Network Working Group
Request for Comments: 2917
Category: Informational

K. Muthukrishnan
Lucent Technologies
A. Malis
Vivace Networks, Inc.
September 2000

Архитектура ядра MPLS IP VPN

A Core MPLS IP VPN Architecture

Статус документа

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

Авторские права

Аннотация

В этом документе представлена модель построения ядра службы Виртуальных Частных Сетей (VPN[1]) в сети MPLS сервис-провайдера. Эта модель использует многопротокольную коммутацию меток (MPLS[2]) в опорной сети для предоставления более высокого качества услуг. Основной задачей сервис-провайдера является предоставление заказчикам услуг виртуальных маршрутизаторов. Основными преимуществами этой архитектуры является простота настройки, защита пользователей, безопасность сети, динамическое обнаружение соседей, масштабирование и использование существующих протоколов маршрутизации без необходимости их изменения.

1. Используемые сокращения

ARP	- протокол преобразования адресов (Address Resolution Protocol)
CE	- краевой маршрутизатор пользователя (Customer Edge router)
LSP	- путь коммутации меток (Label Switched Path)
PNA	- администратор частной сети (Private Network Administrator)
SLA	- соглашение об уровне обслуживания (Service Level Agreement)
SP	- сервис провайдер (Service Provider)
SPED	- краевое устройство сервис-провайдера (Service Provider Edge Device)
SPNA	- администратор сети сервис-провайдера (SP Network Administrator)
VMA	- групповой адрес VPN (VPN Multicast Address)
VPNID	- идентификатор VPN (VPN Identifier)
VR	- виртуальный маршрутизатор (Virtual Router)
VRC	- консоль виртуального маршрутизатора (Virtual Router Console)

2. Введение

В этом документе представлена модель построения ядра службы Виртуальных Частных Сетей (VPN[3]) в сети MPLS сервис-провайдера. Возможны два варианта построения ядра - оверлейная модель и модель на основе виртуальных маршрутизаторов. Оверлейная модель основана на расширение семантики существующих протоколов маршрутизации для передачи информации о доступности (сетей). В этом документе основное внимание уделено модели на основе виртуальных маршрутизаторов.

Представленная здесь модель не требует изменения существующих протоколов маршрутизации. Обнаружение соседей осуществляется за счет использования эмулируемых ЛВС и протокола преобразования адресов ARP. В этом документе проводится линия раздела между SP и PNA - SP владееет услугами уровней 1 и 2, а также управляет ими, а услуги уровня 3 относятся к PNA и управляются им. За счет поддержки логически полностью независимых доменов маршрутизации PNA получает гибкость использования незарегистрированных и приватных адресов. За счет применения приватных LSP и инкапсуляции VPNID с использованием стеков меток в разделяемых LSP предотвращаются проблемы с защитой данных.

Описанная здесь модель отличается от варианта RFC 2547 [Rosen1] тем, что не задается конкретный протокол маршрутизации для переноса маршрутов VPN. В RFC 2547 определены изменения протокола BGP, которые требуется

[1]Virtual Private Network
[2]Multiprotocol Label Switching
[3]Virtual Private Network

внести для передачи индивидуальных (unicast) маршрутов VPN через опорную сеть SP. Для передачи групповых маршрутов потребуются дополнительные исследования архитектуры.

3. Виртуальные маршрутизаторы

Виртуальный маршрутизатор представляет собой набор статических или динамических «нитей» (thread), обеспечивающий услуги маршрутизации и пересылки, подобно физическому маршрутизатору. Для виртуального маршрутизатора не требуется (хотя может использоваться) отдельный процесс в операционной системе - просто создается иллюзия существования реального маршрутизатора, удовлетворяющего потребности сетей, к которым он подключен. Виртуальный маршрутизатор, подобно своему физическому аналогу, является элементом домена маршрутизации. Другие маршрутизаторы этого домена могут быть физическими или виртуальными. Из того, что виртуальный маршрутизатор соединен с конкретным (логически отделенным) доменом маршрутизации, а физический маршрутизатор может поддерживать множество виртуальных маршрутизаторов, следует, что один физический маршрутизатор может поддерживать множество (логически отделенных) доменов маршрутизации.

