

Рекомендация RFC 2547bis: Основы виртуальных частных сетей на базе BGP/MPLS

Чак Семерия
Инженер по маркетингу

Содержание

Введение.....	3
Обзор ВЧС на базе BGP/MPLS.....	4
Компоненты сети.....	4
Устройства на границе сети клиента.....	4
Устройства на границе сети провайдера.....	4
Маршрутизаторы поставщика услуг.....	5
Модель функционирования.....	5
Пример сетевой топологии.....	5
Поток управления.....	6
Поток данных.....	7
Преимущества ВЧС BGP/MPLS.....	8
Проблемы и решения.....	8
Наложение адресных пространств клиента.....	8
Семейство адресов VPN-IPv4.....	9
Мультипротокольные расширения BGP.....	10
Ограничение связей в сети.....	10
Множество таблиц форвардинга.....	10
Атрибуты Extended Community протокола BGP.....	11
Обновление маршрутной информации ВЧС.....	13
Экономия полосы пропускания магистрали и ресурсов пакетной обработки маршрутизатора PE.....	14
Пример единой магистрали поставщика услуг.....	14
Распространение маршрутной информации ВЧС.....	16
Распространение на участке от маршрутизатора CE до входного маршрутизатора PE.....	16
Распространение маршрутов по магистрали от входного PE к выходному PE.....	18
Распространение маршрута от выходного маршрутизатора PE к CE.....	21
Продвижение трафика клиента ВЧС через магистраль BGP/MPLS.....	22
Форвардинг от маршрутизатора CE источника до входного маршрутизатора PE.....	23
Форвардинг входного маршрутизатора PE.....	23
Форвардинг маршрутизатора P.....	23
Форвардинг от маршрутизатора PE к маршрутизатору CE назначения.....	23
Пример 1. Форвардинг трафика красной ВЧС с сайта 1 на сайт 4.....	24
Пример 2. Форвардинг трафика красной ВЧС от сайта 4 к сайту 1.....	25
Пример 3. Форвардинг трафика зеленой ВЧС от сайта 6 на сайт 7.....	26
Доступ к общественной сети Интернет с сайта ВЧС.....	27
Доступ в Интернет без использования таблиц VRF.....	27
Доступ хостов ВЧС к сети Интернет.....	27

Взаимодействие сети Интернет с хостами ВЧС	27
Масштабируемость ВЧС BGP/MPLS	28
Заключение	28
Литература	29
Рабочие документы Интернет	29
Рекомендации	29
Книги	29

Введение

До недавнего времени существовали ясные различия между общественными и частными сетями. Общественная сеть, подобная обычной телефонной сети (ТфОП) или Интернету, - это группа независимых систем, в которой допускается свободный обмен информацией между всеми системами группы. Частная сеть состоит из компьютеров, осуществляющих взаимный обмен информацией и находящихся в собственности одной организации, которая осуществляет и администрирование сети. Различные сайты частной сети связаны между собой арендуемыми линиями, и предприятие, которое развертывает частную сеть - единственная организация, использующая эту сеть.

Хотя развертывание единственной модели обслуживания виртуальной частной сети (ВЧС) могло бы упростить сетевые операции, этот подход не может удовлетворить различные требования абонентов, так как все они уникальны. Каждый абонент предъявляет разные требования к безопасности, числу сайтов, сложности маршрутизации, критичным специализированным приложениям, моделям и объемам трафика, уровню квалификации персонала сети и готовности предоставления внешних сетевых услуг. Для удовлетворения широкого спектра требований, поставщики услуг должны предлагать абонентам разные модели доставки услуг. Существует несколько различных моделей ВЧС.

- Традиционные ВЧС
 - Frame Relay (Уровень 2)
 - ATM (Уровень 2)
- ВЧС на основе клиентского оборудования (CPE)
 - L2TP и PPTP (Уровень 2)
 - IPSec (Уровень 3)
- ВЧС, формируемые поставщиком услуг
 - ВЧС уровня 2 на основе MPLS
 - ВЧС, поддерживающие BGP/MPLS или рекомендацию RFC2547bis (уровень 3)

В данной статье детально изучается модель обслуживания ВЧС, предложенная в рекомендации RFC 2547bis, которая вызывает большой интерес у поставщиков услуг. Она предлагает механизм, упрощающий операции территориальной, глобальной вычислительной сети (ГВС) для разнообразных групп абонентов, имеющих ограниченные знания в области IP маршрутизации. Применение рекомендации RFC 2547bis позволяет эффективно масштабировать сети при оказании высоко рентабельных услуг.

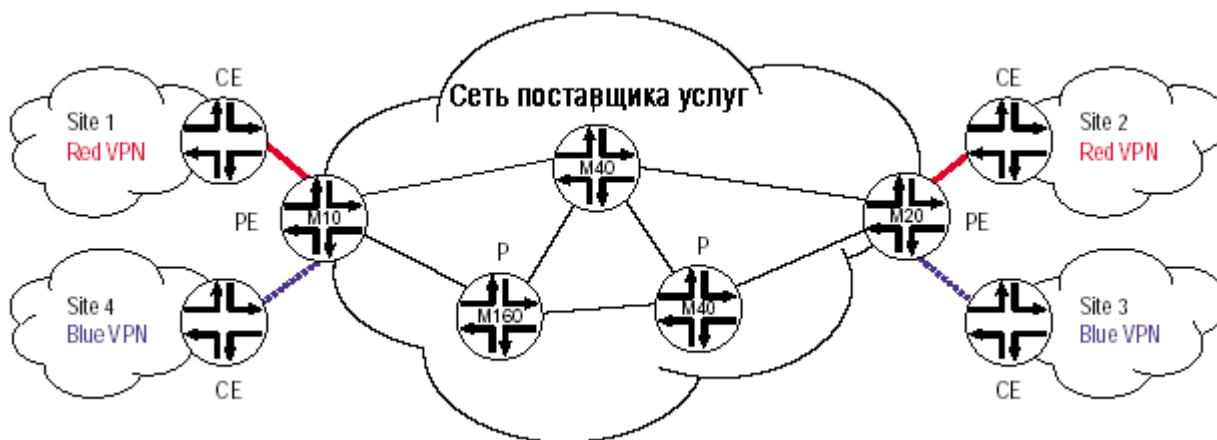
Обзор ВЧС на базе BGP/MPLS

Рекомендация RFC 2547bis определяет механизм, позволяющий поставщикам услуг использовать IP магистраль для предоставления абонентам услуг ВЧС. ВЧС, соответствующую рекомендации RFC 2547bis, можно назвать так же ВЧС BGP/MPLS, так как для распространения маршрутной информации по магистральной поставщика услуг используется протокол BGP, а для продвижения трафика от одного сайта ВЧС к другому используется протокол MPLS (MultiProtocol Label Switching - многопротокольная коммутация меток). Первоначальные цели этого подхода включали следующее.

- Сделать обслуживание очень простым для абонентов, даже если у них нет опыта IP маршрутизации.
- Сделать обслуживание очень гибким и масштабируемым для облегчения крупномасштабного развертывания.
- Разрешить реализацию правил создания ВЧС только поставщику услуг или поставщику совместно с клиентом.
- Обеспечить оказание современных дополнительных услуг, стимулирующих укрепление доверия абонента.

Компоненты сети

В контексте рекомендации RFC 2547bis ВЧС является набором правил, управляющих связью между множеством сайтов. Сайт абонента подключен к сети поставщика услуг через один или несколько портов, ассоциируемых провайдером с таблицей маршрутизации ВЧС. В терминах RFC 2547bis таблица маршрутизации ВЧС называется *таблицей маршрутизации и форвардинга (VRF) ВЧС*. На рис. 1 показаны основные блоки, составляющие ВЧС BGP/MPLS.



CE (Customer Edge) - граница сети клиента

P (Provider Router) - маршрутизаторы поставщика услуг

PE (Provider Edge) - граница сети поставщика услуг

Рисунок 1. Компоненты сети в соответствии с рекомендацией RFC 2547bis

Устройства на границе сети клиента

Устройства, установленные на границе сети клиента (CE), обеспечивают доступ к сети поставщика услуг по линии передачи данных к одному или нескольким маршрутизаторам на границе сети поставщика услуг (PE). Устройство CE может быть хостом или коммутатором уровня 2, но обычно это IP маршрутизатор, устанавливающий отношения смежности (adjacency) с непосредственно подключенными к нему маршрутизаторами PE. После установления отношений смежности маршрутизатор CE объявляет *локальные маршруты* ВЧС маршрутизатору PE и узнает о маршрутах *удаленной* ВЧС от маршрутизатора PE.

Устройства на границе сети провайдера

Маршрутизаторы PE обмениваются маршрутной информацией с маршрутизаторами CE с использованием статической маршрутизации, протоколов RIPv2, OSPF или EBGP. Маршрутизатор PE должен хранить маршрутную информацию ВЧС для тех ВЧС, к которым он непосредственно подключен. Это значительно

увеличивает масштабируемость модели RFC 2547bis, так как исключается необходимость для PE маршрутизаторов обслуживать все маршруты ВЧС поставщика услуг.

Каждый маршрутизатор PE хранит таблицу VRF для всех непосредственно подключенных сайтов. Каждое клиентское соединение (Frame Relay PVC, ATM PVC, VLAN) отображается на отдельную VRF. Поэтому с таблицей VRF ассоциируется не сайт, а порт маршрутизатора PE. Заметим, что с одной VRF может ассоциироваться несколько портов маршрутизатора PE. Возможность маршрутизаторов PE обслуживать несколько таблиц форвардинга поддерживает разделение маршрутной информации по каждой ВЧС.

После получения информации о маршрутах локальной ВЧС от маршрутизаторов CE, маршрутизатор PE обменивается маршрутной информацией ВЧС с другими маршрутизаторами PE по протоколу IBGP. Маршрутизаторы PE могут обслуживать сессии IBGP с рефлексорами маршрутов (route reflectors) как альтернативу полносвязным сессиям IBGP. Развертывание множества рефлексоров улучшает масштабируемость модели RFC 2547bis, так как устраняется необходимость хранения одним компонентом сети всех маршрутов ВЧС.

Наконец, когда для продвижения трафика ВЧС через магистраль поставщика услуг используется MPLS, входной маршрутизатор PE функционирует как входной LSR и выходной маршрутизатора PE - как выходной LSR.

Маршрутизаторы поставщика услуг

Маршрутизатор поставщика услуг (P) - это любой маршрутизатор в сети поставщика услуг, не подключенный к устройствам CE. При продвижении трафика ВЧС между маршрутизаторами PE маршрутизаторы P функционируют как транзитные MPLS LSR. Так как трафик продвигается через магистраль MPLS с использованием двухуровневого стека меток, маршрутизаторам P требуется обслуживать только маршруты к маршрутизаторам поставщика услуг PE; от них не требуется хранить конкретную маршрутную информацию ВЧС для всех клиентских сайтов.

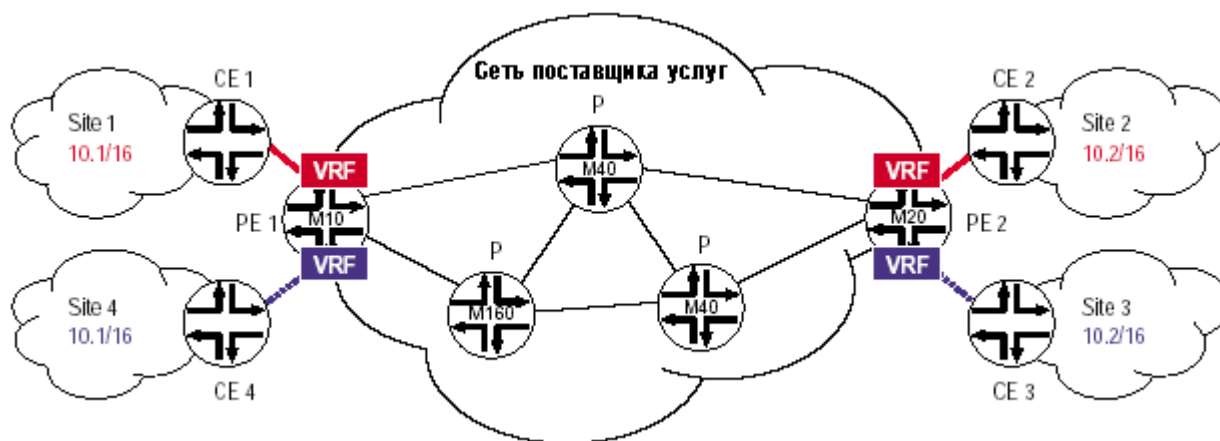
Модель функционирования

В сети ВЧС BGP/MPLS имеют место два основных потока трафика.

- Поток управления, используемый для распространения маршрута ВЧС и установления пути коммутации меток (LSP).
- Поток данных, который используется для продвижения трафика данных абонента.

Пример сетевой топологии

На рис. 2 показана примерная топология сети, в которой единственный поставщик услуг предоставляет услуги ВЧС BGP/MPLS различным корпоративным клиентам. В этой сети имеются два маршрутизатора PE, подключенных к четырем различным сайтам.



CE (Customer Edge) - граница сети клиента

P (Provider Router) - маршрутизаторы поставщика услуг

PE (Provider Edge) - граница сети поставщика услуг

VRF (VPN Routing and Forwarding Table) - таблица маршрутизации и форвардинга ВЧС

Рисунок 2. Пример топологии ВЧС BGP/MPLS

Связь между сайтами описывается следующими правилами:

- Любой хост сайта 1 может связываться с любым хостом сайта 2.
- Любой хост сайта 2 может связываться с любым хостом сайта 1.
- Любой хост сайта 3 может связываться с любым хостом сайта 4.
- Любой хост сайта 4 может связываться с любым хостом сайта 3.

