

О методике построения корпоративных сетей передачи данных на базе технологии MPLS VPN

Нана Д. Григорян

Государственный педагогический университет им. Х.Абовяна
zgachak@dolphin.am

Аннотация

Статья посвящена попытке анализа методики построения корпоративных сетей передачи данных на базе технологии MPLS VPN (MultiProtocol Label Switching Virtual Private Network) - организации ВКС на базе многопротокольной коммутации IP-пакетов по меткам. Технология MPLS позволяет обеспечить управляемость, легкую наращиваемость, надежность и высокую готовность решений, необходимых для предоставления мультисервисных услуг организациям. Данный метод целесообразно использовать при создании КСПД единой информационной системы Армении, целью которой является повышение эффективности контроля и надзора за безопасностью и качеством продукции и услуг при их создании, поступлении и обращении на потребительском рынке Армении.

Одной из основных задач в сфере телекоммуникаций, особенно при построении корпоративных сетей передачи данных (КСПД), является определение оптимальной инфраструктуры проектируемой сети.

В данной статье делается попытка анализа методики построения корпоративных сетей передачи данных на базе технологии MPLS VPN (MultiProtocol Label Switching Virtual Private Network) - организации ВКС на базе многопротокольной коммутации IP-пакетов по меткам [1]-[8].

Многопротокольная коммутация по метке -MPLS- является технологией быстрой коммутации пакетов, работающей с любым протоколом сетевого уровня. MPLS сочетает в себе преимущества, изначально заложенные в технологию ATM, с точки зрения коммутации и гарантированного сервиса, и технологию IP, с точки зрения маршрутизации пакетов и оптимизации этой маршрутизации.

Применение технологии MPLS VPN позволит строить мультисервисные ВКС организаций на ресурсах публичной Интернет-сети, уменьшая тем самым необходимую общую пропускную способность сети для передачи разнородного трафика (по предварительным оценкам на 20-30 %) при меньшей стоимости передачи суммарного трафика и существенно большей динамике использования сетевых ресурсов.

Наибольшая разница между сервисами «виртуальных» каналов и виртуальными корпоративными сетями, кроме стоимости, состоит в различии транспортных характеристик. В случае MPLS VPN - корпоративные пользователи не имеют информации о реальной канальной емкости между точками присутствия (филиалами, сайтами). Данная емкость изменяется в соответствии с общим алгоритмом работы провайдерской.

операторской сети. Результат - потенциальная гибкость сетевых ресурсов и динамическое изменение характеристик сервиса. Чтобы конкретизировать неопределенность характеристик сервиса для потребителя, в договоре с ним определяется соглашение об уровне сервиса (Service Level Agreement-SLA-), которое провайдер обязуется соблюдать.

Главная идея MPLS заключается в создании механизмов для ускоренной передачи пакетов по наименее загруженным маршрутам и решение проблемы непредсказуемости задержек в IP-сетях.

Таким образом, MPLS представляет собой новаторскую технологию использования метода перепачи информации не по адресам, а по универсальным меткам. С помощью меток определяются и маршруты, и атрибуты услуг. На периферии сети, в точке входа, происходит обработка входящих пакетов. Здесь же выбираются и присваиваются метки. Опорная сеть считывает метки, обрабатывает соответствующим образом пакеты и передает их далее в соответствии с метками. Действия, требующие больших процессорных мощностей (анализ, классификация и фильтрация), выполняются только один раз, в точке входа. После этого пакеты с метками по простому алгоритму замены меток на Р-узлах передаются по опорной сети.

Архитектура КСПД и используемая в ней технология организации мультисервисных виртуальных корпоративных сетей MPLS VPN позволяют поддерживать большое число новых сетевых структур и защищенных мультисервисных услуг.

Для совместной работы организаций, а также их филиалов и подразделений, являющихся абонентами КСПД, создаются следующие основные функциональные сетевые структуры и соответственно формируются следующие услуги:

- интранет ВКС, позволяющие связать в единую корпоративную сеть на базе Интернет все географически распределенные филиалы и подразделения одной организации;
- экстранет ВКС, создающие междокуративные сети различных организаций для совместной работы;
- общий доступ к приложениям, т. е. доступ к общим вычислительным и информационным ресурсам, позволяющий многим потребителям использовать ресурсоемкие дорогостоящие приложения в режиме клиент-сервер;
- доступ к Интернет, т.е. доступ организаций к глобальным Интернет-услугам без ущерба для внутренних конфиденциальных процессов ведения бизнеса.

Безопасность передачи информации по MPLS-сети сравнима с безопасностью передачи по сетям с традиционными технологиями FrameRelay и ATM. MPLS обеспечивает защищенность передаваемой информации на базе разделения ВКС организаций аналогично разделению виртуальных каналов для FrameRelay и ATM, но если FrameRelay и ATM обеспечивают только базовый транспорт, MPLS поддерживает масштабируемые ВКС-сервисы и различные классы IP-приложений.

Следует, однако, отметить, что MPLS-сеть, обеспечивающая сравнимую с FrameRelay и ATM-технологиями безопасность передачи ВКС-информации, может не устраивать потребителей, желающих дополнительно использовать туннелирование (инкапсуляцию) и/или шифрование информации.

В этих случаях используется технология IPsec, которая предлагает дополнительную защиту поверх MPLS-сети.

IPsec-технология обеспечивает защищенность и целостность при передаче конфиденциальной информации.

IPsec обеспечивает безопасные коммуникации по IP-протоколу внутри локальных сетей, по частным и публичным сетям, через Интернет. Существенно, что IPsec работает на сетевом (достаточно низком) уровне, поэтому защищает IP-коммуникации для всех приложений и пользователей, является для них «прозрачным». Все распределенные

приложения, включая logon, client-server, e-mail, ftp, web-access и т.д. могут быть защищены.

