Проблемы перехода к мультисервисным сетям

А.Б. ГОЛЬДШТЕЙН, начальник сектора ЛОНИИС

Постановка проблемы

Общие принципы построения мультисервисной сети выглядят, на первый взгляд, очень просто – транспортные каналы и протоколы, способные передавать информацию любого типа (речь, видео, данные и т. п.), плюс оборудование доступа к такой сети и разнообразные терминальные устройства. А сегодня и того проще – объединить существующие сети разных операторов (традиционные ТфОП, сети мобильной связи и IP-сети) в единую сеть, и проблема будет решена. Это же можно назвать конвергенцией существующих сетей разных операторов и технологий, что является общепринятым решением проблемы. Но это «просто» только на первый взгляд.

Сегодня еще нет технологий, которые бы полностью удовлетворяли запросам перспективной мультисервисной сети. Однако технологические решения, способные стать ее основой, существуют уже сейчас, т. е. можно построить прообраз мультисервисной сети, который со временем сможет легко эволюционировать к мультисервисной сети будущего. Для простоты (и в соответствии с устоявшейся терминологией) назовем промежуточную сеть-прообраз конвергентной (К-сетью), а мультисервисную сеть следующего поколения – М-сетью (рис. 1).

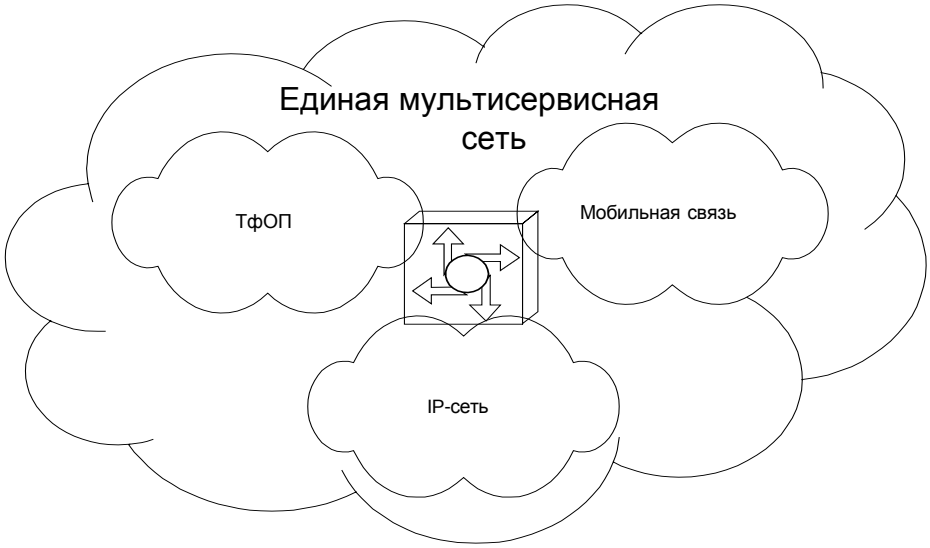

Рис. 1. Мультисервисная сеть связи

На чем же базируется конвергентная сеть? Прежде чем ответить на этот вопрос, перечислим требования, которым она должна удовлетворять. Если ограничиться основными требованиями, то их будет всего три:

во-первых, обеспечение передачи данных,

во-вторых, обеспечение передачи трафика реального времени,

в-третьих, обеспечение гарантированного качества обслуживания QoS.

И, конечно же, нельзя забывать о системах управления современными сетями. Т. е. необходимо наметить четыре направления (рис. 2), которые приведут нас к сети будущего.