Поток управления

В ВЧС BGP/MPLS поток управления состоит из двух субпоток.

- Первый субпоток управления отвечает за обмен маршрутной информацией между маршрутизаторами CE и PE на границах магистральной поставщика услуг и между маршрутизаторами PE через магистраль поставщика услуг.
- Второй субпоток управления отвечает за установление пути LSP между маршрутизаторами PE через магистраль поставщика услуг.

Обмен маршрутной информацией

В этом примере PE 1 сконфигурирован для ассоциирования красной VRF с интерфейсом или субинтерфейсом, по которому он узнает маршруты от CE 1. Когда CE1 объявляет маршрут для префикса 10.1/16 к PE 1, PE 1 устанавливает локальный маршрут к 10.1/16 в красную VRF.

PE 1 объявляет маршрут для 10.1/16 к PE 2, используя IBGP. Перед объявлением маршрута PE 1 выбирает метку MPLS (например, 222) для объявления вместе с маршрутом и использует loopback address как следующий транзит BGP (BGP next hop) для маршрута.

RFC 2547bis поддерживает наложение адресных пространств (частная адресация определена в RFC 1918), используя отличительные признаки маршрута (RD) и семейство адресов VPN-IPv4. RFC 2547bis ограничивает распространение маршрутной информации между маршрутизаторами PE при помощи маршрутных фильтров, построенных на расширенных атрибутах BGP (route targets).

Когда PE 2 принимает объявление маршрута от PE 1, он определяет, следует ли встраивать маршрут к префиксу 10.1/16 в красную таблицу VRF путем фильтрации маршрута на основе атрибутов extended community протокола BGP, полученных с маршрутом. Если PE 2 решает установить маршрут в красную таблицу VRF, он затем объявляет CE 2 маршрут к префиксу 10.1/16.

Установление пути LSP

Чтобы использовать протокол MPLS для продвижения трафика ВЧС через магистраль поставщика услуг необходимо установить пути LSP между маршрутизатором PE, узнающим маршрут, и маршрутизатором PE, объявляющим маршрут (рис. 3).

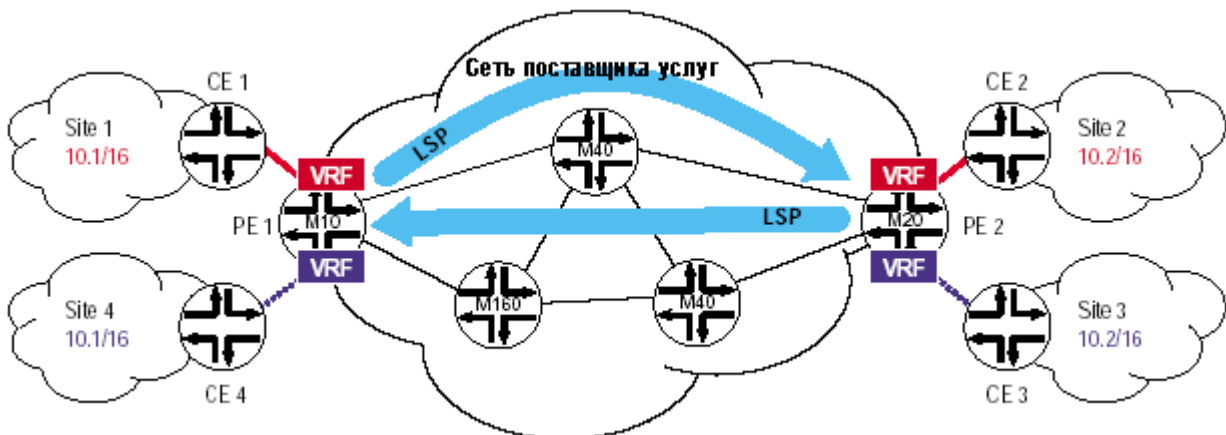


Рисунок 3. Пути LSP между сайтом 1 и сайтом 2

Пути LSP могут прокладываться и обслуживаться через сеть поставщика услуг с использованием либо протокола распространения метки LDP (Label Distribution Protocol), либо протокола резервирования ресурсов RSVP (Resource Reservation Protocol).

- Если поставщик услуг хочет проложить между двумя PE маршрутизаторами путь LSP класса *best-effort* (с максимально возможным качеством), используется LDP.
- Если поставщик услуг хочет выделить полосу пропускания для пути LSP или использовать регулирование трафика для установления явного пути LSP, используется RSVP. LSP на основе RSVP поддерживают заданное качество обслуживания (QoS) и регулирование трафика.

Для взаимной совместимости с оборудованием различных производителей от всех маршрутизаторов PE и Р как минимум требуется поддержка LDP.

- Если поставщик услуг выбирает использование LDP, в магистральной для поддержки связей PE-PE прокладываются полносвязные пути LSP класса *best-effort*.
- Если поставщик услуг выбирает использование RSVP, то LSP на основе RSVP имеют больший приоритет, чем LSP на основе LDP. Между парой маршрутизаторов PE присутствуют LSP как на основе LDP, так и на основе RSVP. Входной маршрутизатор коммутации меток (LSR) выберет LSP-RSVP, но не LSP-LDP. Эта модель поддерживает инкрементное наращивание конфигурации LSP на основе RSVP в магистральной поставщика услуг. Заметим, что при этом между маршрутизаторами PE возможна прокладка одного или нескольких параллельных LSP (возможно с различным качеством обслуживания). Кроме того, рефлектор маршрута просто работает как сервер, отражающий маршруты от входного маршрутизатора PE к выходному маршрутизатору PE. Если поставщик услуг использует отражение маршрута, ему все равно требуется прокладывать LSP между маршрутизаторами PE, так как рефлекторы маршрута не являются необходимой частью транзитного пути между маршрутизаторами PE.

Поток данных

На рис. 4 показан поток трафика данных ВЧС через магистраль поставщика услуг от одного сайта клиента к другому сайту клиента. Допустим, хост 10.2.3.4 на сайте 2 хочет связаться с сервером 10.1.3.8 на сайте 1.

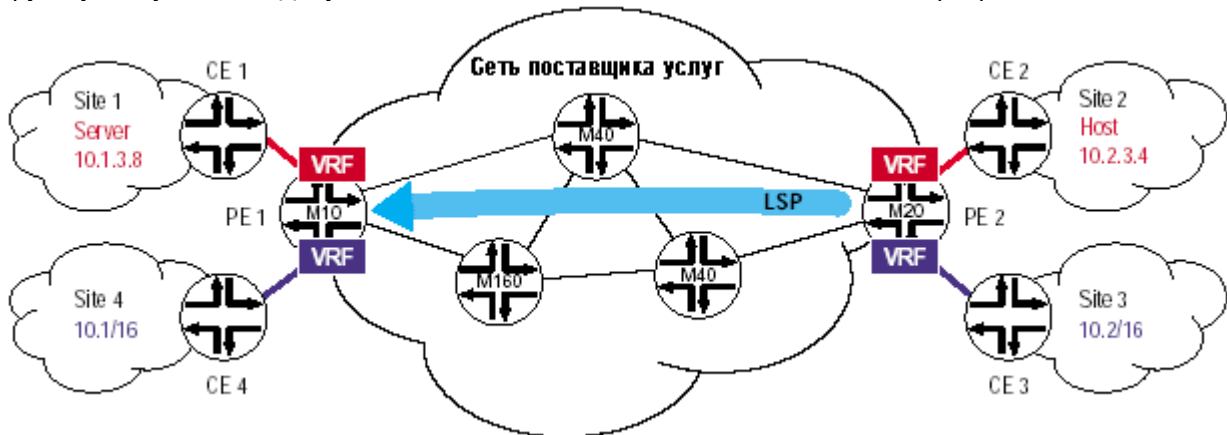


Рисунок 4. Поток данных от сайта 2 к сайту 1

Хост 10.2.3.4 продвигает все пакеты данных для сервера 10.1.3.8 в шлюз по умолчанию. Когда пакет поступает на маршрутизатор CE 2, он производит поиск самого длинного согласующегося маршрута и продвигает пакет IPv4 к PE 2.

PE 2 принимает пакет, производит поиск маршрута в красной VRF и получает следующую информацию:

- Метку MPLS, которая была присвоена маршрутизатором PE 1 маршруту (метка=222).
- Следующий транзит BGP для маршрута (loopback address PE 1).
- Исходящий субинтерфейс для пути LSP от PE 2 к PE 1.
- Начальная метку MPLS для пути LSP от PE 2 к PE 1

Трафик пользователя продвигается от PE 2 к PE 1 с использованием MPLS со стеком меток, содержащем две метки. Для этого потока данных PE 2 является входным LSR для пути LSP, и PE 1 является выходным LSR для пути LSP. До передачи пакета PE 2 помещает метку 222 в стек меток, делая ее нижней (или внутренней) меткой. Эта метка изначально встраивается в красную таблицу VRF в тот момент, когда PE 2

принимает объявление протокола IBGP для маршрута к 10.1/16. Затем PE 2 помещает в стек метку, ассоциированную с путем LSP на основе LDP или RSVP к маршрутизатору PE 1 (следующий транзит BGP), делая ее верхней (или внешней) меткой.

После создания стека меток PE 2 продвигает пакет MPLS на выходной интерфейс к первому маршрутизатору Р по пути LSP от PE 2 к PE 1. Маршрутизаторы Р коммутируют пакеты по магистрали сети поставщика услуг на основе верхней метки. Предпоследний по отношению к PE 1 маршрутизатор выталкивает верхнюю метку (открывая нижнюю или внутреннюю метку) и продвигает пакет к PE 1. Когда PE 1 принимает пакет, он выталкивает метку, создавая стандартный (native) пакет IPv4. PE 1 использует нижнюю метку (222) для идентификации непосредственно подключенного CE, который является следующим транзитом маршрута к 10.1/16. Наконец, PE 1 продвигает стандартный пакет IPv4 к CE 1, который затем продвигает пакет к серверу 10.1.3.8 на сайте 1.

Преимущества ВЧС BGP/MPLS

Основной целью ВЧС BGP/MPLS является упрощение сетевых операций для клиентов и обеспечение для поставщика услуг возможности предоставления масштабируемых, рентабельных дополнительных услуг. Преимущества ВЧС BGP/MPLS включают:

- Отсутствуют ограничения на план адресов, используемый каждым клиентом ВЧС. Клиент может использовать либо уникальное, либо частное адресное пространство IP. С точки зрения поставщика услуг, клиенты могут иметь перекрывающиеся адресные пространства.
- Маршрутизатор CE на каждом из сайтов клиента не обменивается непосредственно маршрутной информацией с другими маршрутизаторами CE. Клиенты не должны вникать в проблемы маршрутизации между сайтами, за которые несет ответственность поставщик услуг.
- У клиентов ВЧС нет магистрали или *виртуальной магистрали*, которую им нужно было бы администрировать. Следовательно, клиентам не нужен доступ к маршрутизаторам PE или Р на уровне управления.
- Поставщики услуг не занимаются администрированием отдельной магистрали или виртуальной магистрали для каждого клиента ВЧС. Следовательно, поставщикам услуг не требуется доступ к маршрутизаторам CE на уровне управления.
- Правила, определяющие принадлежность конкретного сайта к данной ВЧС, являются правилами, устанавливаемыми клиентом. Модель администрирования ВЧС RFC 2547bis позволяет сделать так, что правила клиента реализуются либо одним только поставщиком услуг, либо совместно поставщиком услуг и клиентом.
- ВЧС могут охватывать множество поставщиков услуг. Хотя эта особенность ВЧС BGP/MPLS и важна, в этой статье решения ВЧС с взаимодействием различных поставщиков услуг не рассматриваются.
- Без использования каких-либо методов криптографии, безопасность эквивалентна той, которая обеспечивается магистральными сетями уровня 2 (ATM или Frame Relay).
- Поставщики услуг могут использовать общую инфраструктуру как для предоставления услуг ВЧС, так и для доступа в Интернет.
- Гибкое и масштабируемое качество обслуживания услуг ВЧС поддерживается путем использования экспериментальных битов в поле заголовка MPLS (shim header) или за счет использования регулирования трафика LSP (по сигнализации RSVP).
- Модель RFC 2547bis не зависит от уровня канала (уровня 2).

Проблемы и решения

Рекомендация RFC 2547bis использует несколько механизмов для улучшения масштабируемости и решения специфических проблем функционирования ВЧС. Эти проблемы перечислены ниже.

- Поддержка перекрывающихся адресных пространств клиента.
- Ограничения на связи в сети.
- Обслуживание обновленной маршрутной информации ВЧС.
- Экономия полосы пропускания магистрали и ресурсов обработки пакетов маршрутизатора PE.

Наложение адресных пространств клиента

Клиенты ВЧС часто управляют своими собственными сетями и используют частное адресное пространство в соответствии с RFC 1918. Если клиенты не используют глобальных уникальных IP адресов, один и тот же 32-битный адрес IPv4 может использоваться для идентификации различных систем в различных ВЧС. В результате, могут наблюдаться трудности маршрутизации, так как протокол BGP предполагает, что каждый

доставляемый им адрес IPv4 является глобально уникальным. Для разрешения этой проблемы ВЧС BGP/MPLS поддерживают механизм, который преобразует неуникальные адреса в уникальные путем комбинирования используемого семейства адресов VPN-IPv4 с мультипротокольными расширениями BGP (MP-BGP).

