Журнал «Вестник связи», №2, 2005

«СОЛЯНКА» ПРО MPLS

А.А. АТЦИК, инженер ЛОНИИС,
А.Б. ГОЛЬДШТЕЙН, начальник сектора ЛОНИИС

Как правило, в начале статьи принято обосновывать актуальность обсуждаемого вопроса и формулировать ключевые тезисы, однако в данном случае часть этих процедур представляется ненужной, а другая – невозможной.

Действительно, актуальность технологии MPLS очевидна, поэтому мы зададимся вопросом как она применяется сегодня. Назвать эту статью обзором или аналитическим исследованием вариантов реализации вряд ли можно. Так получилось, что попытка проанализировать виды оборудования и решения на базе технологии MPLS привела к необходимости обсуждения целого ряда вопросов, которые с трудом укладываются в единый материал. Поэтому авторам осталось лишь объединить обсуждаемые вопросы по принципу "солянки" и попытаться упорядочить их хотя бы по времени возникновения. Итак, начнем.

Основы технологии и протоколов MPLS описаны в недавно вышедшей монографии [1]. Однако, следует отметить, что при кажущейся простоте идеологии, MPLS таит довольно большое число сюрпризов и распространенных заблуждений. Изначально задумывавшаяся как средство для упрощения сопряжения сетей IP и ATM, а также для снижения нагрузки на маршрутизаторы, MPLS достигла своей популярности, благодаря реализованным на ее основе приложениям, таким как инжиниринг трафика TE (Traffic Engineering), виртуальные частные сети (VPN), Fast ReRoute (FRR), обеспечение качества обслуживания QoS (Quality of Service). Более того, именно реализация QoS, возможности MPLS VPN и TE вывели ее на лидирующие позиции.

Другим технологиям, некогда считавшимся перспективными и призванным решать схожие задачи, пришлось довольствоваться ролью встроенных в MPLS механизмов. В связи с этим, нам следует немного вернуться к основам и прояснить ряд моментов, которые часто не совсем верно интерпретируются при обсуждении MPLS.

MPLS-маршрутизаторы

Как раз при попытке описать варианты реализации оборудования MPLS у авторов и возникли первые сложности. Основными элементами сети MPLS являются устройства LSR (Label Switching Router) – маршрутизаторы, способные назначать и анализировать метки MPLS, принимать на основе значения метки решение о дальнейшей пересылке пакета по сети, т. е. осуществлять коммутацию по меткам. Что же представляют собой эти устройства и чем они отличаются от обычных

маршрутизаторов IP-сетей? Существуют ли в действительности эти отличия, и насколько они принципиальны?

На второй вопрос большинство с уверенностью отвечает утвердительно, имея в виду, что IP-маршрутизаторы маршрутизируют пакеты на основе обработки IP-заголовка, а LSR работают только с метками. Казалось бы все очевидно.

Дело в том, что среди сетевых специалистов, не занимающихся непосредственно MPLS, распространено мнение, что LSR – это простое устройство, основным требованием к которому является поддержка таблиц коммутации по меткам и ее осуществление. При этом LSR не обязано уметь читать заголовки протоколов сетевого уровня, за исключением случаев, когда оно устанавливается на границе MPLS-домена.

Логика этого утверждения проста: раз мы анализируем и классифицируем пакеты только на входе сети (что является одной из основных идей MPLS), то маршрутизаторы MPLS-ядра могут быть избавлены от этой функции, что несомненно значительно снизит их стоимость.

В действительности это не совсем верно. Узлы LSR должны как минимум унаследовать от IP-маршрутизаторов поддержку протоколов маршрутизации IP-сетей (таких как OSPF или IS-IS) для вычисления маршрутов путей коммутации по меткам LSP (Label Switched Path) в сети, что соответствует принципам работы MPLS. А если вспомнить, что протокол LDP (Label Distribution Protocol) – основной инструмент базовой версии MPLS для распространения меток – устанавливает свои LDP-сессии поверх TCP-соединения, то станет ясно, что по своей функциональности LSR вынужден приближаться к IP-маршрутизатору.

При этом постановка второго вопроса теряет строгость и четкость. На первый план выходит то, что при работе MPLS постоянно возникает необходимость в обычных IP-соединениях и получается, что маршрутизатору LSR необходимо иметь всю функциональность IP-маршрутизатора.

Таким образом, ответить на вопрос о разнице между LSR и IP-маршрутизатором с точки зрения их реализации можно так: LSR – это IP-маршрутизатор с поддержкой MPLS. Не больше, но и не меньше.

Посмотрим, что же входит в понятие "поддержка MPLS", превращающее обыкновенный маршрутизатор в LSR. Для этого нам придется составить минимальные требования к LSR. Во-первых, LSR должен уметь читать как метки, так и заголовки протокола сетевого уровня, а также различать на входе пакеты, снабженные меткой и без нее. После этого пакеты с меткой должны пройти процедуру Label Swapping и отправляться на соответствующий порт, согласно таблице коммутации по меткам.

Таким образом, LSR должен поддерживать таблицы коммутации по меткам и уметь осуществлять такую коммутацию. Для формирования вышеуказанной таблицы LSR должен поддерживать упоминавшиеся протоколы маршрутизации и протокол LDR причем последний потребует еще и транспорта TCP.

Пакеты без метки поступают из первого классификатора, назовем его MPLS-классификатор, на адресный классификатор, задачей которого является доставка пакета на основе его IP-заголовка. Таким образом, либо осуществляется традиционная маршрутизация IP-пакета, либо, если адресатом является сам LSR, пакет доставляется на классификатор портов, распределяющий приходящие пакеты по различным служебным подсистемам. Общая структура MPLS-узла показана на рис. 1.

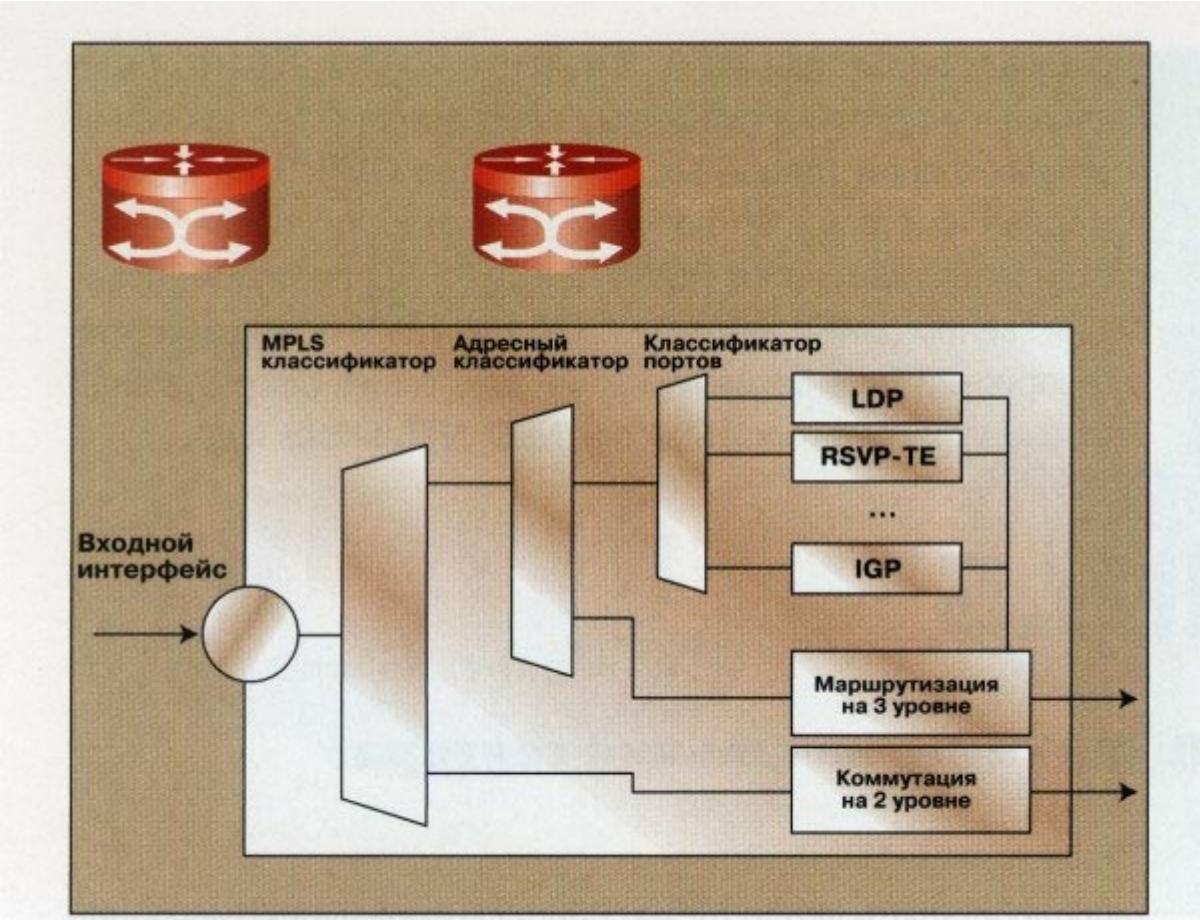

Рис. 1. Структура LSR

Если узел LSR будет находиться в граничной области, то его входные интерфейсы, обращенные наружу от MPLS-домена, должны быть сконфигурированы так, чтобы пакеты, которые должны быть переданы через сеть MPLS попадали на FEC-классификатор и после присвоения им метки пересылались в область MPLS-ядра.

Поскольку обмен служебными сообщениями в MPLS часто происходит между парой соседних маршрутизаторов, то снабжать такие пакеты меткой нет смысла. Поэтому сообщения всех служебных протоколов, таких как OSPF(TE), IS-IS(TE), (CR-)LDP, BGP, RSVP(-TE) пересылаются без меток. Исключением может служить протокол IS-IS, который предусматривает возможность передачи своих сообщений в пакетах, снабженных меткой.

Получается, что для дальнейшего понимания необходимо обратиться к базе данных меток LSR. В противном случае суть работы оборудования MPLS ускользает.

Forwarding Information Base

Forwarding Information Base (FIB) состоит из трех компонентов:

Next Hop Label Forwarding Entry (NHLFE), содержащего информацию о следующей пересылке (next-hop), в частности интерфейсе и адресе, а также инструкции по обработке метки (Label Swapping, удаление). К тому же он может содержать данные о кодировании метки, инкапсуляции на втором уровне и другую информацию, необходимую для обработки пакета;

Incoming Label Map (ILM), определяющего привязку входных меток к соответствующим NHLFE;

FEC-to-NHLFE map (FTN), определяющего привязку каждого FEC к NHLFE.

Как ILM, так и FTN могут содержать привязку не к одному NHLFE, а к нескольким, но перед обработкой пакета должен быть выбран конкретный NHLFE согласно некоторому алгоритму. Использование таблиц ILM и FTN зависит от роли, отведенной LSR на данном LSP: если он является входным, то необходимо обратиться к FTN, если транзитным – к ILM.

Данная структура рекомендована комитетом IETF, но конкретные реализации производителей могут отличаться. Структура LSR, представленная на рис. 1, с точки зрения базы данных FIB может быть проиллюстрирована алгоритмом, показанным на рис. 2.

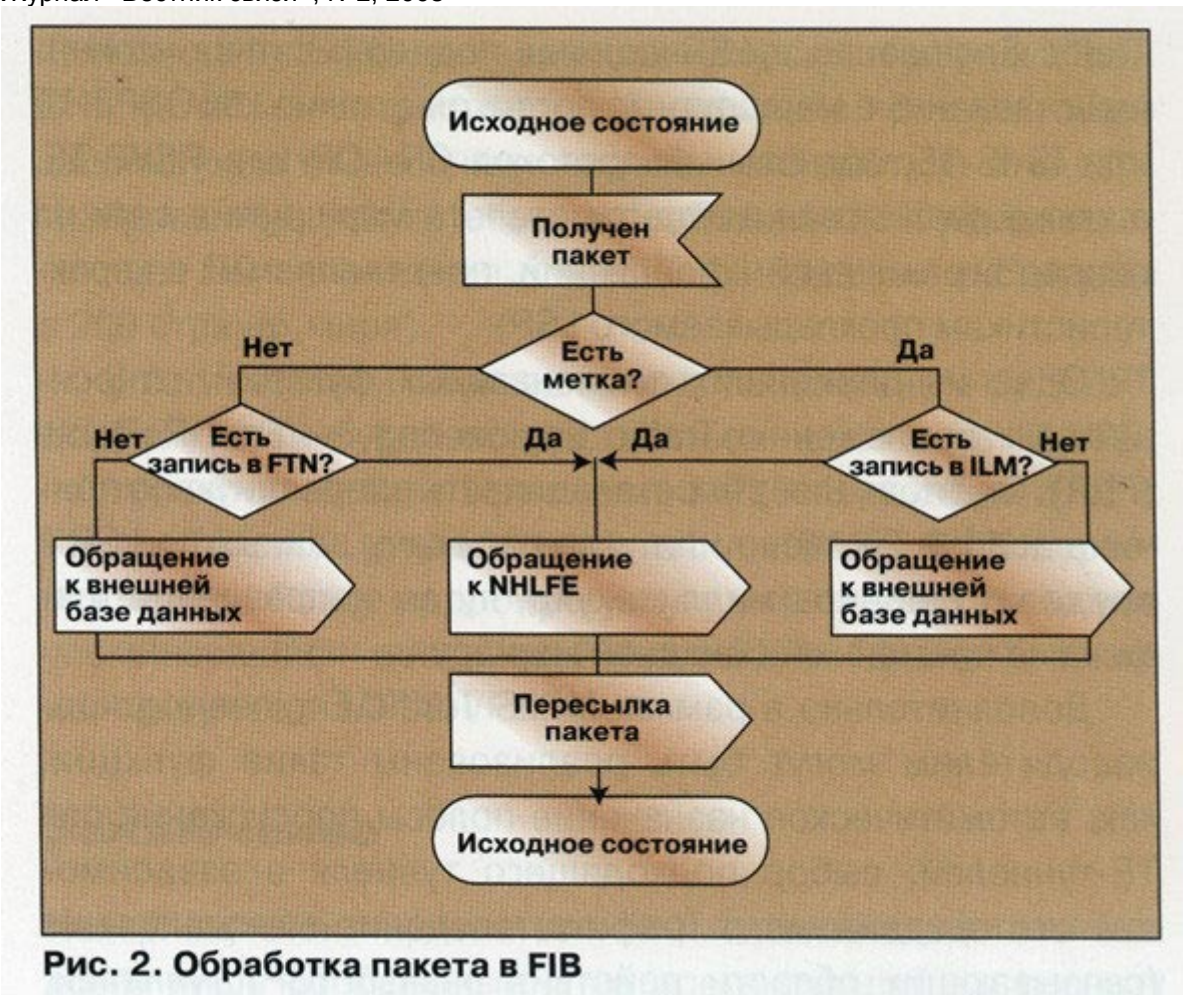

Рис. 2. Обработка пакета в FIB

Благодаря наличию адресного классификатора и возможности обращения к внешней базе данных (таблице маршрутизации) в случае отсутствия записи в FTN достигается удобное сопряжение сетей IP и IP/MPLS.

Мы выяснили, что значит поддержка маршрутизаторами технологии MPLS. Теперь разберемся, как она осуществляется и какими дополнительными возможностями обладают современные LSR. Здесь мы снова делаем небольшой шаг в сторону и задаем вопрос...

SOFTWARE или HARDWARE?

Не секрет, что львиная доля функциональности современных маршрутизаторов, а соответственно и LSR, обеспечивается установленным программным обеспечением (ПО). Примером может служить ПО Cisco IOS Software: оно имеет несколько версий, различающихся реализованными возможностями. Каждая версия обладает набором функций Feature Set, которые устанавливаются в зависимости от применения маршрутизатора. В дальнейшем к конкретному Feature Set можно добавить дополнительные функции, благодаря модульности ПО.

На примере данного программного пакета легко показать, как маршрутизаторы превращались в LSR. Cisco IOS Software предназначено для установки на IP-маршрутизаторы Cisco, и только начиная с версии 12.0 ПО Cisco IOS Software начинает включать в себя поддержку MPLS. Таким образом, если платформа поддерживает необходимую версию ПО, то она может иметь функции MPLS.

В оборудовании Cisco на сегодняшний день MPLS в той или иной степени поддерживают маршрутизаторы старших серий, начиная с 3600, а также маршрутизатор 2691 из 2600 серии и некоторые коммутаторы Cisco Catalyst.

Наряду с программной поддержкой функций MPLS, часть производителей оборудования выпускает специализированные устройства с аппаратной поддержкой MPLS. Иллюстрацией может служить оборудование компании Juniper Networks, которая имеет свой собственный программный пакет JUNOS, аналогичный уже упомянутому, но и реализует в своем оборудовании аппаратную поддержку MPLS. Для этого могут применяться различные решения, например, использование программируемых логических матриц FPGA (Field-Programmable Gate Arrays), как это делает компания Marvell, или специализированных интегральных схем ASIC (Application Specific Integrated Circuit), нашедших свое место в оборудовании Riverstone Networks.

Аппаратная поддержка имеет сторонников и противников, положительным моментом будет упрощение и ускорение аппаратно-реализуемых функций, однако в дальнейшем оператору может потребоваться модернизация, которая при аппаратной реализации, несомненно, обойдется ему существенно дороже, чем обновление ПО.

Казалось бы логичным теперь поговорить о том, что же могут маршрутизаторы MPLS, т. е. перейти к рассмотрению дополнительных функций MPLS, которые встречаются в маршрутизаторах LSR. Однако это напрямую связано с дополнительными возможностями самой технологии, о которых мы упомянули в начале статьи, назвав их чуть ли не главными при использовании MPLS.

О возможностях MPLS

Одним из наиболее востребованных приложений MPLS является Traffic Engineering (TE), представляющий собой методы и механизмы достижения сбалансированности загрузки всех ресурсов сети за счет рационального выбора путей прохождения трафика через сеть. Для решения задач Traffic Engineering в LSR должны поддерживаться усовершенствованные маршрутные протоколы, такие как OSPF-TE или IS-IS-TE, сигнальный протокол CR-LDP или RSVP-TE, а также реализован алгоритм расчета маршрута в сети на основе ограничений (требований, предъявляемых к характеристикам прокладываемого LSP).

Одна из ценнейших опциональных функций, относящихся к приложению Traffic Engineering, – Fast ReRoute (FRR). Она позволяет восстанавливать прерванную по причине аварии на звене или узле передачу данных по LSP в пределах десятков миллисекунд, путем направления трафика на временный обходной маршрут.

Дополнительно в рамках MPLS Traffic Engineering производителем могут быть реализованы такие функции, как: автоматическое назначение полосы пропускания для TE-туннелей; выбор подходящего туннеля в зависимости от передаваемого трафика; создание межзональных (связывающих области действия разных IGP) туннелей; исключение ресурса, имеющего определенный IP-адрес, при расчете маршрута LSP; возможность объявления протоколу IGP TE-туннеля, как обыкновенного звена и некоторые другие.

Здесь следует упомянуть о том, что некоторые производители уже реализуют поддержку не до конца специфицированной комитетом IETF технологии DiffServ-aware MPLS-TE, требующей наличия дополнений к маршрутным и сигнальным протоколам и обеспечивающей гарантии по полосе пропускания для каждого из классов DiffServ. Это одна из наиболее перспективных технологий для обеспечения гарантированного уровня QoS в IP-сетях.

Другим известным и популярным приложением в MPLS является MPLS-VPN. Для предоставления этой услуги достаточно, чтобы LSR, через которые происходит подключение клиентских подсетей к магистральной сети оператора, поддерживали MPLS-VPN, остальные узлы могут ограничиться поддержкой MPLS.

Граничные LSR, называемые PE (Provider Edge), должны поддерживать протокол внешнего шлюза BGP-4 и его многопротокольное расширение MP-BGP, а также иметь сложную структуру маршрутных таблиц, при которой на каждый интерфейс маршрутизатора устанавливается отдельный IGP-модуль. Таким образом на одном маршрутизаторе организуется несколько виртуальных. Часто приложения MPLS-VPN и MPLS-TE совмещаются для повышения качества услуги VPN.

Производитель может расширить возможности MPLS-VPN, добавив такие опции как: перенос протоколом BGP, наряду с маршрутами, MPLS меток для них; функции, позволяющие одному провайдеру сдавать в аренду другому сегмент своей

магистральной сети; присвоение и использование идентификатора VPN; применение маршрутизации на основе политики (Policy-based routing) для выбора соответствующей таблицы маршрутизации на PE и ряд других.

Помимо функциональности, предназначенной для реализации тех или иных приложений, LSR может поддерживать дополнительные возможности для базовой MPLS-сети. Например, может быть задействовано поле Class of Service формата MPLS метки для обслуживания разнородного трафика в сети. Также в сеть MPLS могут быть перенесены такие знакомые утилиты IP-сетей, как Ping и Traceroute. Может быть организована поддержка уведомительных сообщений SNMP (traps) для некоторых критических событий в работе протокола LDP. Также существует возможность переноса информации о классе DiffServ, копируемом из IP-заголовка и переносимого в метке.

Не следует забывать и об активно развиваемой компанией Cisco технологии AToM (Any Transport over MPLS), позволяющей работать поверх MPLS различным технологиям и протоколам: Ethernet, ATM, Frame Relay, HDLC и PPP.

Что же происходит на российском рынке?

MPLS в России

Можно смело утверждать, что на российском телекоммуникационном рынке представлено оборудование для MPLS-сетей большинства ведущих мировых производителей и оно пользуется высоким спросом, вызванным проектами новых мультисервисных и модернизацией существующих IP-сетей. Самым ярким примером является первая Мультисервисная IP/MPLS-сеть, которая была построена в Краснодарском крае ОАО "Южная телекоммуникационная компания" осенью 2002 г., с использованием оборудования Cisco Systems.

На сегодня в России одной из крупнейших IP/MPLS-сетей обладает компания "ТрансТелеКом". Эта сеть, построенная компанией "Миктротест" на базе оборудования Cisco, предоставляет 57 % услуг IP VPN в России. В качестве основной транспортной среды для IP-сети используются каналы первичной сети уровня STM-1, с перспективой наращивания до уровня STM-4 и STM-16.

Ядром сети являются высокопроизводительные коммутирующие маршрутизаторы. Граничный слой состоит из маршрутизаторов Cisco Systems, обеспечивающих агрегирование клиентского трафика абонентов IP-сети и коммутаторов Fast Ethernet для объединения инфраструктуры узла и подключения оборудования пользователей.

В состав IP-сети входит система управления устройствами и услугами, а также комплекс серверов, обеспечивающих традиционные Интернет-сервисы, такие как DNS, SMTP, WWW. Помимо уже упомянутой услуги MPLS-VPN "ТрансТелеКом" предоставляет с использованием MPLS доступ в Интернет и услуги IP-телефонии.

Первым же услуги IP VPN на базе MPLS стал предоставлять провайдер "Раском" и чуть позже "Эквант". MPLS поддерживается на всех узлах магистральной сети Раскома. Его сеть полностью строится на оборудовании Cisco. Основу ее составляют мощные маршрутизаторы Cisco GSR 12000, устанавливаемые на московской и питерской площадках. Каждый из них обеспечивает пропуск до 40 Гбит/с трафика по сети. Клиентский трафик агрегируется маршрутизаторами Cisco 7000, соединенными с опорной сетью гигабитными оптическими интерфейсами.

В настоящее время поэтапный переход на использование MPLS осуществляет крупнейший российский Интернет-провайдер "РТКомм.Ру", самыми известными акционерами которого являются ОАО "Связьинвест", ОАО "Ростелеком" и ОАО "РТК-Лизинг". Основа сети компании – магистральная сеть Ростелекома, взятая в аренду. На 78 из 132 узлов уже используется технология MPLS.

Оборудование IP/MPLS функционирует в сети передачи данных общего пользования компании МГТС, доступ к которой осуществляется по существующей кабельной распределительной сети МГТС с использованием технологии xDSL. Основа сети – магистральное ядро, которое объединяет 10 мощных узлов пакетной коммутации, соединенных по волоконно-оптическим линиям каналами STM 16 (технология IP/MPLS) и STM 4 (технология ATM).

Первое кольцо – это основная рабочая магистраль, второе служит "горячим" резервом для первого, а также выполняет служебные и технологические функции для ряда систем МГТС. В магистральных узлах сети, установлены маршрутизаторы Cisco GSR 12012 и концентраторы Cisco 6400.

Другой московский MPLS-проект реализован компанией "Комстар", теперь объединившейся с "Телмос" и "МТУ-Информ" под общим названием "Комстар-объединенные системы". Но строительство MPLS-сети она начала еще в одиночку в начале 2003 г. Сеть создавалась на оборудовании Riverstone Networks, совместимом с коммутаторами и мультиплексорами Alcatel, на которых построены сети ATM/Frame Relay компании "МТУ-Информ", что естественно способствовало слиянию. На MPLS-сети Комстара внедрены приложения Traffic Engineering и Fast ReRoute, предоставляются услуги VPN, как на третьем уровне, так и на втором (VPLS).

Но проникновение технологии MPLS происходит не только в Москве и у крупнейших провайдеров и операторов. MPLS можно обнаружить у операторов по всей стране: MPLS сеть функционирует у Уралсвязьинформа, Северо-Западный Телеком также ведет строительство мультисервисной сети с использованием MPLS. В октябре 2003 г. небезызвестная компания Голден Телеком" объявила о заключении соглашения с компанией AT&T о предоставлении доступа к защищенной IP-сети SWIFT Secure IP Network – SIPN на территории России и других стран СНГ (SWIFT – отраслевое объединение, оказывающее защищенные от несанкционированного доступа стандартизированные услуги обмена сообщениями и предоставляющее ПО сопряжения для 7500 финансовых институтов в 200 странах мира).

В соответствии с соглашением, заключенным со SWIFT, доступ к сети будет осуществляться через сеть IP VPN, построенную на базе технологии MPLS. В декабре 2003 г. Голден Телеком успешно подключил к SWIFT SIPN первого клиента. Ранее подобную услугу уже предоставлял уже упоминавшийся российский провайдер "Эквант", также используя сеть MPLS-VPN.

Заключение

Наверное, стоит признаться, что первоначально это был всего лишь обобщенный и не претендующий на полноту обзор MPLS-решений в России, призванный продемонстрировать, как относительно молодая технология MPLS прочно закрепляется на отечественном рынке, как на ее базе реализуется ряд масштабных национальных и международных проектов.

Но обращение к техническим аспектам представляется авторам не менее важной частью статьи, и можно лишь с сожалением отметить, что многое осталось за ее рамками. Отчасти это компенсируется монографией [1], где рассмотрены вопросы назначения меток при организации туннелей, переход к GMPLS, взаимодействие протоколов при работе MPLS сети и др. Однако эволюция этих подходов в процессе их реализации в сетях операторов связи требует отдельного анализа и обсуждения.

Данная же статья всего лишь "солянка", первое блюдо, призванное пробудить аппетит истинного гурмана

.

Литература

1. А.Б. Гольдштейн, Б.С. Гольдштейн. Технология и протоколы MPLS/.-/СПб.: БХВ.,2005.