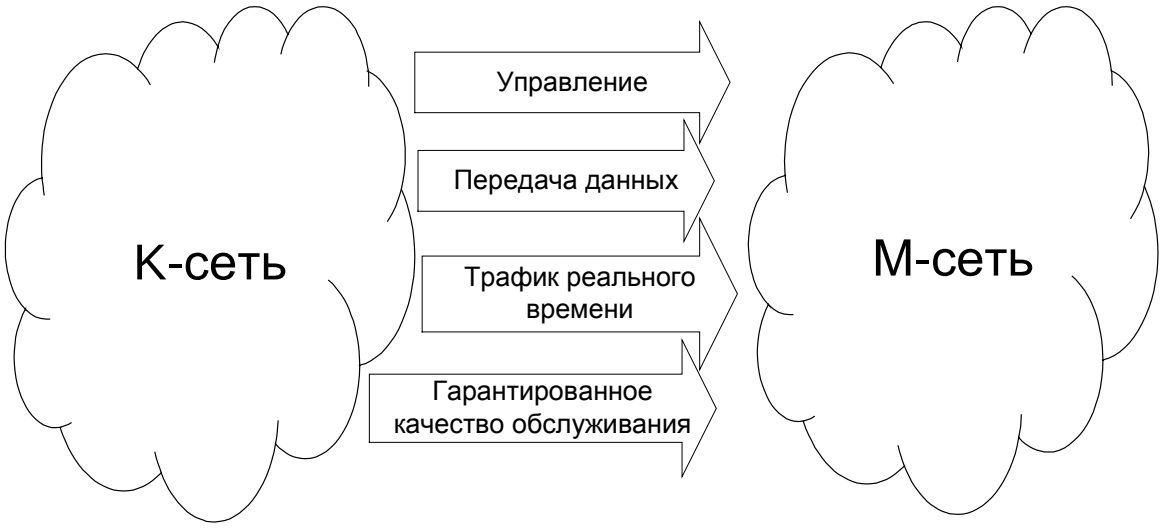

Рисунок 2. Направления развития сети

Прежде всего, следует подобрать для транспортной сети такую технологию, которая удовлетворяла бы всем трем требованиям. Но при этом нельзя упускать из виду, что наша сеть должна «вписаться» в сегодняшнюю сетевую инфраструктуру и иметь возможность совершенствоваться. Логичнее всего отталкиваться от наиболее развитой сегодня технологии, т. е. TCP/IP, и взять за основу протокол IP. Он прекрасно удовлетворяет первому требованию и благодаря технологии VoIP (передачи речи по IP сетям) отвечает второму. Но как же быть с третьим? Ведь протокол IP абсолютно не приспособлен для того, чтобы обеспечивать гарантированное качество обслуживания.

Итак, IP не идеален. Может быть его главный конкурент - технология ATM - окажется лучше, ведь она удовлетворяет всем вышеназванным требованиям? Но здесь возникает проблема стоимости оборудования ATM, значительно превышающей стоимость оборудования IP. Да и развитость сетей на основе IP сильно выигрывает по сравнению с ATM-сетями, а ведь мы собираемся развить нашу конвергентную К-сеть настолько, чтобы она превратилась в единую мультисервисную М-сеть.

Решение для транспортной сети: MPLS-подход

Получается, что определить какой из протоколов, IP или ATM, будет играть главную роль в единых мультисервисных сетях будущего (и в нашей строящейся сети), весьма непросто, но если рассматривать сегодняшние тенденции построения сетей, то несомненным лидером в транспортных технологиях является MPLS – многопротокольная коммутация по меткам. Действительно, споры продолжаются, а сети MPLS строятся (в том числе и на территории СНГ). К тому же, технология MPLS вполне удовлетворяет нашим требованиям и лишена недостатков ATM.

Стоимость оборудования MPLS, по сравнению с ATM, не пугает, а метод коммутации по меткам реализуется весьма удачно. На входе в сеть MPLS IP-адресу ставится в соответствие короткий идентификатор определенного формата, которым и оперируют маршрутизаторы MPLS, так что им не нужно тратить время на разбор заголовков пакетов, благодаря чему существенно сокращается общее время передачи.

Реализуется передача данных любого вида, MPLS может работать и «поверх» IP, и «поверх» ATM, обеспечивается гарантированное качество обслуживания. Разработки оборудования ведутся многими ведущими компаниями, например Cisco Systems, Alcatel, Avaya и др. Таким образом, реализация проекта транспортной сети на базе MPLS не должна вызвать особых затруднений.

В обычных IP-сетях любой маршрутизатор, находящийся на пути следования пакетов, анализирует заголовок каждого пакета, чтобы определить, к какому потоку этот пакет относится, и выбрать направление для его пересылки к следующему маршрутизатору. При использовании технологии MPLS соответствие между пакетом и потоком устанавливается один раз на входе в сеть MPLS. Более точно соответствие устанавливается между пакетом и так называемым “классом эквивалентности пересылки” FEC (Forwarding Equivalence Class). К одному FEC относятся пакеты всех потоков, пути следования которых через сеть MPLS (или через часть этой сети) совпадают в том смысле, что с точки зрения выбора очередного маршрутизатора пакеты этих потоков неразличимы. Пакеты снабжаются метками – идентификаторами небольшой и фиксированной длины, которые определяют принадлежность каждого пакета тому или иному FEC.

Метка имеет локальное значение – она действительна на участке между двумя соседними маршрутизаторами, являясь исходящей меткой определенного FEC для одного из них и входящей – для второго. Второй маршрутизатор, пересылая пакет этого FEC к следующему маршрутизатору, снабжает его другой меткой, которая идентифицирует тот же FEC на следующем участке маршрута, и т. д. Таким образом, каждый FEC имеет свою систему меток.

Использование меток значительно упрощает процедуру пересылки пакетов, так как маршрутизаторы обрабатывают не весь заголовок IP-пакета, а только метку, что занимает значительно меньше времени.

Простейшую MPLS-сеть функционально можно разделить на две области — ядро и граничную область. Ядро образуют устройства, минимальным требованием к которым является поддержка MPLS и участие в процессе маршрутизации трафика для того протокола, информация которого коммутируется с помощью MPLS, т.е. транзитные маршрутизаторы MPLS (Label Switching Routers - LSR).

Маршрутизаторы ядра занимаются только коммутацией. Все функции отнесения пакетов к тому или иному FEC, а также реализацию таких дополнительных сервисов, как фильтрация, явная маршрутизация, выравнивание нагрузки и управление трафиком, выполняют граничные LSR или пограничные маршрутизаторы MPLS (Label Edge Routers – LER).

Таким образом, интенсивные вычисления приходятся на граничную область, а высокопроизводительная коммутация выполняется в ядре, что позволяет оптимизировать конфигурацию устройств MPLS в зависимости от их местоположения в сети. По отношению к любому потоку пакетов, проходящему через MPLS-сеть, один LER является входным, а другой – выходным.

Входной LER анализирует заголовок пришедшего извне пакета, устанавливает, какому FEC он принадлежит, снабжает этот пакет меткой, которая присвоена данному FEC, и пересылает пакет к соответствующему LSR. Далее, пройдя в общем случае через несколько LSR, пакет попадает к выходному LER, который удаляет из пакета метку, анализирует заголовок пакета и направляет его к адресату, находящемуся вне MPLS-сети.

Последовательность ($LER_{вх}$, LSR_1, ... , LSR_n, $LER_{вых}$) маршрутизаторов, через которые проходят пакеты, принадлежащие одному FEC, образует виртуальный коммутируемый по меткам тракт LSP (Label Switched Path). Так как один и тот же LER для одних потоков является входным, а для других – выходным, в сети, содержащей N LER, в простейшем случае может существовать N(N-1) FEC и, соответственно, N(N-1) LSP.

Заметим, однако, что потоки пакетов из разных FEC, приходящие к одному выходному от разных входных LER, могут в каких-то LSR сливаться в более мощные потоки, каждый из которых образует новый FEC со своей системой меток. Возможно и обратное, т. е. группа потоков может идти до некоторого LSR по общему маршруту и, следовательно, принадлежать одному и тому же FEC, а затем разветвиться, и тогда каждая ветвь будет иметь свой FEC (со своей системой меток). Кроме того, существует возможность образования внутри некоторого LSP одного или нескольких вложенных в него LSP (так называемых LSP-туннелей).