Таким образом, IPSec, установленный на оборудовании потребителя в его точках присутствия, может дополнительно усилить защищенность передачи информации в его ВКС, образуя наложенную сеть (overlay structure) на MPLS-сети провайдера. Технология MPLS позволяет строить вложенные туннели, так как в ней используется механизм стека меток.

Существенно, что технология MPLS позволяет обеспечить управляемость, легкую наращиваемость, надежность и высокую готовность решений, необходимых для предоставления мультисервисных услуг организациям.

Если для организации-абонента КСПД важными характеристиками сервиса являются качество и безопасность передачи информации через публичную Интернет-сеть, то для провайдера не менее важными представляются вопросы предоставления и сопровождения указанных сервисов.

Предоставление сервиса ВКС автоматизируется с решением следующих вопросов управления:

- создание нового ВКС-узла;
- установка новой ВКС между заданными узлами;
- генерация сетевых конфигураций на основе запрошенных сервисов;
- мониторинг сети с целью обнаружения ошибок или проблем;
- мониторинг характеристик предоставляемых сквозных ВКС-сервисов, включая задержки, джиттер, число сбитых IP-пакетов и т.п.
- создание процедур для отслеживания неисправностей, сбоев и их устранения.

Кроме этого, в КСПД используется возможность сегментирования ВКС с целью расширения предложений абонентского управления. В перспективе организациям могут предоставляться такие сервисы управления, как мониторинг характеристик собственных корпоративных сетей, сбор статистики и самообслуживание в плане авторегистрации на нужный сервис.

Система управления безопасностью в сети провайдера не только отслеживает безопасный доступ к сетевым ресурсам, но также обеспечивает механизмы для реализации и соблюдения политики безопасности между ВКС.

Выводы

1. Технология MPLS позволяет обеспечить управляемость, легкую наращиваемость, надежность и высокую готовность решений, необходимых для предоставления мультисервисного доступа абонентам КСПД, а также решает следующие основные задачи:

- передачи мультимедийного трафика с гарантированным уровнем сервиса;
- определения оптимальных маршрутов и маршрутизации потоков данных с учетом приоритетов разнородного трафика;
- обеспечения конфиденциальности передаваемой информации и защиты ее от несанкционированного доступа;
- анализа сетевых информационных потоков с учетом характеристик функционирования приложений в узлах сети;
- регистрации трафика с целью возможности автоматизации биллинговых расчетов с потребителями при передаче трафика;
- иерархического распределенного управления сетью;
- обеспечения надежности функционирования сети.

2. Использование рассматриваемого метода при создании глобальных корпоративных сетей, в том числе и сети передачи данных единой информационной системы Армении обеспечит «мультисервисность», т.е. одновременную передачу данных, голоса и видео или их комбинаций с требуемым для потребителя качеством. Созданная на базе современной инновационной технологии (MPLS VPN) сеть будет гибкой и в высокой степени масштабируемой, что дает возможность наращивать сервисы как количественно (по числу потребителей услуг, по числу и типу обслуживаемых ВКС, по числу общих информационных и вычислительных центров), так и качественно, посредством введения новых типов современных передовых сервисов.

Литература

- [1] М. Шестаков, Принципы построения корпоративных сетей передачи данных, «Компьютерра», № 256, 1997 г.
- [2] М. Захватов, Построение виртуальных частных сетей (VPN) на базе технологии MPLS. Руководство Cisco., 2001 г.
- [3] Edited by Jeff Doyle and Matt Kolon. McGraw-Hill/Osborne // Juniper Networks Routers: The Complete Reference, 2002.
- [4] Ivan Pepelnjak, Jim Guichard elnjak, Jeff Apcar. Cisco Systems // MPLS and VPN Architectures, Vol. 2, 2004.
- [5] R. Aggarwal et al., Multicast in 2547 VPNs and VPLS, Internet Draft, Work in progress, <http://www.ietf.org/internet-drafts/draft-raggarwa-l3vpn-mvpn-vpls-mcast-01.txt> November, 2004.
- [6] R. Aggarwal, D. Papadimitriou, S. Yasukawa (Editors) et al., Extensions to RSVP-TE for Point to Multipoint TE LSPs // Internet Draft, Work in progress, <http://www.ietf.org/internet-drafts/draft-ietf-mpls-rsvp-te-p2mp-01.txt> November, 2004.
- [7] В. Олвейк, Структура и реализация современной технологии MPLS., 2004 г.
- [8] Y. Serbest, Ray Qiu, Rob Nath. Supporting IP Multicast over VPLS, February, 2005, <http://www.ietf.org/internet-drafts/draft-serbest-l2vpn-vpls-mcast-02.txt>

PLS տեխնոլոգիայի հիման վրա տվյալների հաղորդման կորպորատիվ ցանցերի կառուցման մեթոդիկայի վերլուծությունը

Ն. Գրիգորյան

Ամփոփում

Հոդվածը MPLS տեխնոլոգիայի հիման վրա տվյալների հաղորդման կորպորատիվ ցանցերի կառուցման մեթոդիկայի վերլուծության փորձ է:

MPLS տեխնոլոգիան թույլ է տալիս ապահովել այն որոշումների կարգավորելիությունը, արագ աճն ու հուսալիությունը, որոնք անհրաժեշտ են կազմակերպություններին բազմազան ծառայությունների մատուցելու համար:

Տվյալ մեթոդը մատակարարում է օգտագործել Հայաստանի միասնական տեղեկատվական համակարգի տվյալների հաղորդման կորպորատիվ ցանց ստեղծելու ժամանակ: