структуре номер автономной системы, что не позволяет непосредственно соединить части VPN в единое целое, так как параметры VPN будут отличаться друг от друга в разных AS у разных операторов. Третья – маркирование заголовков пакетов для разных классов обслуживания, в общем случае, будет разным у разных операторов связи и, как следствие, может привести к наихудшему обслуживанию трафика, маркированного Заказчиком как наиболее приоритетный.

Для решения этих проблем необходимо, во-первых, обеспечить передачу маршрутной информации и MPLS-меток узлов между автономными системами разных операторов. Соответствующие рекомендации закреплены в принятом IETF документе RFC 4364, п.10 "Multi-AS Backbones" и носят название опций A, B и C (рис.3). Во-вторых, надо определить в межоператорском соглашении сквозное правило кодирования идентификаторов VPN и классов качества обслуживания пакетов (QoS).

ОРГАНИЗАЦИЯ VPN MPLS В ПРЕДЕЛАХ ОДНОЙ AS

Виртуальные частные сети на основе MPLS (MPLS VPN) привлекают сегодня всеобщее внимание. Рассмотрим кратко организацию виртуальной частной сети по технологии MPLS в

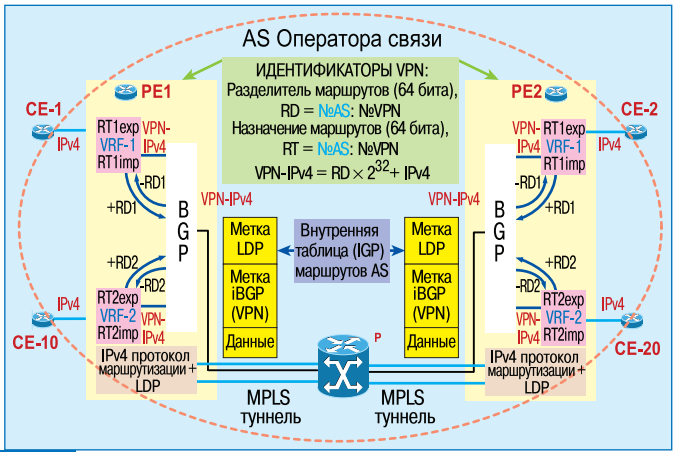

Рис.4 Организация VPN IP/MPLS в одной автономной системе

пределах одной автономной системы. Для формирования IP VPN необходимо (рис.4):

1. Соединить узлы автономной системы – внутренний протокол маршрутизации (OSPF, IS-IS) распространяет маршруты к внутренним узлам AS.

2. Назначить метки внутренним маршрутам узлов AS – протокол LDP осуществляет распределение меток.

3. Сформировать VPN-туннель – протокол граничного шлюза MP-BGP добавляет в пакет метку пункта назначения VPN перед отправкой его для транспортировки.

4. Обеспечить уникальность адресного пространства и маршрутов разных VPN – виртуальная маршрутная таблица VRF добавляет к IP-адресам множитель, называемый "Разделитель маршрутов" (Route Distinguisher), и формирует уникальные адреса VPN-IPv4, а маршрутам каждой VPN присваивает признаки "Назначение маршрутов" (Route Target) для отсылаемых и получаемых маршрутов.

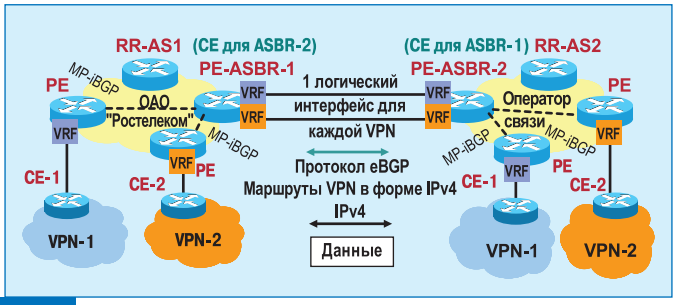

Рис.5 RFC 4364 опция A

Взаимодействие указанных компонентов в процессе создания VPN происходит следующим образом:

- Внутренний протокол маршрутизации сообщает об имеющихся маршрутах всем маршрутизаторам AS.
- Протокол распределения меток LDP обеспечивает связь между маршрутизаторами по технологии MPLS, назначая метки полученным маршрутам AS.
- Протокол граничного шлюза MP-BGP, опираясь на наличие связи между внутренними маршрутизаторами AS, устанавливает соединение между входным PE1 и выходным PE2 маршрутизаторами VPN.
- Виртуальная маршрутная таблица VRF на PE1 получает данные о маршрутах с оконечного оборудования CE1 Заказчика, назначает им метки, добавляет признаки RT-экспорта, посредством RD преобразует их в форму VPN-IPv4, и передает вместе с метками, используя MP-BGP, на выходной маршрутизатор PE2. По значению признака RT экспорта/импорта поступившие маршруты размещаются в VRF, соответствующую VPN Заказчика.

RFC 4364. ОПЦИЯ A

В случае использования опции A соединение VPN осуществляется через пограничные маршрутизаторы ASBR. ASBR-маршрутизатор является оконечным PE-маршрутизатором для VPN. Между собой соединяются выходные PE-маршрутизаторы участков VPN, размещенных в разных AS (back-to-back). Соеди-

нение осуществляется через интерфейсы маршрутизаторов (физические/логические), соответствующие VRF-таблицам продлеваемых VPN. Обмен данными осуществляется по протоколу IPv4 (CE – PE). Для передачи информации о маршрутах между участками VPN, размещенными в разных AS, используется протокол eBGP (внешний протокол граничного шлюза), предназначенный для связи различных AS между собой и обладающий необходимой гибкостью и надежностью. Таким образом, для каждой из AS подключение по опции A не отличается от обычного подключения Заказчика для услуги IP VPN (рис.5).

При соединении MPLS VPN по опции A выявились определенные сложности использования опции A:

- так как пограничный ASBR-маршрутизатор выполняет функции оконечного PE-маршрутизатора продлеваемых VPN, его ресурсы должны удовлетворять повышенным требованиям (на нем размещаются таблицы маршрутов IPv4, IP-VPNv4 всех продлеваемых VPN, векторы атрибутов BGP, блоки описания соединяемых интерфейсов),
- необходимо согласование параметров кодирования качества обслуживания сетей (уровней QoS) с взаимодействующим оператором,
- из-за множества соединенных интерфейсов сложно организовать резервирование,
- адреса IPv4, назначаемые соединяемым интерфейсам пограничных маршрутизаторов ASBR, относятся к адресному пространству Заказчика VPN и должны быть с ним согласованы,
- при организации VPN с использованием опции A необходимо выполнять двойную работу по настройке оборудования – на площадках Заказчика и в месте соединения MPLS VPN.

К особенностям соединений MPLS VPN по опции A можно отнести следующее:

- для предотвращения DoS-атак на ограниченные ресурсы маршрутизатора ASBR целесообразно использовать возможности протокола BGP по ограничению получаемых маршрутов,
- для проверки получаемых от партнера маршрутов необходимо использовать авторизацию MD5 в протоколе eBGP.

Вместе с тем, преимущества опции A вполне оправдывают ее применение:

- возможен полный контроль соединения и параметров проходящего трафика VPN,
- не требуется согласования параметров MPLS, организуемой VPN (Route Distinguisher, RouteTarget), с взаимодействующим оператором,
- возможно использование стандартного оборудования IPv4 для соединения VPN без поддержки технологии MPLS на сетевом уровне и увеличенного значения MTU на канальном уровне (для этого достаточно обеспечить для каждой из продлеваемых MPLS VPN логически независимое подключение по уровню 2 модели ISO/OSI, например, с использованием TDM таймслотов, VC контейнеров SDH, Ethernet VLAN.C),
- тарификация межоператорского трафика может быть выполнена с разбивкой по VPN с использованием Flow-технологий,
- минимально необходимое взаимодействие сетей операторов облегчает выполнение требований информационной безопасности,
- мониторинг стыка на сетевом уровне позволяет осуществить контроль функционирования сети и соглашений SLA.

Опция A рассматривается ОАО "Ростелеком" в настоящее время как основная при организации межоператорского продления VPN MPLS.

