Технология MPLS VPN третьего уровня

В этом типе VPN пользовательские сети (называемые также сайтами) объединяются на основе адресной информации третьего уровня, то есть IP-адресов (а не MAC-адресов и идентификаторов VLAN как в MPLS VPN второго уровня). При этом IP-адреса могут быть как публичными, так и частными, в последнем случае они должны быть уникальными в пределах одной виртуальной сети.

В то же время между MPLS VPN третьего уровня и второго имеется много общего:

- услуги предоставляются провайдером с помощью сети IP/MPLS;
- пограничные маршрутизаторы PE выполняют всю работу по поддержанию VPN;
- внутренние маршрутизаторы провайдера P нужны только для передачи MPLS пакетов между пограничными маршрутизаторами PE; они не знают о существовании VPN;
- для передачи информации о принадлежности пакета к определенной сети VPN используется *метка MPLS второго уровня*.

Разграничение маршрутной информации

Каждый пограничный маршрутизатор PE обменивается маршрутной информацией с соединенными с ним клиентскими маршрутизаторами CE по какому-нибудь протоколу маршрутизации класса IGP, например, OSPF или IS-IS (рис. 1). С каждым из клиентов может использоваться свой протокол IGP, то есть с сайтом A протокол OSPF, а с сайтом B — протокол IS-IS. С помощью этих протоколов маршрутизатор узнает о том, какие сети достижимы в сайтах клиентов. Кроме того, маршрутизатор PE поддерживает сеанс протокола IGP с остальными маршрутизаторами сети провайдера (как P, так и PE) для того, чтобы знать топологию этой сети и маршрутизировать пакеты в пределах этой сети.

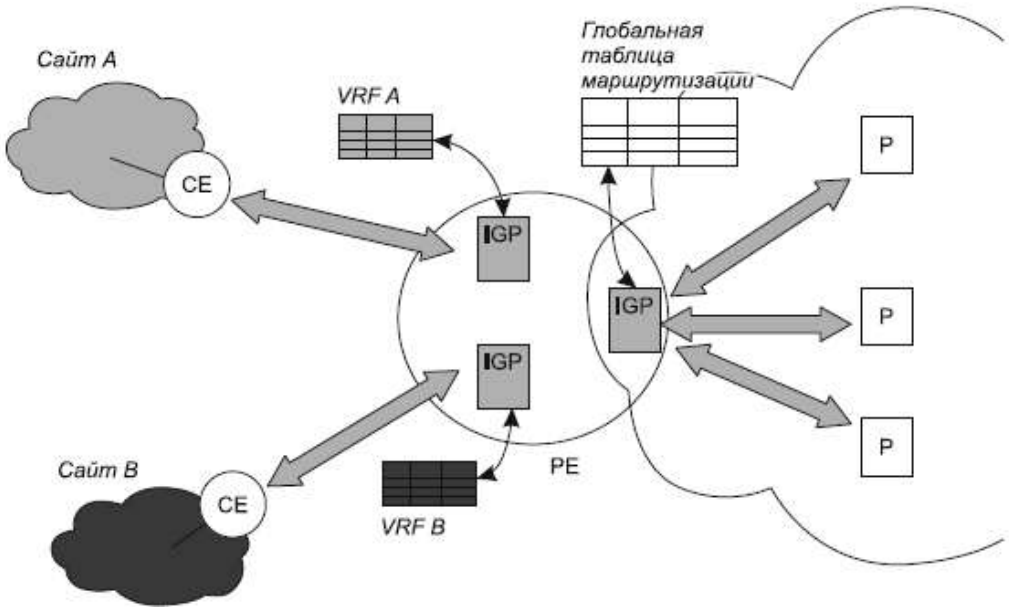

Рис. 1. Разграничение маршрутных объявлений в сети MPLS VPN третьего уровня

Для корректной работы VPN требуется, чтобы информация о маршрутах через сеть провайдера не распространялась за ее пределы, а сведения о маршрутах в клиентских сайтах не становились известными за границами определенных сетей VPN.

Барьеры на пути распространения маршрутных объявлений могут устанавливаться соответствующим конфигурированием маршрутизаторов PE. Протоколы маршрутизации этих маршрутизаторов должны быть оповещен о том, с каких интерфейсов и от кого они имеют право принимать объявления определенного сорта и на какие интерфейсы и кому их распространять.

Можно представить, что через маршрутизатор PE проходит невидимая граница между зоной клиентских

сайтов и зоной ядра сети провайдера. По одну сторону располагаются интерфейсы, через которые PE взаимодействует с маршрутизаторами P, а по другую — интерфейсы, к которым подключаются сайты клиентов. С одной стороны на PE поступают объявления о маршрутах в сети провайдера, с другой — объявления о маршрутах в сетях клиентов.

На рис. 22.8 показан маршрутизатор PE, на котором установлены несколько протоколов класса IGP. Один из них сконфигурирован для приема и распространения маршрутных объявлений только с тех трех внутренних интерфейсов, которые связывают этот маршрутизатор PE с маршрутизаторами P. Два других протокола IGP обрабатывают маршрутную информацию от сайтов клиентов.

Аналогичным образом настроены и остальные маршрутизаторы PE. Таблица маршрутизации, создаваемая на пограничных маршрутизаторах PE на основе объявлений из магистральной сети провайдера, имеет специальное название: **глобальная таблица маршрутизации**. В ней содержатся маршруты в пределах внутренней сети провайдера, информации о маршрутах в сетях клиентов в ней нет. Таблицы маршрутизации, которые PE формирует на основе объявлений, поступающих от сайтов клиентов, получили название таблиц **VRF** (VPN Routing and Forwarding). В них имеется только информация о сетях клиентов.

Маршрутизаторы P принимают и обрабатывают маршрутную информацию IGP, поступающую со всех интерфейсов. В создаваемых ими таблицах маршрутизации имеется информация только о сетях провайдера.

Сайты клиентов представляют собой обычные сети IP, маршрутная информация в которых может передаваться и обрабатываться с помощью любого протокола маршрутизации класса IGP. Очевидно, что этот процесс никак не регламентируется провайдером. Маршрутные объявления свободно распространяются между узлами в пределах каждого сайта до тех пор, пока не доходят до пограничных маршрутизаторов PE, служащих преградой для их дальнейшего распространения.

Разграничение маршрутов разных клиентов обеспечивает установка на маршрутизаторах PE *отдельной копии протокола маршрутизации* на каждый интерфейс, к которому подключен сайт клиента. Этот протокол принимает и передает клиентские маршрутные объявления только с одного определенного для него интерфейса, не пересылая их ни на внутренние интерфейсы, через которые PE связан с маршрутизаторами P, ни на интерфейсы, к которым подключены сайты других клиентов.

Несколько упрощая, можно считать, что на каждом маршрутизаторе PE создается столько таблиц VRF, сколько сайтов к нему подключено. Фактически, на маршрутизаторе PE организуется несколько виртуальных маршрутизаторов, каждый из которых работает со своей таблицей VRF. Возможно и другое соотношение между сайтами и таблицами VRF. Например, если к некоторому маршрутизатору PE подключено несколько сайтов одной и той же сети VPN, то для них может быть создана общая таблица VRF. На рис. 22.8 показаны две таблицы VRF, одна из которых содержит описание маршрутов к узлам сайта A, а другая — к узлам сайта B. К каждой такой таблице можно получить доступ только с сайтов, относящихся к этой же сети VPN.

Обмен маршрутной информацией

Чтобы связать территориально разнесенные сайты заказчика в единую сеть, необходимо, во-первых, создать для них общее пространство распространения маршрутной информации, а, во-вторых, проложить во внутренней сети пути, по которым принадлежащие разным сайтам узлы одной и той же сети VPN могли вести обмен данными защищенным образом.

Механизмом, с помощью которого сайты одной сети VPN обмениваются маршрутной информацией, является **многопротокольное расширение для BGP** (MultiProtocol extensions for BGP-4, **MP-BGP**). С помощью этого протокола пограничные маршрутизаторы PE организуют взаимные сеансы и в рамках этих сеансов обмениваются маршрутной информацией из своих таблиц VRF.

Особенность протокола BGP и его расширений заключается в том, что он получает и передает свои маршрутные объявления не всем непосредственно связанным с ним маршрутизаторам, как протоколы IGP, а только тем, которые указаны в конфигурационных параметрах в качестве соседей. Маршрутизаторы PE сконфигурированы так, что все получаемые от клиентских сайтов маршрутные объявления они с помощью MP-BGP пересылают определенным пограничным маршрутизаторам PE. Вопрос о том, кому отправлять маршрутные объявления, а кому нет, целиком зависит от топологии виртуальных частных сетей, поддерживаемых данным провайдером.

Таким образом, кроме маршрутов, поступающих от непосредственно подсоединенных к PE сайтов, каждая таблица VRF дополняется маршрутами, получаемыми от других сайтов данной сети VPN по

протоколу MP-BGP. Целенаправленное распространение маршрутов между маршрутизаторами PE обеспечивается надлежащим выбором атрибутов протокола MP-BGP (эти атрибуты описаны в RFC 4360), что детально рассматривается далее.

Независимость адресных пространств сайтов

Одним из свойств частных сетей является независимость их адресных пространств. MPLS VPN третьего уровня имитируют это свойство, разрешая использовать одно и то же адресное пространство, например, пространство частных IP-адресов, во всех экземплярах VPN провайдера. При этом в пределах одной и той же сети VPN адреса не должны повторяться, иначе сайты не смогут взаимодействовать друг с другом.

Использование в разных сетях VPN одного и того же адресного пространства создает проблему для маршрутизаторов PE. Протокол BGP изначально был разработан в предположении, что все адреса, которыми он манипулирует, во-первых, относятся к семейству адресов IPv4, во-вторых, однозначно идентифицируют узлы сети, то есть являются глобально уникальными в пределах всей составной сети. Ориентация на глобальную уникальность адресов выражается в том, что получив очередное маршрутное объявление, протокол BGP анализирует его, не обращая внимания на то, какой сети VPN принадлежит полученный маршрут. Если на вход BGP поступают описания маршрутов к узлам разных сетей VPN, но с совпадающими адресами IPv4, то BGP считает, что все они ведут к одному и тому же узлу, а, следовательно, как и полагается в таком случае, он помещает в соответствующую таблицу VRF только один кратчайший маршрут.

Проблема решается за счет применения вместо потенциально неоднозначных адресов IPv4 расширенных и однозначных адресов нового типа, а именно — адресов VPN-IPv4, получаемых в результате преобразования исходных адресов IPv4. Преобразование заключается в том, что ко всем адресам IPv4, составляющим адресное пространство той или иной сети VPN, добавляется префикс, называемый **различителем маршрутов** (Route Distinguisher, **RD**). RD уникально идентифицирует каждую сеть VPN. В результате на маршрутизаторе PE все адреса, относящиеся к разным сетям VPN, обязательно будут отличаться друг от друга, даже если они имеют совпадающую часть — адрес IPv4.

Здесь оказалась полезной способность расширенного протокола MP-BGP переносить в маршрутных объявлениях адреса разных типов, в том числе IPv6, IPX, а также VPN-IPv4. Адреса VPN-IPv4 используются только для маршрутов, которыми маршрутизаторы PE обмениваются по протоколу BGP. Прежде чем передать своему напарнику некоторый маршрут, входной маршрутизатор PE добавляет к его адресу назначения IPv4 префикс RD для данной сети VPN, тем самым преобразуя его в маршрут VPN-IPv4.

Как уже отмечалось, различители маршрута должны гарантированно уникально идентифицировать VPN, чтобы избежать дублирования адресов. Упростить выбор RD, не создавая для этих целей дополнительных централизованных процедур (например, распределения RD органами Интернета подобно распределению адресов IPv4), предлагается за счет использования в качестве основы для RD заведомо уникальных чисел — либо номеров автономных систем, либо публичных адресов интерфейсов PE с магистральной сетью провайдера (сети провайдера всегда необходимы публичные адреса для взаимодействия с сетями других провайдеров).

На рис. 2 показано, как входной маршрутизатор PE1 добавляет различитель маршрутов 123.45.67.89:1 (123.45.67.89 — это глобальный адрес интерфейса маршрутизатора PE, а 1 — назначенный администратором номер) ко всем адресам с префиксом 10.1/16, которые он получает от маршрутизатора CE сайта 1 в VPN A, и пересылает эти маршруты на два других выходных маршрутизатора PE. Аналогично, маршрутизатор PE1 добавляет различитель маршрутов 123.45.67.89:2 к адресам с префиксом 10.1/16 в маршрутах, которые он получает от маршрутизатора CE сайта 1 в VPN B, и передает сформированные маршруты на другие два маршрутизатора PE. Только благодаря этим добавлениям протокол BGP, работающий на удаленных маршрутизаторах PE, способен различать маршруты с совпадающими адресами IPv4, относящиеся к разным сетям VPN.

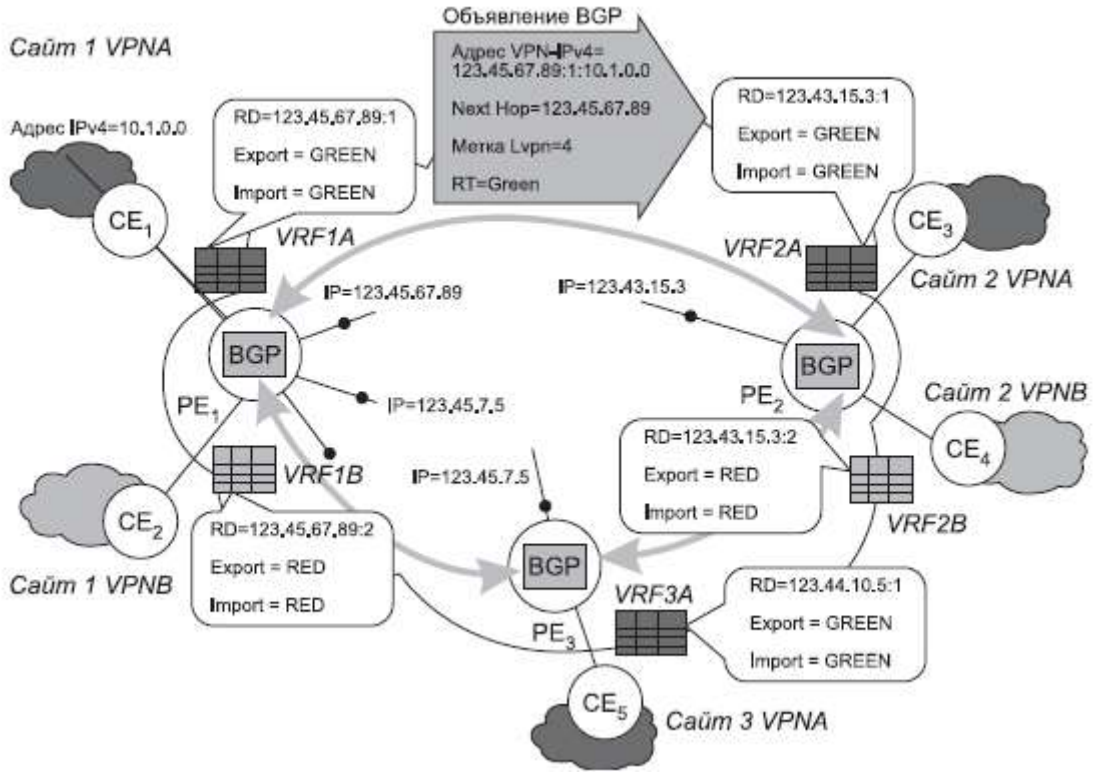

Рис. 2. Маршрутные объявления MB-BGP

Когда выходной маршрутизатор PE получает маршрут к сети VPN-IPv4, он делает обратное преобразование, отбрасывая префикс RD, и только потом помещает маршрут в таблицу VRF и объявляет его связанному с ним маршрутизатору заказчика CE из данной сети VPN. Таким образом, все маршруты в таблицах VRF содержат адреса в формате IPv4.

Конфигурирование топологии VPN

MPLS VPN третьего уровня позволяют создавать различные топологии связей между сайтами одной и той же сети VPN. Этим свойством сети VPN данного типа отличаются от сетей MPLS VPN второго уровня, в которых сайты одной и той же сети VPN всегда достижимы друг для друга. Например, в MPLS VPN третьего уровня можно создать звездообразную топологию, в которой периферийные сайты могут взаимодействовать с центральным сайтом, а между собой нет — эту топологию сервис MPLS VPN второго уровня обеспечить не может.

Такая гибкая форма создания топологии VPN достигается за счет атрибутов экспорта-импорта маршрутов в объявлениях MP-BGP. Атрибут **route-target** (**RT**) идентифицирует входящих в данную сеть VPN набор сайтов (VRF), которым маршрутизатор PE должен посылать маршруты.

Значение атрибута route-target в объявлении о маршруте определяется политикой экспорта маршрутных объявлений, которая была задана при конфигурировании таблицы VRF, содержащей данный маршрут. Если же маршрут не входит в число экспортируемых, то он не передается другим маршрутизаторам PE, а используется локально. Такое возможно в случае, когда два маршрутизатора CE в одной и той же сети VPN непосредственно подключены к одному и тому же маршрутизатору PE. Формат атрибута route-target аналогичен формату различителя маршрутов (RD), что обеспечивает его уникальность в пределах всех сетей VPN.

При получении объявлений MP-BGP вступает в действие политика импорта маршрутов; как и политика экспорта, она задается при конфигурировании каждой таблицы VRF.

Задание одного и того же значения для политики экспорта и импорта для всех таблиц VRF определенной сети VPN приводит к полносвязной топологии — каждый сайт пересылает пакеты непосредственно тому сайту, в котором находится сеть назначения.

Именно этот случай для VPN A и VPN B показан на рис. 2, так как таблицы VRF сайтов этих сетей VPN

сконфигурированы с одинаковыми значениями политики экспорта и импорта: значением GREEN для VPN A и значением RED для VPN B.

Пример конфигурирования звездообразной топологии представлен на рис. 3.

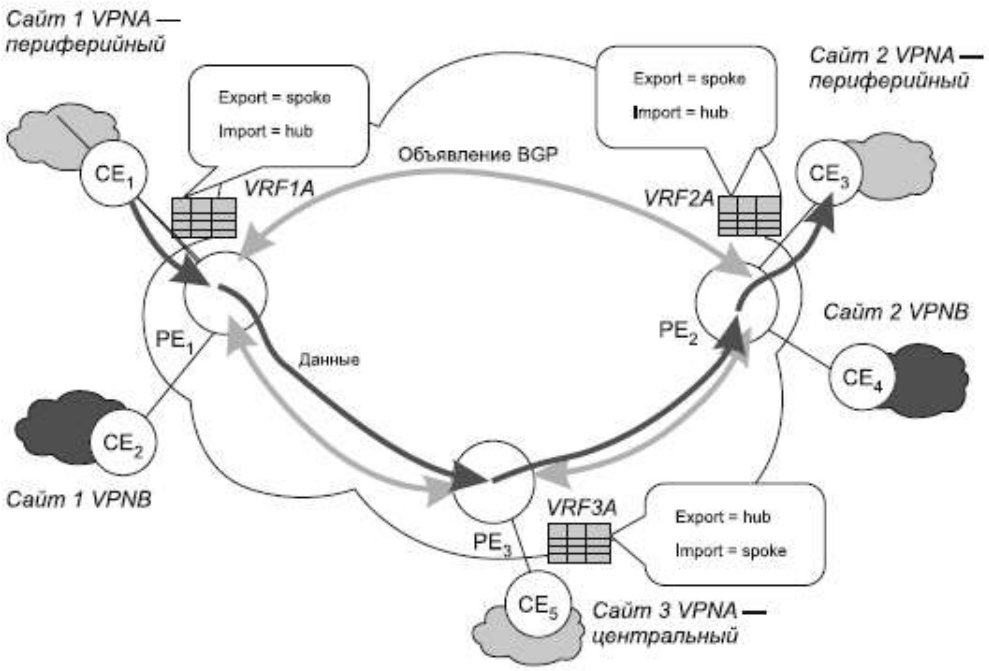

Рис. 3. Конфигурирование звездообразной топологии между сайтами VPNA.

Для достижения этого эффекта достаточно определить для VRF центрального сайта политику импорта как import = spoke, экспорта — как export = hub, а для VFR периферийных сайтов поступить наоборот, задав import = hub и export = spoke. В результате таблицы VRF периферийных сайтов не смогут принимать маршрутные объявления друг от друга, поскольку они передаются по сети протоколом MP-BGP с атрибутом routetarget = spoke, между тем как их политика импорта разрешает получать объявления с атрибутом route-target = hub. Зато объявления таблиц VRF периферийных сайтов принимает таблица VRF центрального сайта, для которого как раз и определена политика импорта spoke. Этот сайт обобщает все объявления периферийных сайтов и отсылает их обратно, но уже с атрибутом route-target = hub, что совпадает с политикой импорта периферийного сайта. Таким образом, в VRF каждого периферийного сайта появляются записи о сетях в других периферийных сайтах с адресом связанного с центральным сайтом интерфейса PE в качестве следующего транзитного узла — поскольку объявление пришло от него. Поэтому пакеты между периферийными сайтами будут проходить транзитом через пограничный маршрутизатор PE3, подключенный к центральному сайту.