С точки зрения пользователя (заказчика VPN) важно, чтобы виртуальный маршрутизатор был как можно сильнее похож на физический маршрутизатор. Иными словами, с незначительными и немногочисленными отличиями виртуальный маршрутизатор во всех аспектах (конфигурация, управление, поиск неполадок) должен выглядеть, как выделенный физический маршрутизатор. Кроме того, важным является требование минимизации усилий по обновлению и изменению конфигурационных параметров установленных маршрутизаторов, а также избавление от необходимости переподготовки сетевых администраторов.

К числу аспектов, которые требуется эмулировать в виртуальных маршрутизаторах, относятся:

1. поддержка любых комбинаций протоколов маршрутизации;
2. мониторинг сети;
3. поиск неисправностей.

Каждая сеть VPN представляет собой логически независимый домен маршрутизации. Это расширяет возможности SP в части предоставления заказчикам услуг маршрутизации без необходимости установки отдельного маршрутизатора для каждой сети VPN. В результате инвестиции SP в оборудование (а именно, в маршрутизаторы и каналы между ними), могут служить множеству заказчиков.

4. Задачи

1. Простая, масштабируемая конфигурация оконечных точек VPN в сети сервис-провайдера. Для добавления CE должно требоваться не более одного элемента конфигурации.
2. Отказ от использования ресурсов SP, являющихся уникальными в глобальном масштабе и дефицитными (таких, как адреса и подсети IP).
3. Динамическое обнаружение VR (виртуальных маршрутизаторов в «сетевом облаке» SP. Это требование не является обязательным, но его выполнение очень важно в целях обеспечения простоты.
4. Для VR следует обеспечить сетевым администраторам VPN полные возможности настройки и мониторинга. Это позволит PNA самостоятельно настраивать VPN или передавать эту задачу на аутсорсинг SP.
5. Настройку качества пересылки данных следовать обеспечивать на уровне VPN-VPN. Уровни качества должны представлять собой ряд (возможно, дискретный) последовательных значений. Примерами уровней качества обслуживания могут служить best effort (по возможности), dedicated bandwidth (выделенная полоса), QOS, policy based forwarding (пересылка на основе правил).
6. Настройку диференцированных услуг следует обеспечивать на уровне VPN-VPN (возможно, с использованием LSP, организованных исключительно для пересылки трафика в VPN).
7. Защита маршрутизаторов Internet распространяется на виртуальные маршрутизаторы. Это означает, что функции пересылки и маршрутизации в виртуальных маршрутизаторах должны быть столь же защищены, как аналогичные функции в выделенном, физическом маршрутизаторе. Не следует допускать непреднамеренной утечки информации (пользовательских данных и информации о доступности сетей) из одного домена маршрутизации в другой.
8. Не следует требовать использования между виртуальными маршрутизаторами специфических протоколов маршрутизации. Это критически важно для того, чтобы заказчики VPN могли организовать свою сеть и политику в соответствии со своими взглядами. Например, некоторые протоколы сложны для фильтрации, а в других может быть слишком сложным формование трафика. Заказчик VPN может пожелать использовать оба протокола для повышения качества работы своей сети.
9. Не должно требоваться специальных расширений для существующих протоколов маршрутизации типа BGP, RIP, OSPF, ISIS и т. п. Это имеет очень важное значение с точки зрения будущих расширений или введения новых типов сервиса (например, NHRP или групповой адресации). В дополнение к сказанному, улучшения и расширения существующих протоколов маршрутизации (такие, как управление трафиком в ISIS и OSPF) должны легко встраиваться в реализации VPN.

5. Архитектурные требования

В сети сервис-провайдера должна работать та или иная форма групповой маршрутизации для всех узлов, имеющих соединения VPN, и узлов, которые должны пересылать групповые дейтаграммы для обнаружения виртуальных маршрутизаторов. Конкретный протокол групповой маршрутизации не задается. SP может выбрать MOSPF, DVMRP или любой другой протокол.

6. Основы архитектуры

1. Каждой сети VPN выделяется идентификатор VPNID, который уникален в масштабе сети SP. Этот идентификатор позволяет однозначно связать VPN с пакетами и соединениями. Нулевое значение VPNID зарезервировано для представления публичной сети Internet. Рекомендуется (но не требуется) выделять идентификаторы VPN в соответствии с RFC 2685 [Fox].

2. Услуги VPN предоставляются в форме «виртуального маршрутизатора». Эти VR остаются в SPED и относятся, таким образом к краю облака SP. Виртуальные маршрутизаторы будут использовать сеть SP для пересылки пакетов данных и управления, но во всех остальных аспектах остаются невидимыми за пределами SPED.

3. Контрактный «размер» VR для VPN в данном устройстве SPED выражается количеством ресурсов IP (интерфейсы, маршрутные фильтры, записи и т. п.). Это значение полностью контролируется SP и обеспечивает гранулярность, требуемую SP для виртуально неограниченного числа уровней обслуживания VR для каждого устройства SPED. [Например, одно устройство SPED может быть точкой агрегирования (скажем, центральный офис корпорации) для данной VPN, а множество других SPED могут служить точками доступа (офисы филиалов). В этом случае устройство SPED, подключенное в центральном офисе, может обеспечивать более мощный VR, а SPED в филиалах могут использовать меньшие (возможно, оконечные) VR]. Такое решение также позволяет SP создавать сети с распределением нагрузки между разными маршрутизаторами.

4. Одним из индикаторов размера VPN является число устройств SPED в сети SP, имеющих подключения к маршрутизаторам CPE в данной VPN. В этом смысле VPN со множеством сайтов, которым требуется подключение, образуют «большую» сеть VPN, а при незначительном числе сайтов - «малую» VPN. Кроме того, можно предполагать изменение размеров VPN с течением времени. Сети VPN могут также объединяться в результате слияния или покупки компаний, а также при заключении партнерских соглашений. Данная архитектура легко адаптируется к подобным изменениям, поскольку для VPN уникальные в глобальном масштабе ресурсы IP не присваиваются и не выделяются. Число устройств SPED не ограничивается какими-либо искусственными конфигурационными пределами.

5. SP владеют и управляют сетевыми объектами уровней 1 и 2. Говоря более конкретно, SP управляют физическими коммутаторами и маршрутизаторами, физическими соединениями, логическими каналами уровня 2 (DLCI в сетях Frame Relay и VPI/VCI в ATM) и LSP (и их привязками к конкретным VPN). В контексте VPN сервис-провайдеры SP отвечают за согласование и выделение сетевых элементов уровня 2 для конкретных VPN.

6. Элементы уровня 3 относятся к частным сетям и управляются администраторами этих сетей (PNA). Примеры таких элементов включают IP-интерфейсы, выбор протоколов динамической маршрутизации или статических маршрутов, а также интерфейсов для маршрутизации. Отметим, что хотя конфигурационные параметры уровня 3 входят в зону ответственности PNA, эти администраторы не всегда обязаны поддерживать их. Достаточно часто PNA передают администрирование IP на уровень виртуальных маршрутизаторов SP. Независимо от того, кто отвечает за настройку и мониторинг, это приближение обеспечивает администраторам PNA полную картину маршрутизации и позволяет им строить сети в соответствии с их реальными задачами.

7. Сетями VPN можно управлять, как физическими маршрутизаторами, а не развернутыми виртуальными маршрутизаторами (VR). Следовательно, для управления может применяться протокол SNMP или аналогичные методы, а также прямое управление с консоли VR (VRC).

8. Стандартные средства поиска неисправностей (ping, traceroute и т. п.) разработаны для доменов маршрутизации, состоящих исключительно из выделенных физических маршрутизаторов. Следовательно, для мониторинга и поиска неисправностей могут применяться эти стандартные методы, а также SNMP и аналогичные средства. В этом случае может также использоваться консоль VRC как на физических маршрутизаторах.

9. Поскольку консоли VRC доступны пользователям, нужно обеспечить проверку прав пользователей VPN на доступ к ресурсам уровня 3 в данной VPN и полностью запрещать доступ к физическим ресурсам маршрутизаторов. Большинство маршрутизаторов реализуют такую возможность с помощью разных представлений баз данных.

10. Консоли VRC доступны и для SP. Если функции настройки и мониторинга переданы SP, сервис-провайдер может использовать VRC для решения этих задач, принимая на себя функции PNA.

11. Маршрутизаторы VR в устройствах SPED формируют VPN в сети SP. Совместно эти элементы образуют виртуальный домен маршрутизации. Динамическое обнаружение элементов реализуется путем эмуляции ЛВС в сети SP.

Каждой VPN в сети SP присваивается один (и только один) групповой адрес, выбираемый из диапазона 239.192/14 [Meyer]. Единственным требованием в данном случае является уникальность адреса для конкретной VPN. Эта задача легко решается маршрутизаторами путем использования простой функции однозначного отображения VPNid на групповой адрес. Подписка на данный групповой адрес позволяет виртуальным маршрутизаторам обнаруживать другие VR и быть доступными для обнаружения другими VR. Важно отметить, что групповой адрес не является настраиваемым параметров.

12. Пересылка данных может выполняться одним из перечисленных способов:

    1. LSP с характеристиками best-effort, доступный для использования всеми VPN;

    2. LSP, выделенный для VPN и построения трафика заказчиком VPN;

    3. приватный LSP с поддержкой дифференциации;

    4. пересылка в соответствии с правилами на выделенном виртуальном устройстве L2.

Выбор метода пересылки согласуется между SP и пользователем VPN, составляя, возможно, часть SLA-соглашения между ними. Это позволяет SP предлагать разные типы обслуживания для различных VPN.

Естественно, обычная поэтапная (hop-by-hop) пересылка поддерживается для пакетов маршрутизации и пользовательских пакетов данных в периоды организации LSP и при возникновении отказов.

13. Эта модель не требует запуска отдельных задач для каждого протокола маршрутизации в операционной системе для каждого VR на устройствах SPED. Для использования на каждом SPED могут быть адаптированы конкретные реализации. Поддержка раздельных баз маршрутных данных и таблиц пересылки для каждого VR является одним из путей обеспечения максимальной производительности для данного устройства SPED.

7. Масштабируемая конфигурация

Предполагается, что типовые VPN в облаке SP будут включать сотни или тысячи конечных станций. Следовательно, сложность конфигурации должна зависеть от числа конечных точек не сильнее, чем линейно от числа. Более конкретно, администратор должен добавлять незначительное число элементов в конфигурационные файлы при подключении нового пользовательского сайта к множеству VR, образующих конкретную VPN. В противном случае задача становится для сервис-провайдеров слишком обременительной. В описываемой архитектуре от сервис-провайдера требуется лишь выделение и настройка входящих/исходящих физических соединений (например, Frame Relay DLCI или ATM VPI/VCI) и виртуальные соединения между VR и эмулируемыми ЛВС.

8. Динамическое обнаружение соседей

VR данной VPN реализуются на множестве устройств SPED в сети. Эти VR должны знать друг о друге и быть соединены между собой.

Одним из способов решения этой задачи является указание соседей в конфигурационных файлах вручную. Например, при добавлении в VPN нового сайта соответствующие изменения вносятся на всех маршрутизаторах VR. Обычно такой путь не обеспечивает достаточного уровня масштабируемости в плане настройки и распределения сетевых ресурсов.

Возникает потребность в обеспечении маршрутизаторам VR возможности автоматически детектировать друг друга. Обнаружение соседей выполняется за счет предоставления каждой VPN ограниченной эмулируемой ЛВС, которая может использоваться разными способами.

1. Преобразование адресов (ARP) в ЛВС позволяет определить (приватный) IP-адрес следующего интервала, связанного с другими VR.
2. Протоколы маршрутизации (например, RIP или OSPF) используют эту ограниченную эмулируемую ЛВС для обнаружения соседей и передачи маршрутных обновлений.