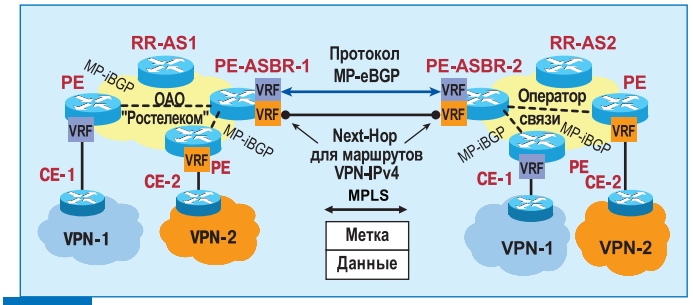

Рис.6 RFC 4364 опция B

RFC 4364. ОПЦИЯ B

Для соединения MPLS VPN по опции B соединяют между собой выходные PE-маршрутизаторы участков VPN из разных автономных систем (single-hop MP-eBGP). Продление VPN в AS оператора-партнера для всех Заказчиков осуществляется через один интерфейс маршрутизатора, на котором устанавливают внешний протокол граничного шлюза с многопротокольным расширениями MP-eBGP. Как и в опции A, функции оконечного PE-маршрутизатора для каждой из VPN, продлеваемых в другую AS, выполняет пограничный ASBR-маршрутизатор, но на нем размещается только таблица маршрутов VPN-IPv4 для всех соединяемых между собой VPN и используется протокол MP-eBGP для передачи всех маршрутов Заказчика для всех VPN. Это позволяет экономить ресурсы маршрутизатора при большом числе подключений, так как не требуется размещения таблиц VRF-маршрутов IPv4 всех соединяемых между собой VPN и необходим только один блок описания интерфейса (рис.6).

Возможные конфликты между пересекающимися адресными пространствами VPN предотвращаются за счет использования маршрутов Заказчика в форме VPN-IPv4. На пограничном маршрутизаторе выполняется замена внутренней MPLS-метки автономной системы на внешнюю метку, назначенную протоколом MP-EBGP. Вместе с маршрутом VPN-IPv4 протокол MP-eBGP передает также связанные с ним атрибуты "Назначение маршрутов" (Route Target) для указания VPN и VRF, к которым данный маршрут относится.

Аналогично опции A использование опции B создает определенные сложности. В связи с тем, что при использовании

опции B MPLS VPN-туннели не прерываются на границе между AS, все параметры VPN и их истолкование операторами связи должны быть заранее согласованы. Это требует более тесной интеграции между сетями и техническими службами операторов связи, что не всегда возможно. Если пограничные маршрутизаторы операторов-партнеров изготовлены разными производителями оборудования, то возможны проблемы совместимости протоколов. Итак, сложности при использовании опции B заключаются в следующем:

- необходимо согласование настроек MP-eBGP пограничных ASBR-маршрутизаторов, в том числе режима "next-hop-self", применение loopback-интерфейсов, отключение ARF (отключение автоматической фильтрации необходимо в связи с отсутствием VRF), использование увеличенных значений MTU,
- невозможно контролировать функционирование отдельных VPN (так как все они передаются по одному соединению), также невозможно дифференцированное применение правил ограничения скорости трафика (в соответствии с классом обслуживания QoS),
- необходимо согласование (и указание в ТУ на подключение) параметров "Разделителя маршрутов" (Route Distinguisher) и атрибута "Назначение маршрута" (Route Target) для соединяемых VPN,
- необходимо согласование (и указание в ТУ на подключение) параметров кодирования (DSCP) классов обслуживания QoS и их перекодирования (при необходимости),
- невозможна тарификация отдельных VPN,
- сложно обеспечить выполнение требований информационной безопасности, так как при DoS-атаке на одну из VPN необходимо отключать трафик всех VPN.

Сложность согласования и настройки параметров подключения в опции B компенсируется сокращением трудозатрат на подключение, так как в отличие от опции A не требуется для каждой VPN настройка маршрутных таблиц на собственном ASBR и ASBR партнера. Упрощается по сравнению с опцией A резервирование, так как используется один интерфейс. Сокращаются требования к ресурсам пограничных маршрутизаторов ASBR, так как на них не размещаются VRF-таблицы каждой VPN и используется только один (при отсутствии резервирования) интерфейс для соединения автономных систем.

При организации соединения MPLS-сетей опция B может быть применена в VPN топологии "звезда" с центром в сети IP/MPLS Ростелеком при наличии значительного количества единовременно подключаемых узлов Заказчика через сеть оператора-партнера.