Семейство адресов VPN-IPv4

Одной из проблем, возникающей вследствие наложения адресных пространств, является то, что если стандартный протокол BGP видит два различных маршрута к одному префиксу адреса IPv4 (где этот префикс присвоен системам в различных ВЧС), BGP трактует префиксы как эквивалентные и прокладывает только один маршрут. В результате вторая система становится недоступной. Для устранения этой проблемы требуется механизм, позволяющий BGP различать префиксы так, чтобы было возможно проложить два абсолютно разных маршрута, направленных в разные ВЧС. RFC 2547bis поддерживает эту возможность через определение адресного пространства VPN-IPv4.

Адрес VPN-IPv4 занимает 12 байт: 8 байт – это отличительный признак маршрута RD, и 4 байта - префикс адреса IPv4. На рис. 5 показана структура адресов VPN-IPv4.

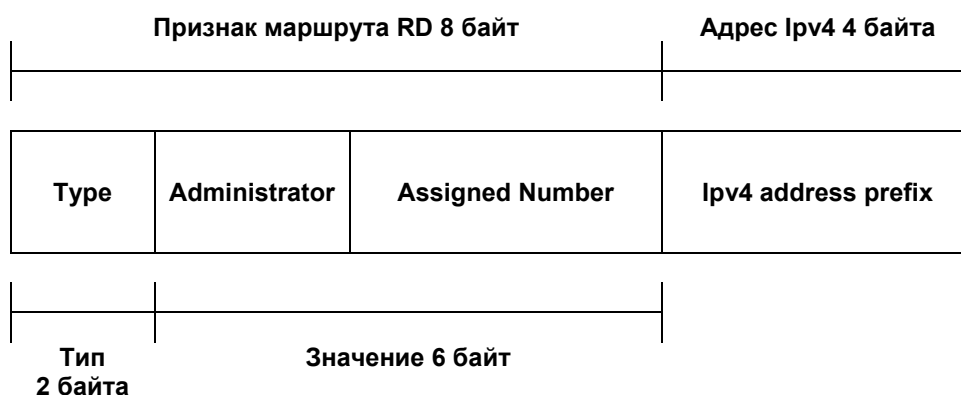


Рисунок 5. Кодирование отличительных признаков маршрута и адресов IPv4.

8-байтное поле RD включает поля типа (2 байта) и значения (6 байт). Тип определяет длину двух внутренних полей поля значения (поле администратора и поле назначенного номера), а также семантику поля администратора. В настоящее время поле типа может принимать значения 0 и 1.

- Для типа 0, подполе Administrator (Администратор) содержит 2 байта, и подполе Assigned Number (присвоенный номер) содержит 4 байта. Подполе Administrator содержит номер автономной системы (ASN). Использование ASN из частного пространства ASN настоятельно не рекомендуется. Подполе Assigned Number содержит значение из пространства нумерации, администрируемого поставщиком услуг ВЧС, которому был присвоен ASN.
- Для Типа 1 подполе администратора содержит 4 байта и подполе Assigned Number содержит 2 байта. Подполе Administrator содержит адрес IPv4. Использование IP адреса из частного IP адресного пространства настоятельно не рекомендуется. Подполе Assigned Number содержит значение из пространства нумерации, администрируемого поставщиком услуг, предлагающим услуги ВЧС, которому был присвоен ASN. Вариант конфигурации для RD типа 1 предполагает использование адреса обратной связи маршрутизатора PE, являющегося источником маршрута, для 4-байтного подполя Administrator и выбор номера, являющегося локальным для этого маршрутизатора PE, для 2-байтного подполя Assigned Number.

Когда на маршрутизаторах PE конфигурируются RD, по рекомендации RFC 2547bis не требуется, чтобы все маршруты ВЧС использовали один и тот же RD, и фактически каждая таблица VRF в ВЧС может использовать собственный RD. Однако поставщик услуг должен убедиться в глобальной уникальности RD. Именно поэтому использование частного пространства ASN или частного адресного пространства IP при определении RD настоятельно не рекомендуется. Использование общественного пространства ASN или общественного пространства IP адресов гарантирует уникальность RD. Глобально уникальные RD обеспечивают механизм, позволяющий каждому поставщику услуг администрировать свое собственное адресное пространство и создавать глобально уникальные адреса VPN-IPv4 без конфликта с RD, присвоенными другими поставщиками услуг. Использование глобально уникальных RD обеспечивает следующее.

- Создание отдельных маршрутов для общего префикса IPv4.

- Создание множества глобально уникальных маршрутов к одной системе.
- Использование правил для принятия решения о том, по какому маршруту направляются какие пакеты.

В заключение приведем несколько замечаний по использованию адресов VPN-IPv4 в ВЧС BGP/MPLS.

- Адреса VPN-IPv4 используются только в сети поставщика услуг.
- Клиенты ВЧС не знают об использовании адресов VPN-IPv4.
- Адреса VPN-IPv4 переносятся только маршрутными протоколами в магистрале поставщика услуг.
- Адреса VPN-IPv4 не переносятся в заголовках пакетов ВЧС при проходе магистрале поставщика услуг.

Мультипротокольные расширения BGP

Другим ограничением использования стандартного протокола BGP4 для поддержки ВЧС BGP/MPLS является то, что он изначально был спроектирован для переноса маршрутной информации только для семейства адресов IPv4. Ликвидируя это ограничение, IETF работает над стандартизацией мультипротокольных расширений для BGP 4 (*Multiprotocol Extensions for BGP4*). Эти расширения были определены в рекомендации RFC 2283 (февраль 1998) и позже скорректированы в рекомендации RFC 2858 (июнь 2000). Расширения позволяют BGP4 переносить маршрутную информацию для множества протоколов сетевого уровня (IPv6, IPX, VPN-IPv4 и т.п.). Поэтому для развертывания ВЧС BGP/MPLS и поддержки распространения маршрутов VPN-IPv4 маршрутизаторы PE требуют поддержки MP-BGP, а не просто BGP.

Перед обменом маршрутной информацией VPN-IPv4 по рекомендации RFC 2547bis требуется согласование возможностей BGP, гарантирующее, что все хосты BGP смогут обработать семейство адресов VPN-IPv4. Заметим, что расширения MP-BGP совместимы сверху вниз, т.е. маршрутизатор, поддерживающий расширения MP-BGP, может взаимодействовать с маршрутизатором, не поддерживающим эти расширения. Однако стандартный BGP4 не поддерживает ВЧС RFC 2547bis.

Ограничение связей в сети

Допустим, что маршрутная таблица не содержит маршрута по умолчанию. Основное положение IP маршрутизации состоит в том, что если маршрут конкретной сети не встроен в таблицу форвардинга, то эта сеть недостижима с этого маршрутизатора. Ограничивая поток маршрутной информации, поставщик услуг может эффективно управлять потоком трафика данных ВЧС клиента. Модель ВЧС BGP/MPLS ограничивает поток маршрутной информации путем использования двух механизмов.

- Множество таблиц форвардинга
- Атрибуты расширенного сообщества BGP

Множество таблиц форвардинга

Каждый маршрутизатор PE обслуживает одну или более таблиц форвардинга для сайта, известных как VRF. Когда маршрутизатор PE сконфигурирован, каждая из его таблиц VRF ассоциируется с одним или несколькими портами (интерфейсами, субинтерфейсами) на маршрутизаторе PE, который непосредственно подключен к клиентам поставщика услуг. Если данный сайт содержит хосты, входящие в несколько ВЧС, тогда таблица VRF, ассоциированная с сайтом клиента, будет содержать маршруты для всех ВЧС, в которые входит этот сайт.

Принимая внешний пакет данных клиента от непосредственно подключенного маршрутизатора CE, маршрутизатор PE производит поиск маршрута в таблице VRF, ассоциированной с этим сайтом. Конкретная VRF определяется субинтерфейсом, по которому был принят пакет. Поддержка множества таблиц форвардинга облегчает маршрутизатору PE разделение маршрутной информации по каждой ВЧС.

Рисунок 6 иллюстрирует заполнение маршрутизатором PE 1 красной таблицы VRF.

- PE 1 узнает маршруты красной ВЧС сайта 1 от CE 1 и встраивает их в красную таблицу VRF.
- Удаленные маршруты узнаются по MP-IBGP от других маршрутизаторов PE, которые непосредственно подключены к сайтам с хостами, входящими в красную ВЧС. PE 1 узнает маршруты красной ВЧС сайта 2 от CE 2 и встраивает их в красную VRF. Импорт удаленных маршрутов в красную таблицу VRF управляется путем использования атрибутов расширенного сообщества маршрутов BGP.
- Локальные маршруты синей ВЧС на сайте 4 и удаленные маршруты синей ВЧС на сайте 3 не ассоциируются с красной ВЧС и не импортируются в красную таблицу VRF.

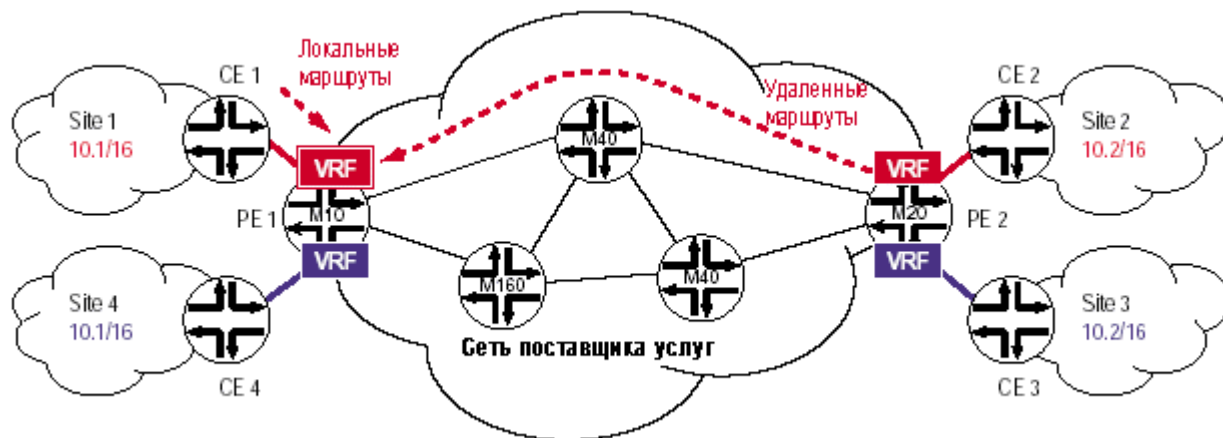


Рисунок 6. Маршрутизатор PE заполняет таблицу маршрутизации и форвардинга ВЧС

Поддержка маршрутизаторами PE множества таблиц форвардинга определяет многочисленные преимущества.

- Различные сайты ВЧС, обслуживаемые одним маршрутизатором PE, могут использовать перекрывающиеся адресные пространства.
- Выбор конкретной таблицы форвардинга для трафика данных определяется правилами (отображения субинтерфейса на VRF), а не содержимым пакета.
- Множество таблиц форвардинга предотвращают связь между сайтами, которые не имеют общей ВЧС.
- Масштабируемость улучшается, так как маршрутизаторам PE не требуются поддерживать выделенную таблицу VRF для всех ВЧС, поддерживаемых сетью поставщика услуг. Каждый маршрутизатор PE обслуживает только VRF для непосредственно подключенных сайтов.
- Наконец, магистральная сеть может поддерживать множество различных маршрутов к одной системе, где маршрут конкретного пакета определяется сайтом, от которого пакет поступил в магистраль поставщика услуг.

Атрибуты Extended Community протокола BGP

Распространение маршрутной информации ВЧС ограничивается использованием атрибутов extended community протокола BGP. Они транспортируются в сообщениях BGP как атрибуты маршрута и идентифицируют принадлежность маршрута конкретному набору маршрутов, все из которых обрабатываются одинаково, в соответствии с правилами маршрутизации. Каждый атрибут BGP должен быть глобально уникальным (содержать либо глобальный IP адрес, либо ASN) и может использоваться только одной ВЧС. Однако ВЧС данного клиента может использовать множество глобально уникальных атрибутов BGP для управления распространением маршрутной информации.

ВЧС BGP/MPLS использует 32-битные атрибуты extended community протокола BGP вместо обычных 16-битных атрибутов community. Использование 32-битных атрибутов улучшает масштабируемость, т.к. один провайдер может поддерживать максимум 2^{32} атрибутов community (а не 2^{16}). Т.к. каждый атрибут содержит глобальный уникальный номер автономной системы провайдера (AS), последний может контролировать локальные назначения и одновременно поддерживать глобальную уникальность этих назначений. ВЧС RFC 2547bis могут использовать три различных типа атрибутов BGP.

- Атрибут цели маршрута (route target) идентифицирует множество сайтов (таблиц VRF), для которых маршрутизатор PE распространяет маршруты. Маршрутизатор PE использует этот атрибут для ограничения импорта удаленных маршрутов в его таблицы VRF.
- Атрибут ВЧС источника (VPN-of-origin) идентифицирует множество сайтов и прокладывает ассоциированный маршрут как проходящий от одного из сайтов в этом множестве.
- Атрибут сайт-источник (site-of-origin) идентифицирует конкретный сайт, от которого маршрутизатор PE узнал маршрут. Он кодируется как атрибут источника маршрута расширенного сообщества, который можно использовать для предотвращения петель маршрутизации.

Модель функционирования

Перед распространением локальных маршрутов другим маршрутизаторам PE, входной маршрутизатор PE прикрепляет атрибут цели маршрута к каждому маршруту, о котором он узнал от непосредственно подключенных сайтов. Цель маршрута определяется на основе значений сконфигурированных в VRF правил экспорта цели. Такой подход обеспечивает большую гибкость в процессе присвоения маршрутизатором PE атрибута цели маршрута некоторому маршруту.

- Входной маршрутизатор PE может быть сконфигурирован для присвоения единственной цели маршрута всем маршрутам, о которых он узнал от данного сайта.
- Входной маршрутизатор PE может быть сконфигурирован для присвоения одной цели маршрута некоторому множеству маршрутов, которые он узнал от сайта, и присвоения другой цели маршрута остальным множествам маршрутов с сайта.

Если маршрутизатор CE связывается с маршрутизатором PE по протоколу EBGP, маршрутизатор CE может указать одну или более целей маршрута для каждого маршрута. При этом подходе управление реализацией правил ВЧС переходит от поставщика услуг на клиента.

Перед встраиванием удаленных маршрутов, которые распространяются другим маршрутизатором PE, каждая таблица VRF на выходном маршрутизаторе конфигурируется с импортом правил цели. Маршрутизатор PE может встраивать маршрут VPN-IPv4 в таблицу VRF только если атрибут цели маршрута, переносимый с маршрутом, согласуется с одной из импортированных целей таблиц VRF маршрутизатора PE.

Это позволяет поставщику услуг использовать единый механизм для поддержки ВЧС клиентов, имеющих большой диапазон правил связи между сайтами. При тщательном конфигурировании правил импорта и экспорта цели, поставщики услуг могут конструировать различные типы топологий ВЧС. Механизмы реализации топологий ВЧС могут быть полностью в ведении поставщика услуг, и клиенты ВЧС не будут знать об этом процессе.

Пример 1. Топология полносвязной ВЧС

Допустим, корпорация Corporation Red, обозначенная красным цветом, дает поручение поставщику услуг ВЧС BGP/MPLS на создание ВЧС, поддерживающей полную связь между сайтами (рис. 7). Каждый из сайтов Corporation Red может отправлять трафик напрямую другому сайту этой корпорации. При этом сайты корпорации Corporation Blue, обозначенной синим цветом, получающие услуги ВЧС BGP/MPLS от того же самого поставщика услуг, не могут обмениваться трафиком с сайтами Corporation Red.

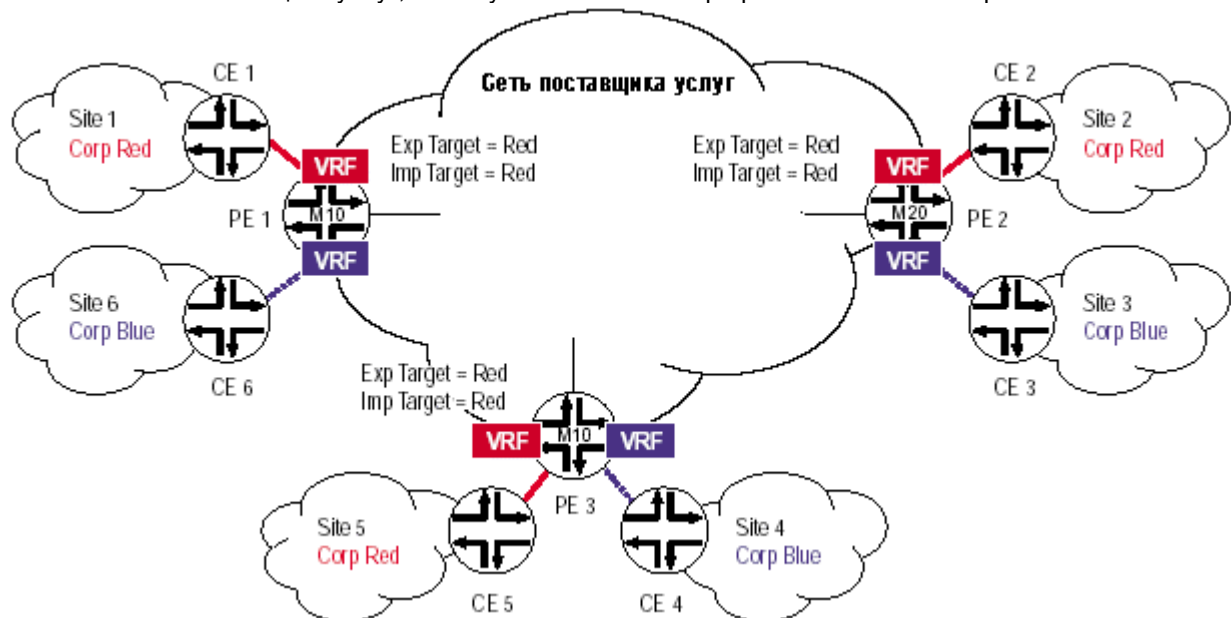


Рисунок 7. Полносвязная ВЧС

Каждый сайт Corporation Red ассоциируется с красной таблицей VRF на своем маршрутизаторе PE. Единственная глобально уникальная цель маршрута (Red) конфигурируется для каждой красной VRF как

цель импорта или экспорта. Эта цель маршрута (Red) больше не ассоциирована ни с какой другой VRF. В результате обеспечивается полная связь между сайтами Corporation Red.

Пример 2. Звездообразная топология ВЧС

Допустим, Corporation Red дает поручение поставщику услуг ВЧС BGP/MPLS на создание ВЧС по звездообразной топологии (рис. 8). Связь между сайтами Corporation Red можно описать нижеследующими правилами.

- Сайт 1 может связываться напрямую с сайтом 5, но не с сайтом 2. Если сайт 1 хочет связаться с сайтом 2, он должен отправлять трафик через сайт 5.
- Сайт 2 может связываться напрямую с сайтом 5, но не с сайтом 1. Если сайт 2 хочет связаться с сайтом 1, он должен отправить трафик через сайт 5.
- Сайт 5 может связываться напрямую с сайтами 1 и 2. При этом конфиденциальность требует, чтобы сайты Corporation Red и Corporation Blue не могли обмениваться трафиком друг с другом.

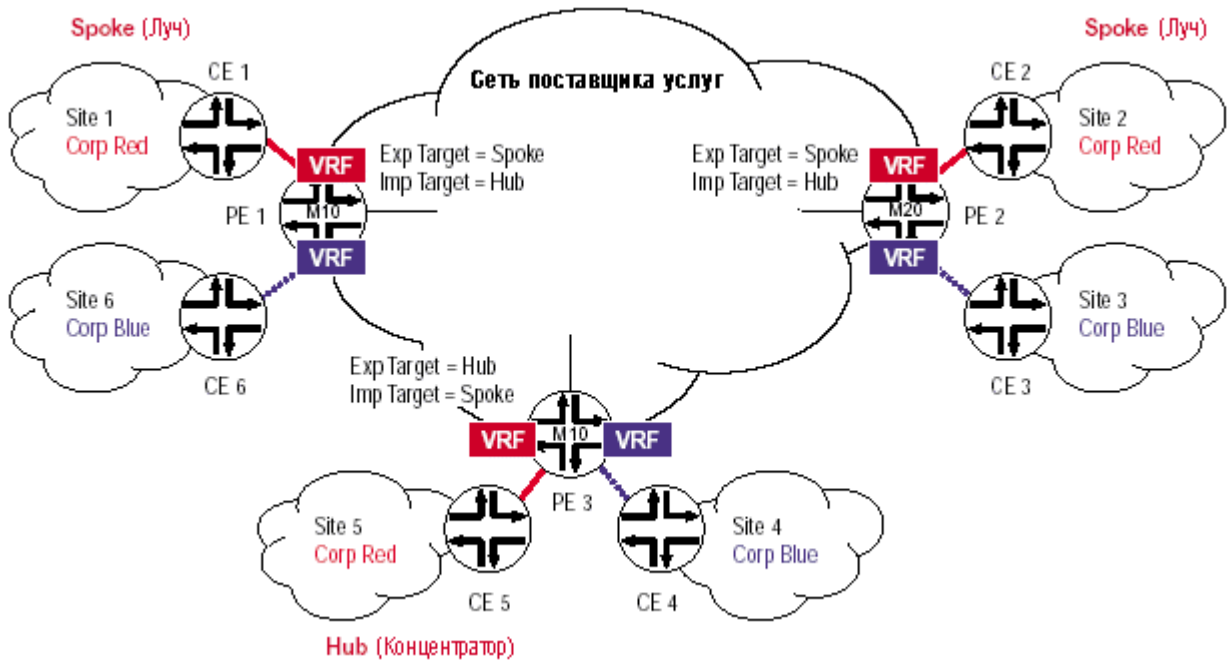


Рисунок 8. ВЧС со звездообразной топологией

Звездообразная топология создается с использованием двух глобально уникальных значений целей маршрута: центр, или концентратор (hub) и луч (spoke).

- Таблица VRF центрального сайта (концентратора) конфигурируется с атрибутами *export target = hub* и *import target = spoke*. VRF на сайте концентратора распространяет все маршруты в VRF с атрибутом концентратора, что заставляет сайты с атрибутом *spoke* импортировать их. VRF на сайте концентратора импортирует все удаленные маршруты с атрибутами *spoke*.
- VRF на каждом сайте луча конфигурируется с атрибутами *export target = spoke* и *import target = hub*. VRF на каждом сайте луча распространяет маршруты с атрибутом луча, который обуславливает их импорт сайтом концентратора и отбрасывание - другими сайтами лучей. VRF на сайте луча импортирует только маршруты с атрибутом концентратора, в результате VRF сайта будет заполняться только маршрутами, о которых оповестил сайт концентратора.

Обновление маршрутной информации ВЧС.

Когда конфигурация маршрутизатора PE изменяется вследствие создания новой таблицы VRF или из-за добавления одного или более правил импорта цели к существующей VRF, маршрутизатору PE могут потребоваться маршруты VPN-IPv4, которые были первоначально отброшены. Скорость доставки обновленной маршрутной информации может при стандартном BGP4 оказаться недопустимо малой, так как это протокол режима *stateful*, не поддерживающий обмен сообщениями об обновлении маршрута с последующим объявлением новых маршрутов. После синхронизации маршрутизаторами BGP своих таблиц маршрутизации, они перестают обмениваться маршрутной информацией вплоть до изменения в этой маршрутной информации.

Решением этой проблемы является возможность обновления маршрута BGP. Во время установления сессии MP-IBGP вещатель BGP, который хочет принять сообщение об обновлении маршрута от соответствующего маршрутизатора (реер) или рефлектора маршрута, объявляет о возможности обновления маршрута BGP. Возможность обновления маршрута BGP гласит, что вещатель BGP может отправлять сообщение маршрута только тогда, когда он принял объявление о возможности обновления маршрута от соответствующего реер-маршрутизатора или рефлектора маршрута. Всякий раз, когда конфигурация маршрутизатора PE изменяется, маршрутизатор PE может запрашивать повторную передачу маршрутной информации от маршрутизаторов MP-IBGP своего уровня для получения ранее отброшенной маршрутной информации. После повторного объявления маршрутов при заполнении маршрутизатором PE своих таблиц VRF применяется обновленное правило импорта цели.

Экономия полосы пропускания магистрали и ресурсов пакетной обработки маршрутизатора PE.

В ходе заполнения своих таблиц VRF, вещатель BGP часто принимает и затем отфильтровывает нежелательные маршруты на основе правил импорта цели таблиц VRF. Так как генерация, передача и обработка обновлений маршрута приводит к расходу полосы пропускания и ресурсов обработки пакетов маршрутизатора, эти ресурсы можно экономить за счет устранения передачи ненужных обновлений маршрутной информации.

Количество обновлений маршрутной информации можно снизить за счет новой возможности кооперативной фильтрации маршрута. В ходе установления сессии MP-IBGP вещатель BGP, желающий обменяться внешними фильтрами маршрута (ORF) с рефлектором маршрута либо реер-маршрутизатором, объявляет по протоколу BGP о возможности кооперативной фильтрации. Вещатель BGP посылает своему реер-маршрутизатору множество фильтров ORF, которые составлены в терминах сообщества BGP. Фильтры ORF транспортируются в сообщениях обновления маршрута BGP. Реер-маршрутизатор применяет принятые фильтры ORF в дополнение к его локально сконфигурированному правилу экспорта цели для ограничения и фильтрации внешних обновлений маршрутной информации в направлении к вещателю BGP. Заметим, что реер-маршрутизатор BGP может принять или не принять фильтры ORF от вещателя BGP. С помощью этого механизма фильтрация кооперативного маршрута BGP может использоваться для экономии полосы пропускания магистрали поставщика услуг и ресурсов пакетной обработки маршрутизатора PE.

Пример единой магистрали поставщика услуг

Допустим, поставщик услуг имеет IP-магистраль для предоставления услуг ВЧС BGP/MPLS различным предприятиям. Пусть в сети имеется три маршрутизатора PE, подключенных к семи различным клиентским сайтам. (рис. 9).