То обстоятельство, что система меток, присваиваемых пакету, может изменяться, приводит к образованию в пакете так называемого “стека меток”. При переходе потока пакетов в другой FEC, метка нового FEC помещается поверх метки прежнего и используется для коммутации, а прежняя метка сохраняется под ней, но не используется до тех пор, пока не восстановится прежний FEC. Ясно, что если FEC пакета меняется несколько раз, в стеке накапливается несколько меток.

Все это, с одной стороны, демонстрирует, насколько широки возможности MPLS в части распределения ресурсов сети при ее проектировании и оперативного их перераспределения при эксплуатации, но, с другой стороны, предъявляет непростые требования к средствам, с помощью которых устанавливается соответствие “FEC-метка” в каждом LER и LSR сети.

Метка, помещаемая в некоторый пакет, представляет FEC, к которому этот пакет относится. Как правило, отнесение пакета к определенному классу производится на основе сетевого адреса получателя. Метка может быть помещена в пакет разными способами – вписываться в специальный заголовок, “вставляемый” либо между заголовками уровня звена данных и сетевого уровня, либо в свободное и доступное поле заголовка какого-то одного из этих двух уровней, если таковое имеется. В любом случае этот специальный заголовок содержит поле, куда записывается значение метки, и несколько служебных полей, среди которых имеется и поле QoS (три бита, т. е. до восьми классов качества обслуживания).

Метки для каждого FEC всегда назначаются “снизу”, т. е. либо выходным LER, либо тем LSR, который является для этого FEC “нижним” (расположенным ближе к адресату), и распределяются по тем маршрутизаторам, которые расположены “выше” (ближе к отправителю).

Распределение меток может быть независимым или упорядоченным. В первом случае LSR может уведомить вышестоящий LSR о привязке метки к FEC еще до того, как получит информацию о привязке “метка-FEC” от нижестоящего маршрутизатора. Во втором случае высылать подобное уведомление разрешается только после получения таких сведений “снизу”.

Метки могут выдаваться нижним маршрутизатором как по собственной инициативе, так и по запросу верхнего. Наконец, возможен “либеральный” или “консервативный” режим распределения меток. В либеральном режиме нижний LSR раздает метки вышестоящим LSR, как имеющим с ним прямую связь, так и доступным лишь через промежуточные LSR. В консервативном режиме вышестоящий LSR обязан принять метку, если ее выдает смежный LSR, но может отказаться от метки, пришедшей к нему транзитом.

Как уже отмечалось, метка должна быть уникальной лишь для каждой пары смежных LSR. Поэтому одна и та же метка в любом LSR может быть связана с несколькими FEC, если разным FEC принадлежат пакеты, идущие от разных маршрутизаторов, и имеется возможность определить, от которого из них пришел пакет с данной меткой. В связи с этим обстоятельством вероятность того, что пространство меток будет исчерпано, очень мала.

Для распределения меток может использоваться либо специальный протокол LDP (Label Distribution Protocol), либо модифицированная версия одного из существующих протоколов сигнализации (например, протокола RSVP).

Каждый LSR содержит таблицу, которая ставит в соответствие паре “входной интерфейс, входящая метка” пару “выходной интерфейс, исходящая метка”. Получив пакет, LSR определяет для него выходной интерфейс (по входящей метке и номеру интерфейса, куда пакет поступил). Входящая метка заменяется исходящей (записанной в соответствующем поле таблицы), и пакет пересылается к следующему LSR. Вся операция требует лишь одноразовой идентификации значений в полях одной строки таблицы и занимает гораздо меньше времени, чем сравнение IP-адреса отправителя с адресным префиксом в таблице маршрутов при традиционной маршрутизации.

MPLS предусматривает два способа пересылки пакетов. При одном способе каждый маршрутизатор выбирает следующий участок маршрута самостоятельно, а при другом заранее задается цепочка маршрутизаторов, через которые должен пройти пакет. Второй способ основан на том, что маршрутизаторы на пути следования пакета действуют в соответствии с инструкциями, полученными от одного из LSR данного LSP (обычно – от нижнего, что позволяет совместить процедуру “раздачи” этих инструкций с процедурой распределения меток).

Поскольку принадлежность пакетов тому или иному FEC определяется не только IP-адресом, но и другими параметрами, нетрудно организовать разные LSP для потоков пакетов, предъявляющих разные требования к QoS. Каждый FEC обрабатывается отдельно от остальных — не только в том смысле, что для него образуется свой LSP, но и в смысле доступа к общим ресурсам (полосе пропускания канала, буферному пространству). Поэтому технология MPLS позволяет очень эффективно поддерживать требуемое QoS, соблюдая предоставленные пользователю гарантии.

Однако для поддержки гарантированного качества обслуживания усилий одного MPLS недостаточно. Необходим симбиоз с механизмами управления трафиком и/или механизмами резервирования ресурсов, например, протоколом RSVP, о котором речь пойдет дальше.

Решение для сети доступа: RSVP-подход

Идем дальше. С транспортом мы разобрались, переходим к доступу. Естественно, на уровне доступа также должна обеспечиваться «мультисервисность». Существует несколько вариантов организации доступа, подходящих для наших условий. Скорее всего, будет применяться интегрированный доступ. Дело в том, что в нашей сети не используются мультисервисные терминалы будущего, способные обрабатывать информацию любого вида. В конвергентной сети будут только те терминалы, которые есть сегодня – персональные компьютеры, телефонные аппараты, IP-телефоны.

Значит в узле доступа должны быть реализованы технологии для любого терминального устройства: оптоволокно, например технология PON; радиодоступ – DECT, Bluetooth, Radio Ethernet и HIPERLAN2 – и, конечно же, доступ по медной паре, в частности, по технологии ISDN или xDSL.

Безусловно, ни одна из перечисленных технологий не может в полной мере удовлетворить потребности мультисервисного доступа. Необходим некий абонентский концентратор, объединяющий

все эти технологии. Такие концентраторы тоже уже существуют. Здесь и AN 2000 (UTStarcom), и Any Media Access System (Lucent), и Протей-МАК (НТЦ Протей), и Ace Map Access Gateway (Samsung).

Проблема доступа и передачи данных разного вида решена, но как быть с обеспечением качества обслуживания? В сети MPLS эта проблема решается, но прежде чем передаваемая информация поступит в сеть MPLS, она будет находиться в общей IP- сети, не поддерживающей гарантированное QoS. Наиболее подходящим решением здесь можно считать протокол резервирования ресурсов RSVP.

RSVP – это протокол сигнализации, который обеспечивает резервирование ресурсов для предоставления в IP-сетях услуг эмуляции выделенных каналов. Протокол позволяет запрашивать, например, гарантированную пропускную способность такого канала, предсказуемую задержку, максимальный уровень потерь. Но резервирование выполняется лишь в том случае, если имеются требуемые ресурсы.

Чтобы обеспечить должное качество обслуживания трафика речевых и видеоприложений, необходим механизм, позволяющий приложениям информировать сеть о своих требованиях. На основе этой информации сеть может резервировать ресурсы, чтобы гарантировать выполнение требований к качеству, или отказать приложению, вынуждая его либо пересмотреть требования, либо отложить сеанс связи.

Для полноты картины опишем процесс резервирования ресурсов на основе RSVP. Отправитель данных передает на индивидуальный или групповой адрес получателя сообщение Path, в котором указываются желательные характеристики качества обслуживания трафика – верхняя и нижняя граница полосы пропускания, средняя длительность задержки и допустимая вариация длительности задержки.

Сообщение Path пересылается маршрутизаторами сети в сторону получателя данных с использованием таблиц маршрутизации в узлах сети, в нашем случае – до ближайшего маршрутизатора MPLS. Каждый маршрутизатор, поддерживающий протокол RSVP, получив сообщение Path, фиксирует элемент “структуры пути” – адрес предыдущего маршрутизатора. Таким образом, в сети образуется фиксированный маршрут. Поскольку сообщения Path содержат те же адреса отправителя и получателя, что и данные, пакеты будут маршрутизироваться корректно даже через сетевые области, не поддерживающие протокол RSVP.

Сообщение Path должно нести в себе шаблон данных отправителя (Sender Template), описывающий тип этих данных. Шаблон специфицирует фильтр, который может отделять пакеты этого отправителя от других пакетов в пределах сессии. Кроме того, сообщение Path должно содержать спецификацию потока данных отправителя Tspec, которая определяет характеристики этого потока. Спецификация Tspec используется, чтобы предотвратить избыточное резервирование.

Шаблон данных отправителя имеет тот же формат, что и спецификация фильтра в сообщениях Resv. В зависимости от идентификатора протокола, заданного для сессии, шаблон может специфицировать только IP-адрес отправителя или (но не обязательно) также и UDP/TCP-порт.

Приняв сообщение Path, его получатель передает к маршрутизатору, от которого пришло это сообщение (т.е. по направлению к отправителю), запрос резервирования ресурсов – сообщение Resv. В дополнение к информации Tspec, сообщение Resv содержит спецификацию запроса (Rspec), в которой указываются нужные получателю параметры качества обслуживания, и спецификацию фильтра (filterspec), которая определяет, к каким пакетам сессии относится данная процедура. Вместе Rspec и filterspec представляют собой дескриптор потока, используемый маршрутизатором для идентификации каждой процедуры резервирования ресурсов.

Когда получатель данных передает запрос резервирования, он может запросить передачу ему ответного сообщения, подтверждающего резервирование.

При получении сообщения Resv каждый маршрутизатор резервируемого пути, поддерживающий протокол RSVP, определяет приемлем ли этот запрос, для чего выполняются две процедуры. С помощью механизмов управления доступом проверяется, имеются ли у маршрутизатора ресурсы, необходимые для поддержки запрашиваемого качества обслуживания, а с помощью процедуры режимного контроля (policy control) – правомерен ли запрос резервирования ресурсов. Если запрос не может быть удовлетворен, маршрутизатор отвечает на него сообщением об ошибке.

Если же запрос приемлем, данные о требуемом качестве обслуживания поступают для обработки в соответствующие функциональные блоки (способ обработки параметров QoS маршрутизатором в протоколе RSVP не определен), и маршрутизатор передает сообщение Resv следующему (находящемуся ближе к отправителю данных) маршрутизатору. Это сообщение несет в себе спецификацию flowspec, содержащую два набора параметров:

“Rspec”, который определяет желательное QoS;

“Tspec”, который описывает информационный поток.

Когда маршрутизатор, ближайший к инициатору процедуры резервирования, получает сообщение Resv и выясняет, что запрос приемлем, он передает подтверждающее сообщение получателю данных.

После окончания вышеописанной процедуры ее инициатор начинает передавать данные, и на их пути к получателю будет обеспечено заданное QoS.

Совместное использование двух протоколов – RSVP на уровне доступа и MPLS на уровне транспортной сети – позволяет предоставлять пользователям нашей конвергентной сети гарантированное качество обслуживания.

Теперь нужно оговорить способ подключения к конвергентной сети абонентов обычной ТфОП. На самом деле, на начальном этапе ТфОП просто станет частью конвергентной сети, а на стыках между ТфОП и сетью IP/MPLS будут устанавливаться VoIP шлюзы – устройства, которые предназначены для преобразования речевой информации, поступающей со стороны ТфОП, в вид, пригодный для передачи по IP-сетям, и наоборот.

Кроме того, в конвергентную сеть войдут сети IP-телефонии альтернативных операторов, построенные, например, на протоколах H.323 и SIP. Сегодня такие сети используются, в основном, для междугородной и международной связи, но в условиях конвергентной сети они станут альтернативой ТфОП. Кстати, с учетом возможности введения повременной оплаты (государственные органы почему-то сильно противятся этому естественному явлению), альтернатива ГТС станет весьма актуальной.