RFC 4364. ОПЦИЯ C

Опция C предназначена для крупномасштабного объединения сетей MPLS. Для продления соединений MPLS VPN пограничные ASBR-маршрутизаторы разных автономных систем соединяют между собой. Продление VPN в AS оператора-партнера для всех Заказчиков осуществляется через один интерфейс маршрутизатора, на котором устанавливают внешний протокол граничного шлюза с многопротокольным расширением MP-eBGP. Однако используется он не для передачи маршрутов VPN (как в опции B), а для передачи внутренних маршрутов IPv4 и меток для доступа к внутренним узлам автономных систем. Каждый из ASBR-маршрутизаторов получает из своей AS список внутренних IPv4 маршрутов вместе с метками и передает его партнеру. Таким образом формируется непрерывное поле IPv4 адресации и меток для сетей MPLS операторов партнеров, что позволяет организовать сквозное MPLS-соединение (рис.7).

В опции C для снижения нагрузки на пограничные маршрутизаторы обмен маршрутами VPN-IPv4 организуется через MP-eBGP-соединение между "Отражателями маршрутов" (Route Reflectors) каждой из автономных систем. MPLS VPN-туннель формируется не через ASBR, а непосредственно между входным и выходным PE-маршрутизаторами VPN в разных автономных системах.

Для обеспечения взаимного соединения MPLS VPN по опции C операторам связи необходимо согласовать и закрепить в ТУ на подключение те же параметры, что и в опции B, но теперь не только для VPN и пограничных маршрутизаторов ASBR, но и для отражателей маршрутов RR. Таким образом, применение опции C еще более усложняет процесс настройки и согласования. Существенно осложняется также выполнение требований информационной безопасности, так как соединенные по опции C MPLS-сети фактически функционируют как единое целое.

Преимуществом опции C является практически полная интеграция MPLS-сетей операторов-партнеров, что имеет существенное значение при массовой миграции VPN-сетей или объединении корпоративных сетей. В настоящее время опция C применяется в основном в процессах слияния/поглощения филиалов корпораций для объединения корпоративных MPLS-сетей с целью внедрения единой системы контроля и управления.

ПРАКТИЧЕСКИЕ ИТОГИ ПОСТРОЕНИЯ СЕТИ IP/MPLS РОСТЕЛЕКОМ

1. Рассмотрение существующих подходов к взаимному соединению MPLS-сетей операторов-связи с целью предоставления услуги IP VPN показывает, что осуществить наиболее полную тарификацию, мониторинг качества предоставляемой услуги и простоту настройки позволяет только соединение по опции A. Следует признать опцию A основным методом организации соединений, предлагаемым Операторам-партнерам для услуги InterAS-VPN.

2. В отдельных случаях, при значительном числе единовременно подключаемых узлов VPN Заказчика, может быть рассмотрена и предложена оператору-партнеру возможность соединения MPLS-сетей по методу опции B. Особое внима-

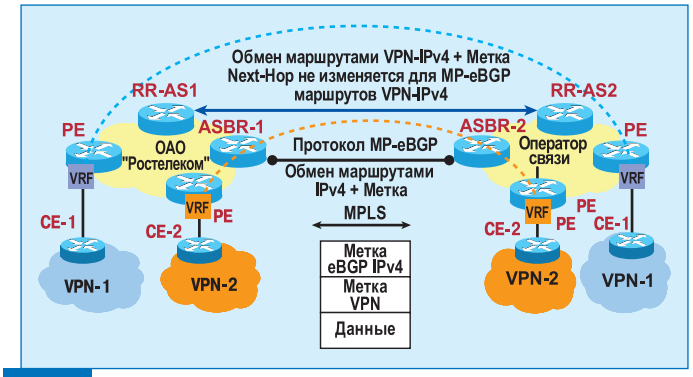

Рис.7 RFC 4364 опция C

ние при этом должно быть обращено на согласование параметров VPN и отражение их в технических условиях на присоединение сетей.

3. Для согласования правил кодирования RD (Разделитель маршрутов), RT (Назначение маршрутов), уровней качества обслуживания QoS при соединении VPN MPLS операторам-партнерам необходимо учитывать следующие общие положения:

- если Заказчиком VPN является Клиент ОАО "Ростелеком", кодирование (RD, RT, QoS), применяемое Клиентом, должно соответствовать правилам сети IP/MPLS Ростелеком. Оператор-партнер принимает необходимые меры по настройке PE-маршрутизаторов для установления соответствия между кодировкой (RD, RT, QoS) сети IP/MPLS Ростелеком и кодировкой (RD, RT, QoS), применяемой в сети Оператора-партнера.
- если Заказчиком VPN является Клиент Оператора-партнера, кодирование (RD, RT, QoS), применяемое Клиентом, должно соответствовать правилам сети Оператора-партнера. "Ростелеком" принимает необходимые меры по настройке PE-маршрутизаторов для установления соответствия между кодировкой (RD, RT, QoS) Оператора-партнера и кодировкой, применяемой в сети IP/MPLS Ростелеком.
- если количество классов обслуживания сети Оператора-партнера меньше количества классов обслуживания сети IP/MPLS Ростелеком, Оператор-партнер маркирует клиентский трафик отсутствующих у него классов обслуживания как соответствующий ближайшему высшему классу обслуживания собственной сети.

Использование указанного правила в качестве основы при взаимном соединении MPLS-сетей закреплено Решением рабочей группы Совета операторов электросвязи на прошедшем в Москве совещании в феврале 2008 года.

4. Опция C, предназначенная для взаимного объединения корпоративных MPLS-сетей при осуществлении массовой миграции VPN, для предоставления услуги InterAS-VPN не рекомендуется.

ЛИТЕРАТУРА

1. RFC 4364 BGP/MPLS IP Virtual private Networks (VPNs).
2. RFC 3031 Multiprotocol Label Switching Architecture.
3. RFC 3036 LDP Specification.
4. RFC 3107 Carrying Label Information in BGP-4.

Новые книги издательства "Техносфера". Серия "Мир связи"

Р. Морелос-Сарагоса
Искусство помехоустойчивого кодирования. Методы, алгоритмы применение.

Новейшее пособие по теории и практике цифровой связи, не имеющее аналогов в литературе на русском языке.

Наиболее активно идеи помехоустойчивого кодирования внедряются в системах мобильной связи и в магистральных высокоскоростных линиях. Быстрое распространение Интернета и мультимедийных средств стимулирует применение кодов, исправляющих ошибки, для защиты банков данных огромной емкости от случайных или преднамеренных искажений.

Помимо классических алгоритмов декодирования блоковых и сверхточных кодов детально рассмотрены современные идеи декодирования с "мягким решением" и итеративного декодирования.

Идеальное учебное пособие для студентов программистских и связных специальностей, инженеров-разработчиков и практиков.

И. Никульский
Оптические интерфейсы цифровых коммутационных станций и сети доступа

Рассматривается широкий круг вопросов построения оборудования оптических интерфейсов цифровых АТС, а также оптимального проектирования сетей доступа на основе этого оборудования.

Приводятся примеры практической реализации системных и схемных решений.

Для начинающих инженерно-технических работников, специализирующихся в области разработки и эксплуатации цифрового коммутационного оборудования, проектирования телекоммуникационных сетей, а также для широкого круга специалистов, проявляющих интерес к волоконно-оптическим интерфейсам и системам. Книга может быть полезна студентам и аспирантам вузов, обучающимся по специальностям, связанным с телекоммуникациями.

Р. Фриман
Волоконно-оптические системы связи. 4-е дополненное издание

Основные разделы книги посвящены следующим темам. Источники и приемники оптического сигнала. Оптоволоконная среда распространения с присущими ей нелинейными эффектами. Технологии SONET/SDH и WDM и используемое ими оборудование: оптические усилители и мультиплексоры. Инженерные аспекты оптических систем передачи в целом, включая планирование, прокладку и тестирование сети, мониторинг ее показателей работоспособности и вопросы функционирования сети и ее управления.

Дополнительные разделы посвящены синхронизации цифровых сетей SDH и оценке показателей ошибок в таких сетях.

Монография не имеет аналогов в литературе на русском языке по полноте комплексного описания оптических систем связи. Адресована профессиональным разработчикам телекоммуникационных систем и инженерам-связистам.