ЛВС на уровне VPN эмулируются с использованием групповых адресов IP. С целью сохранения публичного адресного пространства и по причине того, что эти групповые адреса видны только в сети SP, мы будем пользоваться адресами с областью видимости Organizational (организация) из блока 239.192/14, как описано в [Meyer]. Каждой VPN выделяется адрес из этого диапазона. Для автоматической настройки конфигурации адреса определяются на основе VPNID.

9. Конфигурация домена VPN IP

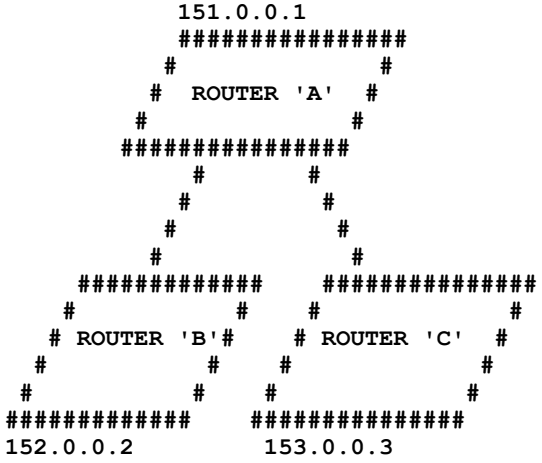

Рисунок 1. Физический домен маршрутизации.

На рисунке 1 показан физический домен в сети SP. В этой сети физические маршрутизаторы A, B и C соединены между собой и каждому маршрутизатору присвоен «публичный» адрес IP. Эти адреса являются уникальными идентификаторами маршрутизаторов в сети SP.

Каждый виртуальный маршрутизатор настраивается PNA, как будто он является частным физическим маршрутизатором. Естественно, SP ограничивает ресурсы, которые такой VR может потреблять на уровне устройств SPED. Каждая VPN имеет множество физических (с маршрутизаторами CPE) и логических (с эмулируемой ЛВС) соединений. Каждое соединение поддерживает IP и может быть настроено на использование любой комбинации стандартных протоколов маршрутизации и маршрутных политик в соответствии с задачами корпоративной сети.

На рисунке 2[1] три маршрутизатора VR сети VPN 1 размещаются на трех устройствах SPED. Маршрутизатор A поддерживает VR-A, маршрутизатор B — VR-B, а маршрутизатор C - VR-C. Виртуальные маршрутизаторы VR-C и VR-B имеют по одному физическому соединении с оборудованием CPE, а VR-A имеет 2 физических соединения. Каждый из этих VR имеет поддерживающие IP соединения с эмулируемой ЛВС. VR-A имеет (физические) соединения с центральным офисом компании и поддерживает для них протокол OSPF. Следовательно, он может маршрутизировать пакеты в сети 172.150.0/18 и 172.150.128/18. На маршрутизаторе VR-B работает протокол RIP в рамках сети филиала (через физическое соединение) и этот же протокол используется (через логическое соединение) для экспорта

[1]В оригинале ошибочно указан рисунок 1. *Прим. перев.*

префикса 172.150.64/18 маршрутизатору VR-A. VR-A анонсирует используемый по умолчанию маршрут через логическое соединение маршрутизатору VR-B. VR-C служит extranet-соединением для подключения базы данных на узле 172.150.128.1. Следовательно, VR-C анонсирует используемый по умолчанию маршрут через логическое соединение маршрутизатору VR-A. VR-A экспортирует только адрес 175.150.128.1 маршрутизатору VR-C. Это позволяет предотвратить проблемы с безопасностью остальной части корпоративной сети.

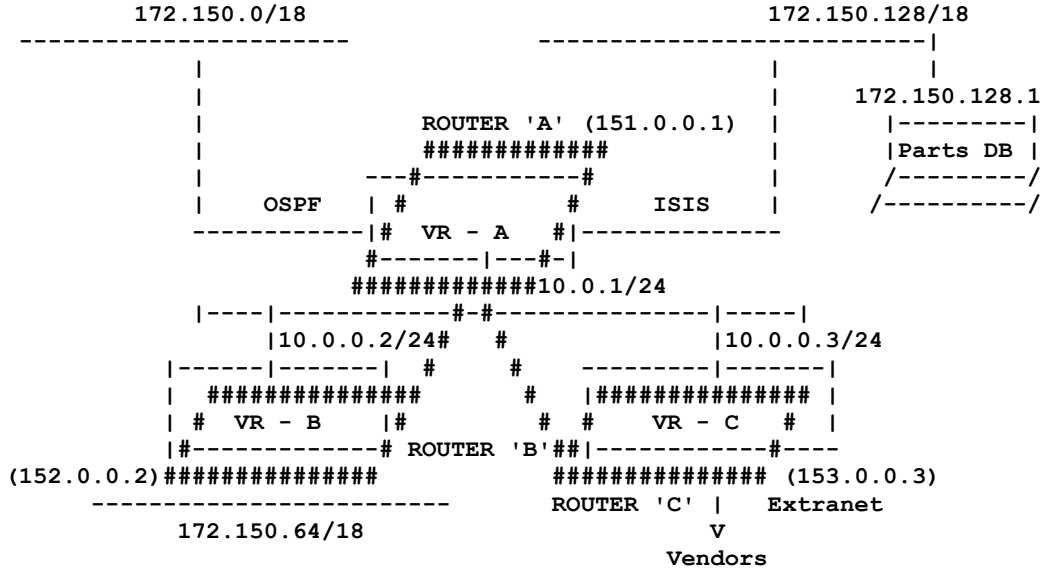

Рисунок 2. Виртуальный домен маршрутизации.

Администратор сети будет настраивать приведенную ниже конфигурацию.

1. Соединения OSPF с сетями 172.150.0/18 и 172.150.128/18 на VR-A.
2. Соединения RIP с VR-B и VR-C на VR-A.
3. Маршрутная политика на VR-A для анонсирования только маршрута по умолчанию в VR-B.
4. Маршрутная политика на VR-A для анонсирования только 172.159.128.1 в VR-C.
5. RIP на VR-B для VR-A.
6. RIP на VR-C для анонсирования маршрута по умолчанию в VR-A.

10. Пример обнаружения соседа

На рисунке 2[1] устройство SPED, на котором базируется VR-A (SPED-A) , использует публичный адрес 150.0.0.1/24, SPED-B - 150.0.0.2/24 и SPED-C - 150.0.0.3/24. Как отмечено выше, соединения между VR осуществляются через эмулируемую ЛВС. В приведенном примере VR-A использует адрес 10.0.0.1/24, VR-B — 10.0.0.2/24, VR-C - 10.0.0.3/24.

Предположим, что VR-A передает пакет VR-B. Для получения адреса VR-B (адрес SPED-B') VR-A отправляет ARP-запрос с адресом VR-B (10.0.0.2) в поле логического адреса. Логическим адресом отправителя будет 10.0.0.1, а «аппаратным» - 151.0.0.1. Запрос ARP инкапсулируется в групповой пакет данной VPN и передается. Копии этого пакета получают устройства SPED B и SPED-C. Устройство SPED-B распознает адрес 10.0.0.2 в контексте VPN 1 и передает отклик с «аппаратным» адресом 152.0.0.2. Этот отклик передается по групповому адресу VPN, чтобы результат ARP был доступен во всей сети (это обеспечивает снижение трафика).

Если обнаружения соседей не используется, нужна будет ручная настройка конфигурации. В приведенном примере на VR-A будет создана статическая запись ARP для VR-B с логическим адресом 10.0.0.1 и «аппаратным» адресом 152.0.0.2.

11. Пересылка

Как было отмечено выше при рассмотрении архитектуры, пересылка данных может осуществляться несколькими способами. Во всех вариантах, за исключением поэтапной (Hop-by-Hop) пересылки пакетов маршрутизации и управления, используемый метод задается конфигурацией. Наиболее быстрое обслуживание обеспечивается при рассылке на основе правил, наименее быстрое — при пересылке best effort через LSP общего пользования. Порядок предпочтений для методов пересылки показан ниже:

1. пересылка на основе правил;
2. пересылка через приватные LSP;
3. пересылка через публичные LSP (Best-effort).

11.1 Приватные LSP

Такие LSP могут настраиваться на уровне VPN. Обычно для таких LSP резервируется некая (отличная от 0) полоса пропускания и/или конкретный класс дифференцированного обслуживания или QOS. При доступности такого LSP он используется для передачи пользовательских данных и пересылки внутренних данных управления VPN.

[1] В оригинале ошибочно указан рисунок 1. *Прим. перев.*

11.2 Публичные LSP

Пакеты данных VPN пересылаются с использованием таких LSP, если приватные LSP с заданной полосой пропускания и/или параметрами QoS не организованы или не доступны по иным причинам. Такой LSP используется для выходного маршрутизатора в VPN 0. Значение VPNID из заголовка служит для демультиплексирования пакетов данных разных VPN на выходном маршрутизаторе.

12. Дифференцированные услуги

Организация приватных LSP для VPN позволяет сервис-провайдерам (SP) предлагать своим коммерческим заказчикам дифференцированные услуги. Такие приватные LSP могут связываться с любыми доступными L2 QoS или кодами Diff-Serv. В рамках VPN может быть организовано множество приватных LSP с разными классами обслуживания и профилями для распределения пакетов между этими LSP. Эта возможность, вкупе с масштабированием виртуальных маршрутизаторов позволяет SP обеспечивать реально дифференцируемые услуги пользователям VPN.

13. Вопросы безопасности

13.1 Безопасность маршрутизации

Использование стандартных протоколов маршрутизации (таких, как OSPF и BGP) в неизменном виде означает, что все методы шифрования и защиты (такие, как аутентификация соседей с применением MD5) полностью применимы для VR. Ответственность за отсутствие непредусмотренной утечки маршрутов из одной VPN в другую лежит на разработчиках. Одним из способов предотвращения таких утечек является поддержка раздельных таблиц маршрутизации и пересылки.

13.2 Безопасность данных

Это позволяет SP гарантировать заказчикам VPN, что пакеты данных одной VPN никогда не будут попадать в другие. С точки зрения маршрутизации это может быть достигнуто за счет поддержки раздельных маршрутных баз данных для каждого виртуального маршрутизатора. С точки зрения пересылки данных использование стеков меток в случае разделяемых LSP [Rosen2] [Callon] или использование приватных LSP гарантирует приватность данных. Дополнительно могут использоваться пакетные фильтры.

13.3 Безопасность конфигурации

Виртуальные маршрутизаторы с точки зрения PNA выглядят как физические устройства. Это означает, что PNA может настраивать их конфигурацию для обеспечения связности между корпоративными офисами. Обычно SP гарантирут, что доступ к VR на устройствах SPED имеют только PNA и указанные ими лица. Поскольку консоль виртуального маршрутизатора функционально эквивалентна консоли физического устройства, доступны все методы аутентификации пользователей, применяемые для физических консолей (пароли, RADIUS-аутентификация и т.п.).

13.4 Безопасность физической сети

При подключении PNA к устройству SPED для настройки или мониторинга VPN, администратор получает доступ к VR для VPN. PNA предоставлены только возможности настройки и мониторинга уровня только 3 в VR. В частности, PNA не имеет возможности настраивать конфигурацию физической сети. Это обеспечивает SP гарантии того, что администраторы VPN не могут нечаянно или осознанно воздействовать на сеть SP.

14. Мониторинг виртуального маршрутизатора

Все функции мониторинга физического маршрутизатора доступны и для виртуальных маршрутизаторов. К таким функциям относятся команды ping и traceroute. Кроме того, обеспечивается возможность просмотра приватных таблиц маршрутизации, баз данных о состояниях каналов и т. п.

15. Производительность

В целях обсуждения вопросов производительности и масштабирования современные маршрутизаторы можно рассматривать в двух плоскостях: маршрутизация (управление) и пересылка.

В плане маршрутизации большинство современных протоколов маршрутизации использует ту или иную методологию оптимизации расчетов для определения кратчайшего пути (путей) к конечным получателям. Например, в протоколах OSPF и ISIS применяется алгоритм Djikstra, а BGP использует Decision Process (процесс принятия решения). Эти алгоритмы основаны на разборе базы маршрутных данных и вычислении наилучшего пути к конечным получателям. Параметры производительности любого из этих алгоритмов основываются на топологических характеристиках (ISIS и OSPF) или числе AS на пути к получателям (BGP). Следует подчеркнуть, что связанные с расчетами накладные расходы в современных маршрутизаторах весьма малы. Это обусловлено тем, что используемые в расчетах «базы данных» в реальности являются структурами данных в оперативной памяти маршрутизатора.

Следовательно, можно сделать ряд заключений:

1. начало расчета маршрутов для домена маршрутизации не представляет собой ничего иного, кроме организации некоторых регистров для указания на объекты базы данных;
2. с учетом п. 1 производительность данного алгоритма не ухудшается значительно издержками на его организацию;
3. из п. 2 следует, что при расчете физическими маршрутизатором множества маршрутов для множества виртуальных маршрутизаторов сложность такого расчета определяется суммой издержек, связанных с маршрутными расчетами для отдельного виртуального маршрутизатора;

4. из п. 3 следует, что при использовании модели с наложением (overlay) или развертывании виртуальных маршрутизаторов параметры производительности маршрутизатора полностью определяются его аппаратными возможностями и выбором структур данных и алгоритмов.

Для иллюстрации предположим, что на физическом маршрутизаторе поддерживается N сетей VPN, для каждой из которых применяется некий протокол маршрутизации RP. Пусть средняя производительность алгоритма маршрутных расчетов в RP составляет f(X,Y), где X и y — параметры, определяющие производительность алгоритма в протоколе маршрутизации. Например, для алгоритма Djikstra, используемого в OSPF, X может задавать число узлов в области, а Y — число каналов. Производительность VPN с номером n выражается f(Xn, Yn). Производительность (физического) маршрутизатора будет представлять собой сумму f(Xi, Yi) для всех значений i в диапазоне 0 <= i <= N. Это заключение не зависит от выбора модели VPN (виртуальный маршрутизатор или наложение).

В обычной ситуации уровень пересылки использует два типа входных данных — таблицу маршрутизации и заголовки пакетов. Основным параметром производительности будет алгоритм поиска[1]. Очень быстрый поиск в таблице маршрутизации IP обеспечивается за счет организации таблицы в форме дерева и использования двоичных методов поиска. Производительность этого алгоритма составляет O(log n).

Следовательно, при использовании для виртуальных маршрутизаторов независимых таблиц производительность будет определяться постоянной величиной, связанной с выбором таблицы, и значением O(log n) для поиска в этой таблице маршрута. Это не хуже и не отличается от производительности любого маршрутизатора, а также не отличается от производительности маршрутизаторы, использующего для VPN модель наложения. Однако при интеграции маршрутизатором в модели с наложением таблиц маршрутизации множества VPN производительность будет задаваться O(log m*n), где m — число VPN, для которых поддерживаются таблицы маршрутизации.

16. Благодарности

Авторы благодарят Dave Ryan из Lucent Technologies за неоценимую глубину обзора этой версии документа.

17. Литература

[Callon] Callon R., et al., "A Framework for Multiprotocol Label Switching", Work in Progress.

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

[Meyer] Meyer, D., "Administratively Scoped IP Multicast", RFC 2365, July 1998.

[Rosen1] Rosen, E. and Y. Rekhter, "BGP/MPLS VPNs", RFC 2547, March 1999.

[Rosen2] Rosen E., Viswanathan, A. and R. Callon, "Multiprotocol Label Switching Architecture", Work in Progress[2].

18. Адреса авторов

Karthik Muthukrishnan
Lucent Technologies
1 Robbins Road
Westford, MA 01886
Phone: (978) 952-1368
EMail: mkarthik@lucent.com

Andrew Malis
Vivace Networks, Inc.
2730 Orchard Parkway
San Jose, CA 95134
Phone: (408) 383-7223
EMail: Andy.Malis@vivacenetworks.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

19. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.

[1] В таблице маршрутизации. *Прим. перев.*
[2] Работа завершена и опубликована в RFC 3031. *Прим. перев.*