Еще раз о Softswitch

Получается, что мы создали сеть, удовлетворяющую всем нашим требованиям, и может обеспечивать передачу трафика любого вида с гарантированным QoS. Но это еще не все. Мы действительно сумели создать сеть, объединяющую существующие отдельно сети ТфОП, сети передачи данных (IP-сети) и сети IP-телефонии. Но как в этой сети будут устанавливаться соединения? Какое устройство сможет управлять трафиком в такой сети? Естественно, в ТфОП есть свои устройства управления, в сети IP-телефонии свои, но ни одно из них не может управлять обеими сетями.

Для решения этой проблемы и было создано специальное устройство управления – коммутатор Softswitch. Работая в нашей конвергентной сети и поддерживая все протоколы управления шлюзами и терминалами пакетной сети, коммутатор Softswitch поддерживает и сигнализацию ТфОП. Он управляет устройствами сети IP-телефонии, работающей по протоколам H.323 и/или SIP, взаимодействует с телефонными станциями по протоколам DSS1 или ОКС-7, а соединение между ними организует с помощью протоколов управления шлюзами MGCP/MEGACO.

Только не следует путать – Softswitch управляет обслуживанием вызовов и не отвечает за соединение через маршрутизаторы. Естественно в сети может существовать несколько коммутаторов Softswitch, а в качестве протокола взаимодействия между ними может выступать SIP. Впрочем, об этом устройстве уже писалось, и мы не будем повторяться, но говоря о Softswitch сегодня, приятно отметить появление российских разработок, таких как Tario.Net Softswitch и Протей-Softswitch.

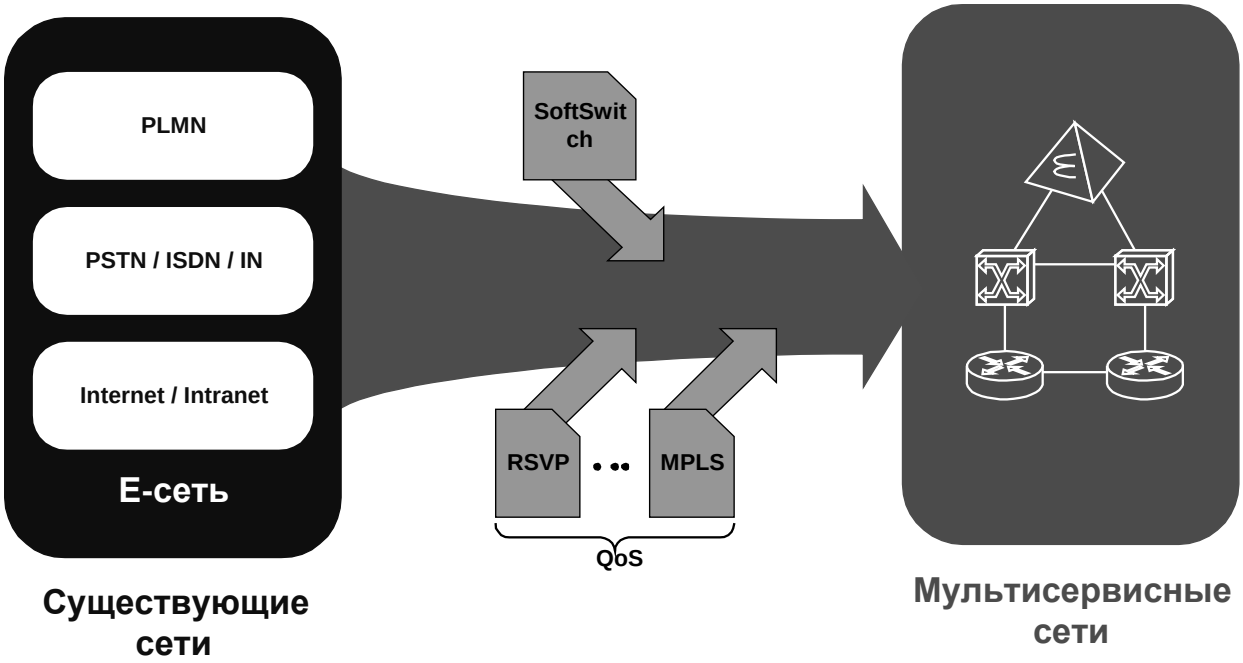

Рисунок 3. Путь развития телекоммуникационной сети.