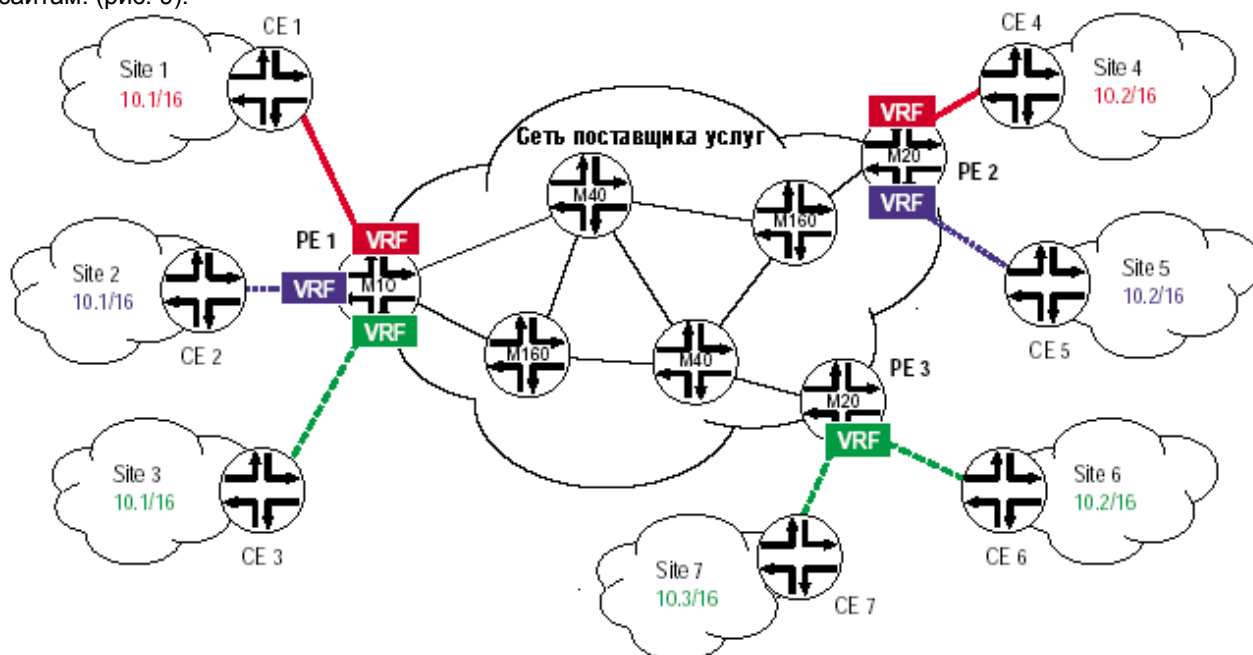


Рисунок 9. Пример сетевой топологии

Желаемые связи между сайтами задаются следующими правилами:

- Любой хост сайта 1 может связываться с любым хостом сайта 4.
- Любой хост сайта 2 может связываться с любым хостом сайта 5.
- Любой хост сайта 3 может связываться с любым хостом на сайтах 6 и 7.
- Любой хост сайта 4 может связываться с любым хостом сайта 1.
- Любой хост сайта 5 может связываться с любым хостом сайта 2.
- Любой хост сайта 6 может связываться с любым хостом на сайтах 3 и 7.
- Любой хост сайта 7 может связываться с любым хостом сайта 3 и сайта 6.

Допустим, поставщик услуг использует для прокладки показанных ниже путей LSP протокол RSVP (рис. 10). Метка, показанная на входе каждого LSP, является меткой, которую маршрутизатор PE ассоциирует с маршрутом, используемым для продвижения трафика к удаленному маршрутизатору PE. Заметим, что если поставщик услуг использует для прокладки путей LSP протокол LDP, то LSP будут путями типа точка-многоточка, а не точка-точка. Общая конфигурация для PE 1 показана на рис. 11, для PE 2 - на рис. 12, для PE 3 - на рис. 13

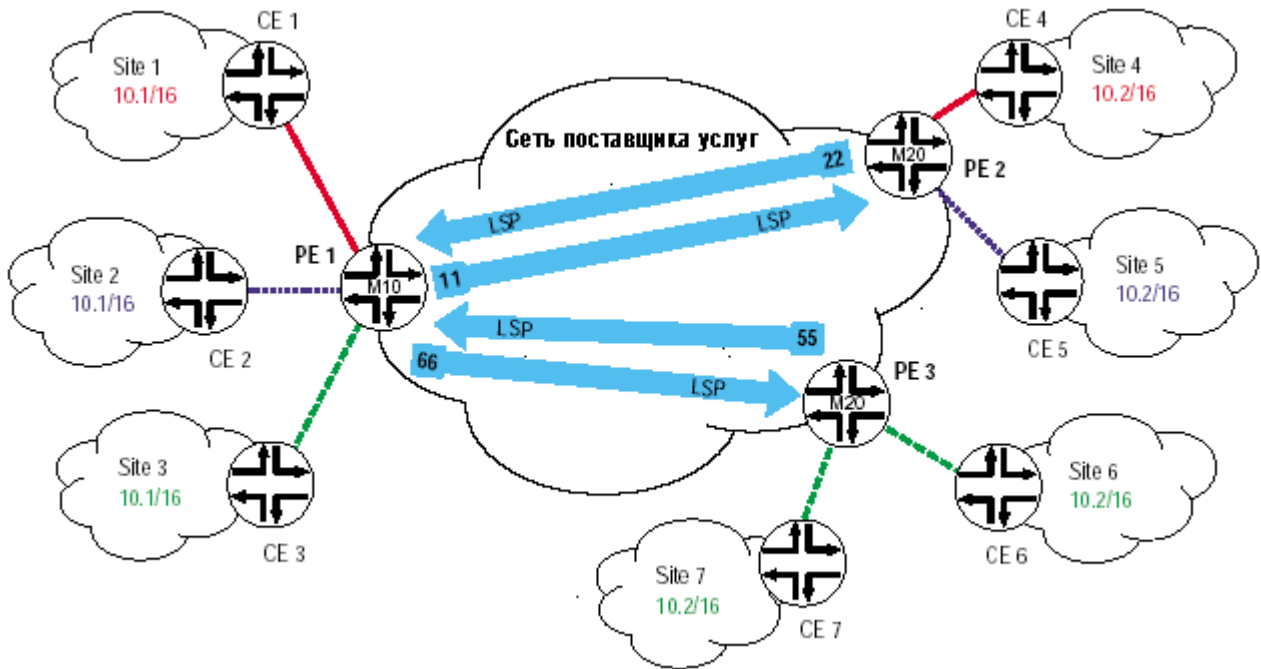


Рисунок 10. Пути коммутации меток

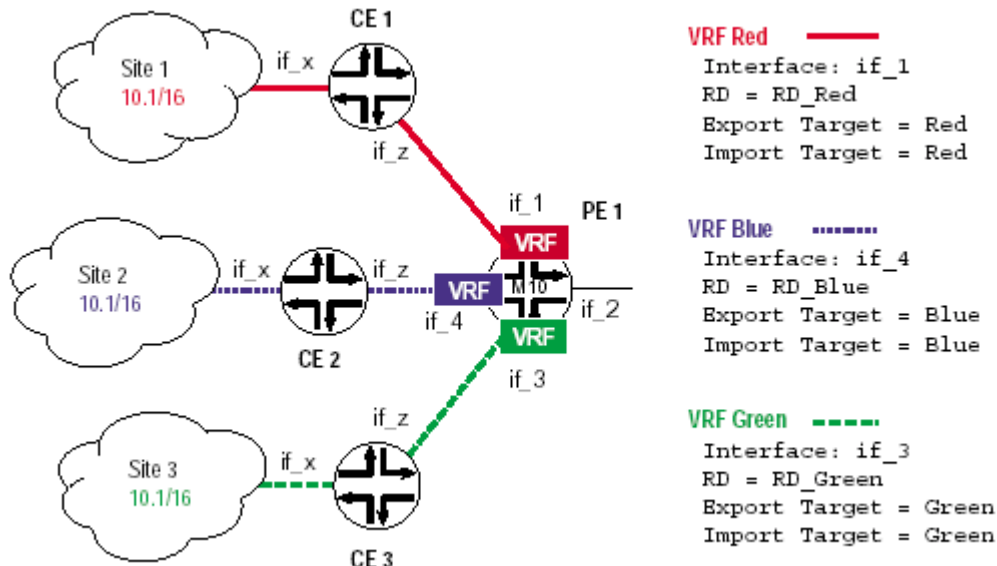


Рисунок 11. Общая конфигурация для PE 1

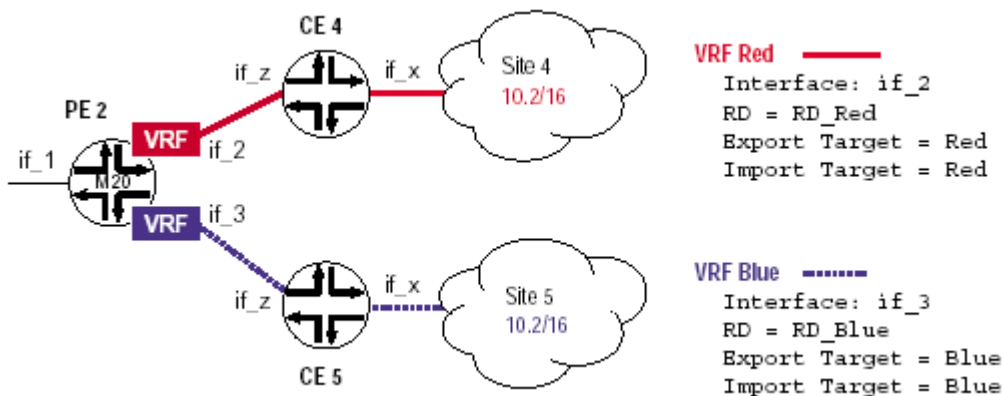


Рисунок 12. Общая конфигурация для PE 2

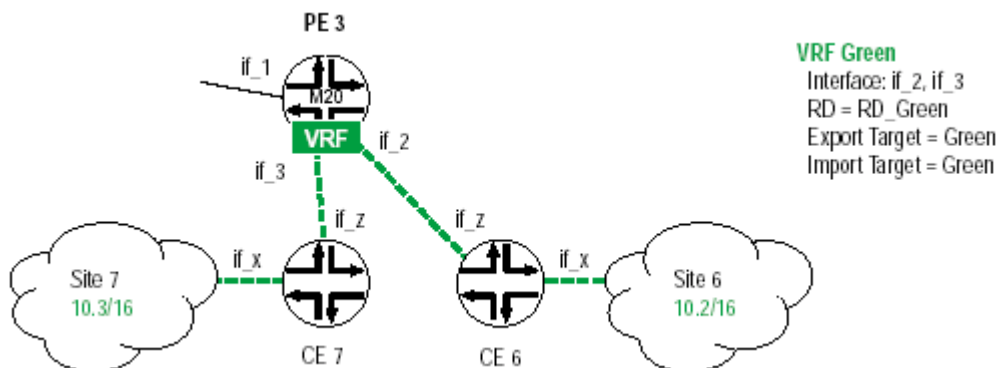


Рисунок 13. Общая конфигурация для PE 3

Распространение маршрутной информации ВЧС

Перед тем как сайт клиента сможет направить трафик ВЧС к удаленному сайту, маршрутная информация ВЧС должна быть распространена от каждого сайта клиента через магистраль к другим сайтам клиентов.

Распространение на участке от маршрутизатора CE до входного маршрутизатора PE

Маршрутизатор CE объявляет префиксы маршрута IPv4 для своего маршрутизатора PE. Существует несколько механизмов, которые маршрутизатор PE использует, чтобы узнать маршруты от каждого из непосредственно подключенных маршрутизаторов CE.

- Статическая маршрутизация
- Выполнение протокола IGP (RIPv2, OSPF) на маршрутизаторе CE
- Установление соединения EBGP с маршрутизатором CE

В потоке маршрутной информации от CE к входу PE маршрутизатор PE выполняет ряд функций. Он создает и хранит VRF для каждого из непосредственно подключенных к нему сайтов. В нашем примере PE 3 сконфигурирован для ассоциирования множества сайтов (6 и 7) с единственной таблицей VRF.

PE проверяет все маршруты на соответствие локально сконфигурированным правилам импорта для протокола маршрутизации, функционирующего между PE и CE. Если маршрут удовлетворяет правилу импорта, префикс встраивается в таблицу VRF как маршрут IPv4. PE должен быть предотвратит попадание маршрутов, о которых он узнал от каждого всех CE (по соединению IGP), в магистраль IGP поставщика услуг.

До объявления маршрута PE присваивает ему метку MPLS.

- Если маршрут получен по каналу точка-точка, метка присваивается на основе входного логического интерфейса. В случае канала точка-точка всем маршрутам присваивается одна и та же метка.

- Если маршрут получен по интерфейсу разделяемой среды, такому как Fast Ethernet, метка присваивается по конкретному маршрутизатору CE, который объявил префикс. На интерфейсе разделяемой среды всем маршрутам, полученным от данного маршрутизатора CE, присваиваются одна метка, а всем маршрутам, полученным от другого маршрутизатора CE, - другая.

Маршрутизатор PE 1

Допустим, маршрутизатор PE 1 присваивает метку 1001 маршрутам, полученным от сайта 1, метку 1002 - маршрутам, полученным от сайта 2, метку 1003 - маршрутам, полученным от сайта 3. PE 1 устанавливает три маршрута MPLS, таким образом, что когда пакет с метками 1001, 1002 или 1003 принимается от магистрали, он просто выталкивает метку и продвигает пакет IPv4 непосредственно к CE 1, CE 2 или CE 3, в зависимости от метки пакета.

Таблица форвардинга MPLS (PE 1)

Input			Output
Interface	Label	Action	Interface
If_2	1001	Pop	if_1
If_2	1002	Pop	if_4
If_2	1003	Pop	if_3

В результате, таблицы VRF маршрутизатора PE 1 будут содержать следующие локальные маршруты.

VRF Red

Destination	BGP	Interface	Bottom	Top
	Next-Hop		Label	Label
10.1/16	Direct	if_1	1001	-

VRF Blue

Destination	BGP	Interface	Bottom	Top
	Next-Hop		Label	Label
10.1/16	Direct	if_4	1002	-

VRF Green

Destination	BGP	Interface	Bottom	Top
	Next-Hop		Label	Label
10.1/16	Direct	if_3	1003	-

Маршрутизатор PE 2

Допустим, что PE 2 присваивает метку 1004 маршрутам, полученным от сайта 4, и метку 1005 - маршрутам, полученным от сайта 5. PE 2 устанавливает два маршрута MPLS таким образом, что когда пакет с меткой 1004 или 1005 принимается от магистрали, он просто выталкивает метку и отправляет пакет IPv4 непосредственно на CE 4 или CE 5, в зависимости от метки пакета.

Таблица форвардинга MPLS (PE 2)

Input			Output
Interface	Label	Action	Interface
If_1	1004	Pop	if_2
If_1	1005	Pop	if_3

В результате этих операций таблицы VRF на PE 2 будут содержать следующие локальные маршруты.

VRF Red

Destination	BGP	Interface	Bottom	Top
	Next-Hop		Label	Label
10.2/16	Direct	if_2	1004	-

VRF Blue

Destination	BGP	Interface	Bottom	Top
	Next-Hop		Label	Label
10.2/16	Direct	if_3	1005	-

Маршрутизатор PE 3

Допустим, что PE 3 присваивает метку 1006 маршрутам, полученным от сайта 6, и метку 1007 – маршрутам, полученным от сайта 7. PE 3 устанавливает два маршрута MPLS таким образом, что когда пакет с меткой 1006 или 1007 принимается от магистрали, он просто выталкивает метку и продвигает пакет IPv4 непосредственно к CE6 или CE 7, в зависимости от метки пакета.

MPLS Forwarding Table (PE 3)

Input			Output	
Interface	Label	Action	Interface	
If_1	1006	Pop	if_2	
If_1	1007	Pop	if_3	

В результате выполнения этих операций таблица VRF Green на PE 3 будет содержать следующие локальные маршруты.

VRF Green

Destination	BGP		Bottom	Top
	Next-Hop	Interface	Label	Label
10.2/16	Direct	if_2	1006	-
10.3/16	Direct	if_3	1007	-

Распространение маршрутов по магистрали от входного PE к выходному PE

Для распространения маршрутов, принятых от сайтов, непосредственно подключенных к выходным маршрутизаторам PE, входные маршрутизаторы PE используют протокол MP-IBGP. Маршрутизаторы PE должны поддерживать сеть MP-IBGP или использовать рефлекторы маршрута для гарантированного распространения маршрутной информации ко всем маршрутизаторам PE.

Перед тем как входной маршрутизатор PE распространяет маршруты локальной ВЧС своим реер-маршрутизаторам MP-IBGP, он конвертирует каждый префикс IPv4 в префикс VPN-IPv4, используя RD, сконфигурированные для таблицы VRF, содержащей маршрут. Объявления для каждого маршрута содержат следующую информацию.

- Префикс адреса VPN-IPv4 для маршрута.
- Следующий транзит BGP, который содержит адрес обратной связи входного маршрутизатора PE. Адрес кодируется как адрес VPN-IPv4 с $RD = 0$, так как MP-BGP требует, чтобы следующий участок входил в то же семейство адресов, что и объявляемый маршрут.
- Метка MPLS, которая была присвоена маршруту входящим маршрутизатором PE, когда он узнавал локальный маршрут от непосредственно подключенного маршрутизатора CE.
- Атрибут цели маршрута, основанный на локально сконфигурированном правиле экспорта цели для таблицы VRF, содержащей локальный маршрут. Вспомним, что все маршрутизаторы PE в этом примере были сконфигурированы с атрибутом *route target = Red* при объявлении маршрутов красной ВЧС, *route target = Blue* - при объявлении маршрутов синей ВЧС и *route target = Green* при объявлении маршрутов зеленой ВЧС.

Как вариант, атрибут сайта-источника может кодироваться как источник маршрута расширенного сообщества.

Когда входной PE маршрутизатор объявляет свои локальные VPN-IPv4 маршруты реер-маршрутизаторам MP-IBGP, он может либо отправить все маршруты таблиц VRF всем реер-маршрутизаторам, либо сконструировать различные объявления для каждого реер-маршрутизатора, исключая те маршруты, которые с данным реер-маршрутизатором не разделяются. Это выполняется за счет использования фильтров ORF, позволяющих вещателю BGP сообщать своему реер-маршрутизатору или рефлектору маршрута то множество маршрутов, которое можно импортировать в одну или несколько таблиц VRF, поддерживаемых маршрутизатором PE.

Когда выходной маршрутизатор PE принимает маршрут VPN-IPv4 от реер-маршрутизатора, он сравнивает маршрут со всеми правилами импорта таблиц VRF для всех ВЧС, которые непосредственно подключены к выходному маршрутизатору PE. Если цель маршрута, транспортированная с маршрутом, соответствует правилам импорта цели по крайней мере в одной из таблиц VRF выходного PE, маршрут VPN-IPv4 встраивается в его таблицу VPN_IPv4.RIB.

Таблица VPN_IPv4.RIB - большая база маршрутной информации (RIB), которая содержит все маршруты, удовлетворяющие правилам импорта по крайней мере одной из таблиц выходного маршрутизатора PE. Эта таблица является единственной, использующей RD для устранения противоречий маршрутов, так как только в ней содержатся все маршруты от всех ВЧС, непосредственно подключенных к данному маршрутизатору PE. Маршруты в этой таблице должны быть глобально уникальными, так как перекрывающимся адресам IPv4 будут присвоены глобально уникальные RD.

Выбор пути BGP в этой таблице происходит до экспорта маршрутов в целевую таблицу VRF. Заметим, что ошибки пользователя при конфигурировании RD могут привести к наличию одинаковых маршрутов VPN-IPv4, тогда как они должны различаться. Если так случится, то выполняется выбор пути BGP, и только один из этих маршрутов устанавливается в таблицу VRF. По этой причине, RFC 2547bis рекомендует провайдером использовать глобально уникальные ASN и адреса IPv4 при определении RD, что критично, если ВЧС BGP/MPLS совместно используется несколькими поставщиками услуг. Для каждого префикса VPN-IPv4 выбирается наилучший маршрут и на основании цели маршрута, хранимой вместе с маршрутом, встраивается в целевую таблицу VRF как маршрут IPv4.

Объявления входного PE маршрута

В этом разделе рассматривается, как входные маршрутизаторы PE объявляют локальные маршруты выходным маршрутизаторам PE по магистрали поставщика услуг.

Объявления маршрута PE 1

PE 1 объявляет всем своим реер-маршрутизаторам MP-IBGP следующие маршруты.

```
Destination = RD_Red:10.1/16  
Label = 1001  
BGP Next Hop = PE 1  
Route Target = Red
```

```
Destination = RD_Blue:10.1/16  
Label = 1002  
BGP Next Hop = PE 1  
Route Target = Blue
```

```
Destination = RD_Green:10.1/16  
Label = 1003  
BGP Next Hop = PE 1  
Route Target = Green
```

Объявления маршрута PE 2

PE 2 объявляет всем своим реер-маршрутизаторам MP-IBGP следующие маршруты.

```
Destination = RD_Red:10.2/16  
Label = 1004  
BGP Next Hop = PE 2  
Route Target = Red
```

```
Destination = RD_Blue:10.2/16  
Label = 1005  
BGP Next Hop = PE 2  
Route Target = Blue
```

Объявления маршрута PE 3

PE 3 объявляет всем своим реер-маршрутизаторам MP-IBGP следующие маршруты.

```
Destination = RD_Green:10.2/16  
Label = 1006  
BGP Next Hop = PE 3  
Route Target = Green
```

```
Destination = RD_Green:10.3/16  
Label = 1007  
BGP Next Hop = PE 3  
Route Target = Green
```

Установка выходного маршрута PE

В этом разделе показано, как выходные маршрутизаторы PE фильтруют и затем устанавливают удаленные маршруты, принятые от входных маршрутизаторов PE.

Установка маршрута PE 1

PE 1 устанавливает следующий маршрут от PE 2 в красную таблицу VRF Red.

```
Destination = RD_Red:10.2/16
Label = 1004
BGP Next Hop = PE 2
Route Target = Red
```

PE 1 устанавливает следующий маршрут от PE 2 в синюю таблицу VRF Blue.

```
Destination = RD_Blue:10.2/16
Label = 1005
BGP Next Hop = PE 2
Route Target = Blue
```

PE 1 устанавливает следующие маршруты от PE 3 в зеленую таблицу VRF Green.

```
Destination = RD_Green:10.2/16
Label = 1006
BGP Next Hop = PE 3
Route Target = Green
```

```
Destination = RD_Green:10.3/16
Label = 1007
BGP Next Hop = PE 3
Route Target = Green
```

После обмена всеми маршрутами содержимое таблиц VRF примет следующий вид:

VRF Red

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1/16	Direct	if_1	1001	-
10.2/16	PE-2	if_2	1004	11

VRF Blue

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1/16	Direct	if_4	1002	-
10.2/16	PE-2	if_2	1005	11

VRF Green

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1/16	Direct	if_3	1003	-
10.2/16	PE-3	if_2	1006	11
10.3/16	PE-3	if_2	1007	66

Установка маршрута PE 2

PE 2 устанавливает следующий маршрут от PE 1 в красную таблицу VRF Red.

```
Destination = RD_Red:10.1/16
Label = 1001
BGP Next Hop = PE 1
Route Target = Red
```

PE 2 устанавливает следующий маршрут от PE 1 в синюю таблицу VRF Blue.

```
Destination = RS_Blue:10.1/16
Label = 1002
BGP Next Hop = PE 1
Route Target = Blue
```

После обмена всеми маршрутами содержимое таблиц VRF PE 2 примет следующий вид:
VRF Red

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1/16	PE-1	if_1	1001	22
10.2/16	Direct	if_2	1004	-

VRF Blue

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1/16	PE 1	if_1	1002	22
10.2/16	Direct	if_2	1005	-

Установка маршрута PE 3

PE 3 устанавливает следующий маршрут от PE 1 в зеленую таблицу VRF Green.

```
Destination = RD_Green:10.1/16
Label = 1003
BGP Next Hop = PE 1
Route Target = Green
```

После обмена всеми маршрутами содержимое таблиц VRF PE 3 примет следующий вид:
VRF Green

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1/16	PE-1	if_1	1003	55
10.2/16	Direct	if_2	1006	-
10.3/16	Direct	if_3	1007	-

Распространение маршрута от выходного маршрутизатора PE к CE

Если выходной маршрутизатор PE устанавливает маршрут в таблицу VRF, используемую для маршрутизации пакетов, принятых от непосредственно подключенного маршрутизатора CE, маршрутизатор PE может распространять этот маршрут к маршрутизатору CE. Есть несколько механизмов, которые маршрутизатор CE может использовать для получения маршрутов ВЧС от своего непосредственно подключенного маршрутизатора PE.

- Выполнение протокола IGP (RIPv2, OSPF) на маршрутизаторе PE.
- Установление соединения EBGP с маршрутизатором PE.

Альтернативой являются следующие действия маршрутизатора PE.

- Протокол маршрутизации PE-CE может распространять маршрут по умолчанию, указывающий на маршрутизатор PE.
- CE может быть сконфигурирован со статическим маршрутом по умолчанию, указывающим на маршрутизатор PE.

После того как все маршруты распространились от выходных маршрутизаторов PE к маршрутизаторам CE, таблицы маршрутизации CE будут содержать следующую информацию.

```
CE 1 Routing Table
Destination      Next-Hop      Interface
10.1/16          Direct        if_x
10.2/16          PE 1          if_z
```

```
CE 2 Routing Table
Destination      Next-Hop      Interface
10.1/16          Direct        if_x
10.2/16          PE 1          if_z
```

```
CE 3 Routing Table
Destination      Next-Hop      Interface
10.1/16          Direct        if_x
10.2/16          PE 1          if_z
10.3/16          PE 1          if_z
```

```
CE 4 Routing Table
Destination      Next-Hop      Interface
10.1/16          PE 2          if_z
10.2/16          Direct        if_x
```

```
CE 5 Routing Table
Destination      Next-Hop      Interface
10.1/16          PE 2          if_z
10.2/16          Direct        if_x
```

```
CE 6 Routing Table
Destination      Next-Hop      Interface
10.1/16          PE 3          if_z
10.2/16          Direct        if_x
10.3/16          PE 3          if_z
```

```
CE 7 Routing Table
Destination      Next-Hop      Interface
10.1/16          PE 3          if_z
10.2/16          PE 3          if_z
10.3/16          Direct        if_x
```

Продвижение трафика клиента ВЧС через магистраль BGP/MPLS

При передаче трафика клиента от одного сайта ВЧС на другой сайт ВЧС принимаются различные решения.

- Решение форвардинга маршрутизатора CE источника до входного маршрутизатора PE.
- Решение форвардинга входного маршрутизатора PE
- Решение форвардинга на каждом маршрутизаторе P
- Решение форвардинга от выходного маршрутизатора PE до маршрутизатора CE назначения.

Форвардинг от маршрутизатора CE источника до входного маршрутизатора PE

Когда маршрутизатор CE принимает исходящий пакет данных IPv4 от системы на своем сайте, он выполняет традиционный поиск самого длинного согласующегося маршрута и продвигает пакет IPv4 к непосредственно подключенному маршрутизатору PE.

Форвардинг входного маршрутизатора PE

Когда маршрутизатор PE принимает пакет IPv4 от маршрутизатора CE, маршрутизатор PE производит поиск маршрута в таблице VRF для сайта на основе входного субинтерфейса пакета. Проверяется согласование адреса назначения пакета с префиксом IPv4. Если совпадение найдено, алгоритм поиска маршрута возвращает следующий транзит и исходящий субинтерфейс.

Если выходной субинтерфейс пакета ассоциирован с той же таблицей VRF, что и входящий пакет, то следующий транзит - это либо другое устройство CE на том же сайте, либо CE от другого непосредственно подключенного сайта, являющегося членом той же самой ВЧС. Вспомним, что единственная таблица VRF маршрутизатора PE обслуживает маршруты от всех непосредственно подключенных сайтов данной ВЧС.

Если выходной и входной субинтерфейсы пакета ассоциированы с разными таблицами VRF, то они являются непосредственно подключенными сайтами, которые имеют по крайней мере одну общую ВЧС, и каждый сайт имеет отдельную таблицу форвардинга. Для продвижения пакета необходимо отыскать адрес назначения пакета в VRF, ассоциированной с выходным интерфейсом.

Если выходной субинтерфейс пакета не ассоциирован с VRF, то пакет должен пройти по крайней мере один транзит по магистрали поставщика услуг, чтобы достичь удаленного маршрутизатора PE. Если пакет должен пересечь магистраль поставщика услуг, то ему предстоит пройти еще два транзита: следующий транзит BGP и следующий транзит IGP.

- Следующим транзитом BGP является входной маршрутизатор PE, который изначально объявил маршрут VPN-IPv4. Он присваивает и распространяет метку с маршрутом посредством MP-IBGP, которую он впоследствии использует для идентификации непосредственно подключенного сайта, который объявил маршрут. Маршрутизатор PE втапливает эту метку в стек меток пакета, и она становится нижней (внутренней) меткой.
- Следующий транзит IGP - это первый транзит в пути LPS к следующему транзиту BGP. Следующий участок IGP будет иметь метку, присвоенную по LDP или RSVP, для пути LSP, который приводит к маршрутизатору BGP следующего транзита. Эта метка втапливается в стек меток пакета и становится верхней (внешней) меткой.

Для рассматриваемого случая маршрутизатор PE, который принимает пакет от CE и создает стек меток, является входным LSR, и следующий транзит BGP – это выходной LSR для пути LSP через сеть поставщика услуг. Если следующий транзит BGP и следующий транзит IGP – это один и тот же маршрутизатор, и если метка выталкивалась на предпоследнем транзите, то пакет может передаваться только с одной нижней (внутренней) меткой BGP.

Форвардинг маршрутизатора P

Магистраль MPLS коммутирует пакет с меткой, меняя верхнюю метку на каждом транзите до тех пор, пока не достигает предпоследнего маршрутизатора перед маршрутизатором PE, к которому отправлен пакет. На предпоследнем маршрутизаторе верхняя метка выталкивается, и пакет отправляется к маршрутизатору PE цели.

Форвардинг от маршрутизатора PE к маршрутизатору CE назначения

Когда маршрутизатор PE принимает пакет, он ищет согласующийся маршрут MPLS (метку, субинтерфейс) для нижней метки. Если есть совпадение, нижняя метка выталкивается, и исходный пакет IPv4

отправляется непосредственно на маршрутизатор CE, ассоциированный с меткой. Заметим, что таблица VRF для непосредственно подключенного сайта при этом не просматривается.

Пример 1. Форвардинг трафика красной ВЧС с сайта 1 на сайт 4

Допустим, что хост 10.1.2.3 на сайте 1 хочет передать пакет на сервер 10.2.9.3 на сайте 4 (рис. 14).

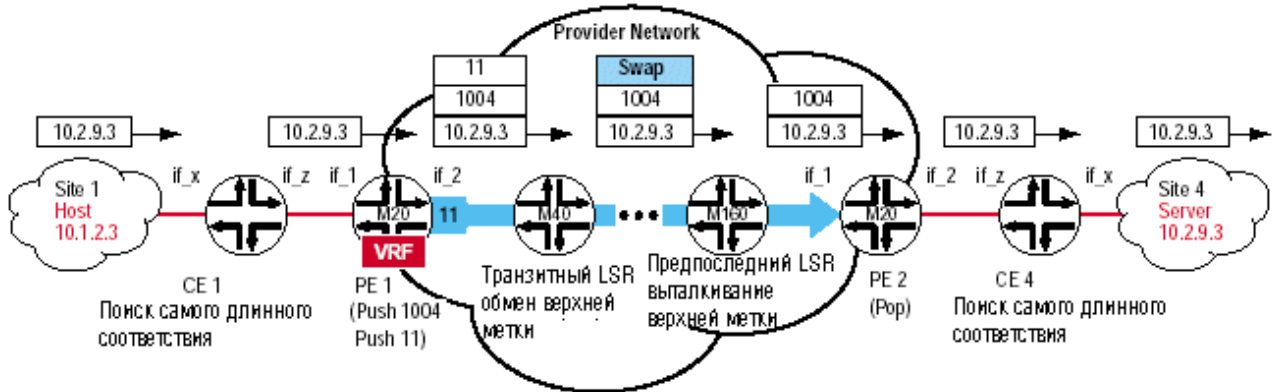


Рисунок 14. Форвардинг трафика красной ВЧС с сайта 1 на сайт 4

Когда стандартный пакет IPv4 поступает на CE 1, последний производит поиск самого длинного согласующегося пути в IP таблице форвардинга:

Destination	Next-Hop	Interface
10.2/16	PE 1	if_z

В результате поиска CE 1 продвигает стандартный пакет IPv4 на if_z к PE 1.

PE 1 принимает исходный пакет IPv4 на if_1. Так как все пакеты, которые поступили на if_1, ассоциированы с красной таблицей VRF Red, PE 1 производит поиск самого длинного согласующегося маршрута в таблице VRF Red. Адрес в таблице VRF Red, который наилучшим образом согласуется с адресом назначения:

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.2/16	PE 2	if_2	1004	11

Так как выходной субинтерфейс пакетов (if_2) не ассоциирован с локальной таблицей VRF, пакет должен пройти по крайней мере один транзит по магистрали MPLS поставщика услуг. PE 1 создает заголовок MPLS для пакета и затем помещает метку 1004 (присвоенную на PE 2, когда он изначально объявил маршрут к 10.2/16) в стек меток пакета, делая ее нижней меткой. Затем PE 1 помещает первую метку (11) для пути LSP от PE 1 к PE 2 в стек меток пакета, делая ее верхней меткой.

Затем пакет продвигается к первому транзитному маршрутизатору на пути LSP от PE 1 к PE 2. Магистраль MPLS коммутрует пакет с меткой в соответствии с LSP, меняя верхнюю метку на каждом транзите, до тех пор пока пакет не достигнет предпоследнего по отношению к PE 2 маршрутизатора. На предпоследнем маршрутизаторе верхняя метка выталкивается, и пакет с единственной меткой (1004) отправляется к PE 2. Когда PE 2 принимает пакет с меткой на интерфейс if_1, он производит поиск точного соответствия в своей таблице форвардинга MPLS. Адрес в таблице форвардинга MPLS, который соответствует метке пакета:

Input Interface	Label	Action	Output Interface
if_1	1004	Pop	if_2

В результате этого поиска PE 2 выталкивает метку и продвигает стандартный пакет IPv4 по интерфейсу if_2 к CE 4.

Когда стандартный пакет IPv4 поступает на CE 4, производится поиск самого длинного согласующегося маршрута в таблице IP форвардинга CE 4. Адрес в таблице форвардинга CE 4, который соответствует адресу назначения пакета:

```
Destination  Next-Hop      Interface
10.2/16      Direct        if_x
```

В результате этого поиска CE 4 продвигает пакет через интерфейс if_x к серверу 10.2.9.3 на сайте 4.

Пример 2. Форвардинг трафика красной ВЧС от сайта 4 к сайту 1

Допустим, что сервер 10.2.9.3 на сайте 4 хочет передать ответный пакет к хосту 10.1.2.3 на сайте 1 (рис. 15).

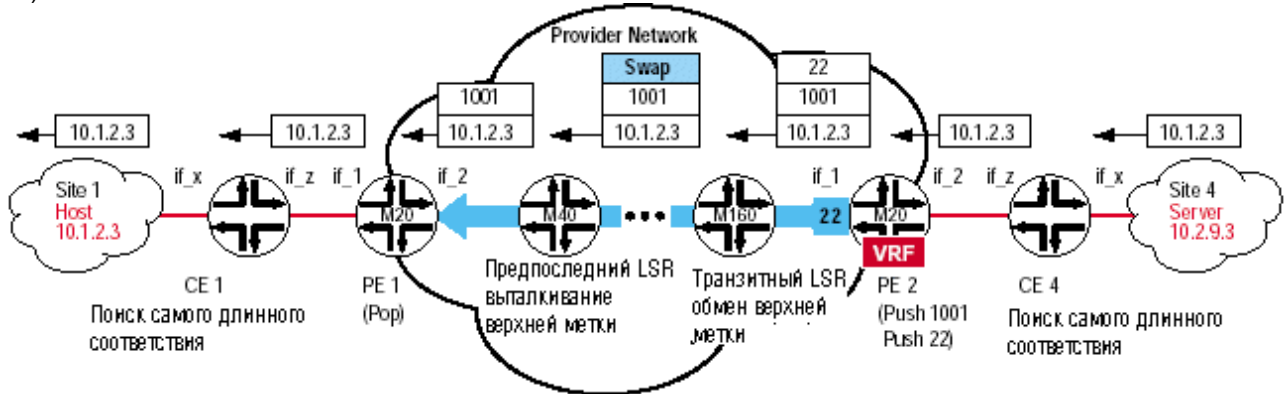


Рисунок 15. Форвардинг трафика красной ВЧС от сайта 4 на сайт 1

Когда стандартный пакет IPv4 поступает на CE 4, производится поиск самого длинного согласующегося маршрута в IP таблице форвардинга CE 4. Адрес таблицы форвардинга CE 4, соответствующий адресу назначения пакета:

```
Destination  Next-Hop      Interface
10.1/16      PE 2          if_z
```

В результате этого поиска CE 4 продвигает стандартный пакет IPv4 к PE 2. PE 2 принимает стандартный пакет IPv4 на интерфейс if_2. Так как все пакеты, которые прибывают на if_2, ассоциированы с красной таблицей VRF Red, PE 2 производит поиск самого длинного согласующегося маршрута в таблице VRF Red, получая следующее соответствие:

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1/16	PE 1	if_1	1001	22

Так как выходной субинтерфейс пакета (if_1) не ассоциирован с локальной таблицей VRF, пакет должен пройти по крайней мере один транзит по MPLS магистрали поставщика услуг. PE 2 создает заголовок MPLS для пакета и затем помещает метку 1001 (присвоенную на PE 1, когда он изначально объявил маршрут к 10.1/16) в стек меток пакета, делая ее нижней меткой. PE 2 затем помещает первую метку (22) для пути LSP от PE 2 к PE 1 в стек меток пакета, делая ее верхней меткой.

Затем пакет продвигается к первому транзитному маршрутизатору на пути LSP от PE 2 к PE 1. Магистраль MPLS коммутирует пакет с меткой вдоль LSP, меняя верхнюю метку на каждом транзите до тех пор, пока пакет не достигнет предпоследнего относительно PE 1 маршрутизатора. На предпоследнем маршрутизаторе, верхняя метка выталкивается, и пакет с единственной меткой (1001) отправляется к PE 1.

Когда PE 1 принимает пакет с меткой на интерфейс if_2, он производит поиск точного согласования в своей таблице форвардинга MPLS., получая следующее соответствие:

Input Interface	Label	Action	Output Interface
if_2	1001	Pop	if_1

В результате этого поиска PE 1 выталкивает метку и продвигает стандартный пакет IPv4 по if_1 к CE 1.

Когда стандартный пакет IPv4 поступает на CE 1, производится поиск самого длинного согласующегося маршрута со следующим результатом:

Destination	Next-Hop	Interface
10.1/16	Direct	if_x

В результате этого поиска CE 1 продвигает пакет через интерфейс if_x к хосту 10.1.2.3 на сайте 1.

Пример 3. Форвардинг трафика зеленой ВЧС от сайта 6 на сайт 7

Допустим, хост 10.2.3.4 на сайте 6 хочет передать пакет на хост 10.3.2.5 на сайте 7 (рис. 16).

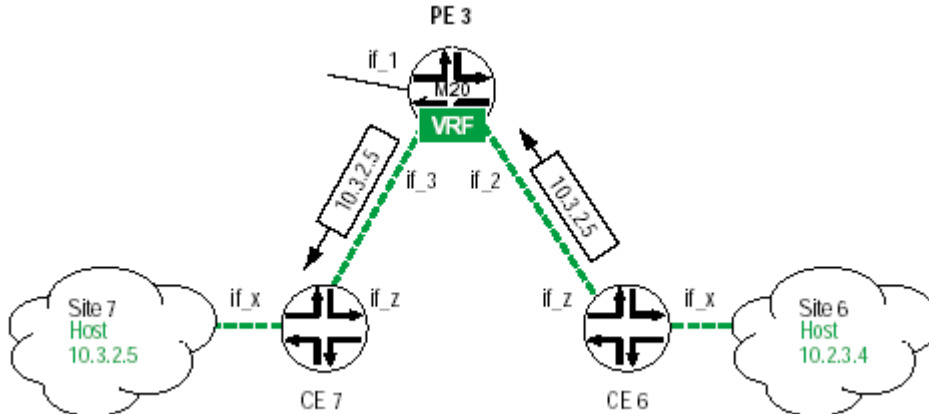


Рисунок 16. Форвардинг трафика зеленой ВЧС от сайта 6 на сайт 7

Когда стандартный пакет IPv4 поступает на интерфейс if_x маршрутизатора CE 6, производится поиск самого длинного согласующегося маршрута в таблице IP форвардинга CE 6, дающий следующий результат:

Destination	Next-Hop	Interface
10.3/16	PE 3	if_z

Основываясь на результатах этого поиска, CE 6 продвигает стандартный пакет IPv4 через интерфейс if_z к PE 3.

PE 3 принимает стандартный пакет IPv4 на интерфейс if_2. Так как все пакеты, прибывающие на if_2, ассоциированы с зеленой таблицей VRF Green, PE 3 производит поиск самого длинного согласующегося маршрута в таблице VRF Green, и получает следующий результат:

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.3/16	Direct	if_3	1008	-

Так как выходной субинтерфейс пакета ассоциирован с таблицей VRF Green, сайт назначения непосредственно подключен к PE 3, следующий транзит – это маршрутизатор CE, и пакет не должен проходить по MPLS магистрали поставщика услуг. В результате этого поиска, PE 3 продвигает пакет IPv4 через if_3 к CE 7.

Когда стандартный пакет IPv4 прибывает на интерфейс if_z маршрутизатора CE 7, на CE 7 производится поиск самого длинного согласующегося маршрута в IP таблице форвардинга, дающий следующий результат:

Destination	Next-Hop	Interface
10.3/16	Direct	if_x

Основываясь на результатах поиска, CE 7 продвигает пакет через if_x на хост 10.3.2.5 сайта 7.

Доступ к общественной сети Интернет с сайта ВЧС

Хостам на сайтах ВЧС необходим доступ к общественной сети Интернет и к сайтам других ВЧС. Во многих ситуациях для частной сети можно использовать частное пространство адресов IP. В целом, существуют три способа, при помощи которых хост в ВЧС может получить глобально уникальный адрес для связи с хостами в Интернете.

- Все системы в частной сети могут использовать глобально уникальные IP адреса.
- Если только небольшому числу систем частной сети нужен доступ в Интернет, этим системам могут быть присвоены глобально уникальные адреса Интернета. Обычной практикой для систем частной сети является использование частных IP адресов, когда в то же время несколько систем в той же сети используют глобальные IP адреса.
- Для доступа систем ВЧС с частными IP адресами к сети Интернет можно применить сервер трансляции сетевых адресов NAT, который размещается в ВЧС.

В модели ВЧС BGP/MPLS есть несколько способов достижения этой цели. Одним из таких подходов является механизм доступа в Интернет без использования таблиц VRF.

Доступ в Интернет без использования таблиц VRF

В типичном случае один или несколько сайтов ВЧС обеспечивают прямой доступ в Интернет через Интернет-шлюз провайдера, того же самого, что предоставляет услуги ВЧС, или другого. Кроме того, шлюз Интернет может функционировать на интерфейсе маршрутизатора CE без таблицы VRF или на другом маршрутизаторе сайта клиента. Интерфейс маршрутизатора, предоставляющий доступ в Интернет, конфигурируется для функционирования в качестве межсетевых экранов и сервера NAT. На рис. 17 доступ в Интернет для красной ВЧС Red обеспечивается через интерфейс CE 1 без таблицы VRF.

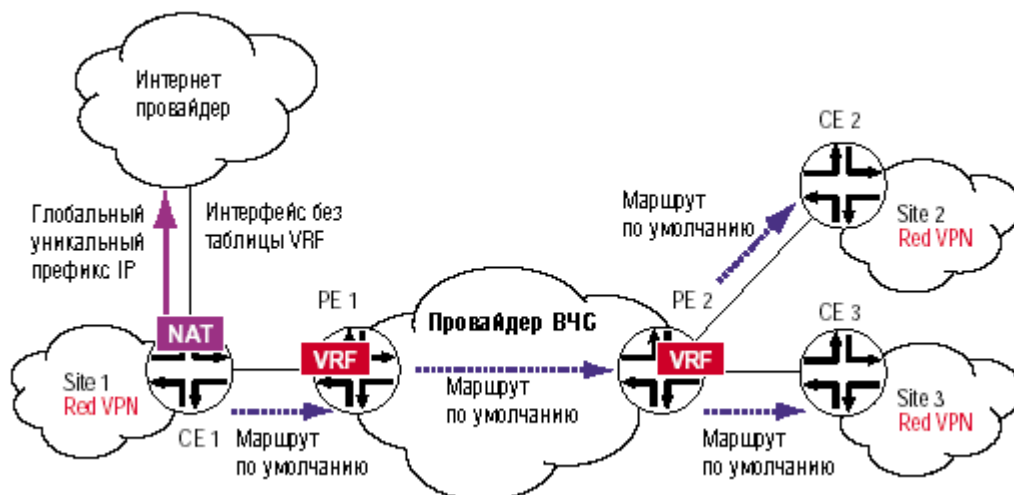


Рисунок 17. Доступ в Интернет без таблицы VRF

Доступ хостов ВЧС к сети Интернет

Для осуществления доступа к сети Интернет хостов красной ВЧС Red маршрутизатор CE 1 на сайте 1 распространяет маршрут по умолчанию к PE 1, который вводит его в таблицу VRF Red (рис. 17). Затем PE 1 распространяет маршрут по умолчанию посредством протокола MP-IBGP в направлении PE 2, который вводит его в таблицу VRF Red. Наконец, PE 2 распространяет маршрут по умолчанию к CE 2 на сайте 2 и к CE 3 на сайте 3. В результате этих объявлений хосты на любом сайте красной ВЧС продвигают трафик Интернет к CE 1 на сайте 1, который маршрутизирует выходной трафик своего интерфейса NAT в сеть Интернет. Служба NAT транслирует частный адрес источника в глобальный адрес источника.

Взаимодействие сети Интернет с хостами ВЧС

Для осуществления ответного доступа серверов Интернета к хостам сайтов красной ВЧС маршрутизатор CE 1 объявляет общественный IP префикс в таблице маршрутизации Интернета. Маршрутизаторы Интернета продвигают трафик к CE 1 на основе этого глобального префикса. Когда пакет прибывает на

интерфейс NAT маршрутизатора CE 1, служба NAT транслирует глобальные адреса в частные адреса назначения. Если хост назначения находится на сайте 1, CE 1 просто продвигает пакет непосредственно к хосту. Если хост назначения находится на сайте 2 или сайте 3, CE 1 продвигает пакет к PE 1, который в свою очередь продвигает пакет к PE 2.

Хотя сайтам без прямого доступа к Интернету требуется использовать интерфейс VRF для доступа к Интернету, все пакеты, вошедшие или вышедшие из ВЧС, в конце концов должны пройти через интерфейс без таблицы VRF и службы NAT, обеспечивающий прямой доступ к Интернету.

Масштабируемость ВЧС BGP/MPLS

В этом разделе дается краткое описание элементов архитектуры, определяемых в RFC 2547bis для улучшения масштабируемости ВЧС BGP/MPLS.

- ВЧС BGP/MPLS не является оверлейной сетью, наложенной на сеть поставщика услуг. Следовательно, отсутствует "проблема N²", характерная для оверлейной модели.
- Если есть несколько подключений между сайтом клиента и маршрутизатором PE, все подключения отображаются в одну таблицу форвардинга для экономии ресурсов маршрутизатора PE.
- Поддерживаются перекрывающиеся адресные пространства, что позволяет клиентам эффективно использовать частное пространство адресов IP.
- Маршрутизаторы PE должны поддерживать маршруты ВЧС, но только для тех ВЧС, к которым они непосредственно подключены.
- Цели маршрута ограничивают распространение маршрутной информации.
- Маршрутизаторы PE не обслуживают маршруты к удаленным маршрутизаторам CE, а только к другим маршрутизаторам PE.
- Маршрутизаторы P не хранят никакой маршрутной информации ВЧС, так как используют стек с двумя метками.
- Не требуется наличия в магистральной поставщика услуг единой системы для хранения маршрутной информации ВЧС, поддерживаемых поставщиком услуг.
- Управление сетью упрощается, так как поставщики услуг не должны администрировать магистраль или виртуальную магистраль для ВЧС каждого клиента.
- Признаки RD структурированы так, чтобы каждый поставщик услуг мог администрировать собственное адресное пространство и создавать глобально уникальные RD, не конфликтующие с RD, присваиваемыми другими поставщиками услуг.
- Фильтры ORF уменьшают количество маршрутной информации, распространяемой в магистральной поставщика услуг, и экономят ресурсы пакетной обработки маршрутизатора PE.
- Проблемы обслуживания полносвязных соединений MP-IBGP устраняются путем использования рефлекторов маршрутов.
- Рефлекторы маршрута - единственные системы в сети, которые должны поддерживать маршрутную информацию ВЧС для сайтов, с которыми они непосредственно не соединены. Сегментированное отражение маршрутов улучшает масштабируемость, так как нет ни одного рефлектора, который должен был бы поддерживать маршрутную информацию обо всех маршрутах VPN-IPv4, развернутых в сети поставщика услуг.
- Пути LSP с регулированием трафика на основе RSVP оптимизируют связь между маршрутизаторами PE.
- Доступ в Интернет не требует репликации маршрутов Интернета в таблицах VRF.

Заключение

Хотя детали функционирования ВЧС, рассмотренные в рекомендации RFC 2547bis, подходят для большого числа клиентских приложений, они не могут удовлетворить все требования конечных пользователей и бизнеса.

ВЧС BGP/MPLS хорошо подходит для клиентов, имеющих относительно простые сети, позволяя переложить сложности управления маршрутизацией на плечи поставщика услуг ВЧС, передать управление полносвязной сетью между сайтами с клиентского маршрутизатора на маршрутизатор провайдера, где может использоваться прямая и обратная передача пакетов по протоколу IBGP, а также позволяет поставщикам услуг использовать разделяемую инфраструктуру MPLS для транспорта частного и общественного трафика данных.

Однако подход ВЧС BGP/MPLS не свободен от ограничений.

- Могут возникнуть затруднения в сложных ситуациях маршрутизации, так как технология ВЧС BGP/MPLS основана на относительно простых маршрутных связях между маршрутизаторами клиента и провайдера.
- Недостаточно изучено управление таблицами форвардинга, число которых может достигать сотен, на единственном маршрутизаторе PE.
- Нет поддержки IP Multicast.
- В условиях работы с множеством поставщиков услуг есть проблемы, касающиеся поддержки сквозного качества или класса обслуживания.
- Взаимодействие сетевого управления и других инструментов эксплуатационной поддержки становится исключительно сложным в условиях работы с множеством поставщиков услуг.

Все архитектуры ВЧС имеют некоторые преимущества и ограничения. Поставщики услуг должны провести тщательный анализ требований клиентов и затем выбрать наилучшее решение для каждого клиента из всего спектра моделей и услуг ВЧС. Есть вероятность, что ВЧС BGP/MPLS будут играть основную роль в любом наборе сервисных моделей ВЧС.

Литература

Рабочие документы Интернет

Chen and Rekhter, *Cooperative Route Filtering Capability for BGP4*, <draft-ietf-idr-route-filter-02.txt>, November 2000.

Ramachandra, Tappan, and Rekhter, *BGP Extended Communities Attribute*, <draft-ramachandra-bgp-ext-communities-08.txt>, January 2001.

Rosen, Rekhter, Bogovic, Brannon, Carugi, Chase, Chung, Dean, De Clercq, Hitchen, Leelanivas, Marshall, Martini, Morrow, Vaidyanathan, Smith, Srinivasan, and Vedrenne, *BGP/MPLS VPNs*, <draft-rosen-rtc2547bis-02.txt>, July 2000.

Рекомендации

RFC 1771, *A Border Gateway Protocol 4 (BGP4)*, Rekhter and Li, March 1995.

RFC 1997, *BGP Communities Attribute*, Chandra, Traina, and Li, August 1996.

RFC 2283, *Multiprotocol Extensions for BGP4*, Bates, Chandra, Katz, and Rekhter, February 1998.

RFC 2547, *BGP/MPLS VPNs*, Rosen and Rekhter, March 1999.

RFC 2796, *BGP Route Reflection: An Alternative to Full Mesh IBGP*, Bates, Chandra, and Chen, April 2000.

RFC 2842, *Capabilities Advertisement with BGP4*, Chandra, and Scudder, May 2000.

RFC 2858, *Multiprotocol Extensions for BGP4*, Bates, Chandra, Katz, and Rekhter, June 2000.

RFC 2918, *Route Refresh Capability for BGP4*, Chen, September 2000.

Книги

Davie, Bruce S. and Yakov Rekhter, *MPLS: Technology and Applications*, Morgan Kaufmann Publishers, San Francisco, 2000, (ISBN 1-55860-656-4-4).

Huston, Geoff, *ISP Survival Guide: Strategies for Running a Competitive ISP*, John Wiley & Sons Inc., New York, 1999, (ISBN 0-471-31499-4).

Scott, Charles, Paul Wolfe, and Mike Erwin, *Virtual Private Networks (Second Edition)*, O'Reilly & Associates, Inc., California 1999, (ISBN 1-56592-527-7).

Copyright © 2002 Poplar systems

Poplar
SYSTEMS

<http://www.poplar.ru>