Итак, путь намечен (рис. 3), осталось разобраться в том, как все это будет работать. Рассмотрим пример установления соединения (рис. 4). Предположим, нужно связать двух пользователей, один из которых является абонентом ТфОП, а второй – пользователем сети IP-телефонии. Пусть инициатором соединения будет VoIP-пользователь (абонент А), а сеть IP-телефонии использует протокол H.323.

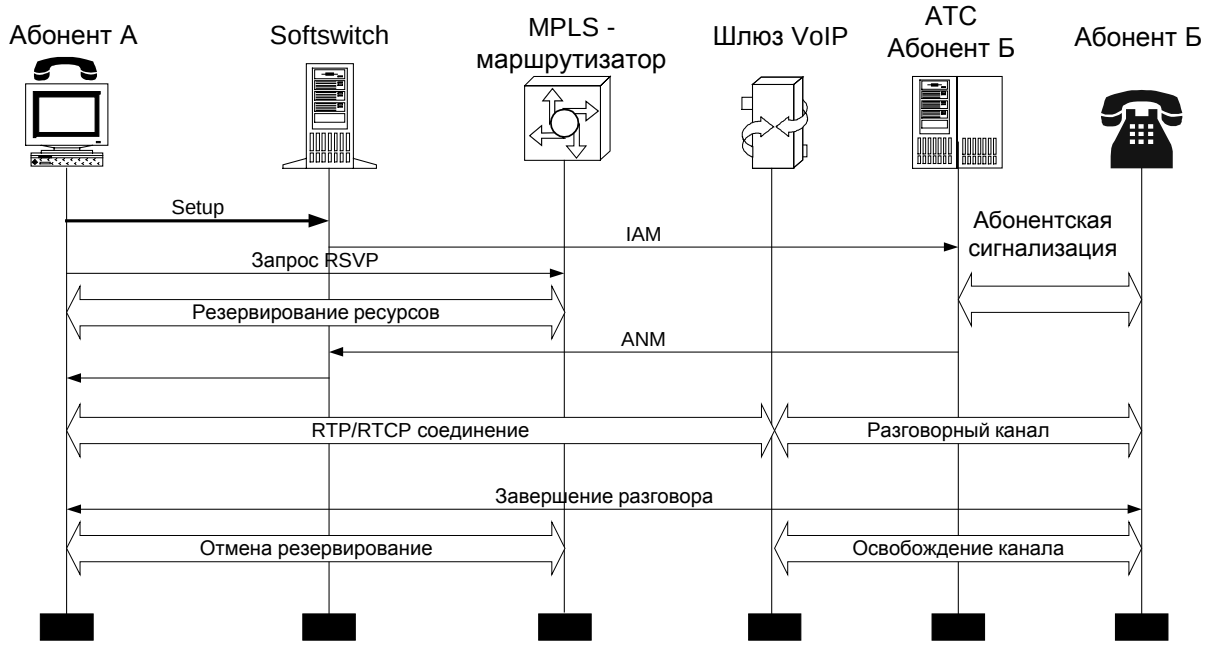

Рисунок 4. Пример установления соединения.

Посредством сигнализации H.323 абонент А сообщит коммутатору Softswitch о своем желании получить соединение с абонентом ТфОП (абонентом Б). Softswitch должен определить местонахождение вызываемого абонента и, так как это абонент ТфОП, найти ближайший к нему шлюз VoIP. Одновременно с передачей к Softswitch номера вызываемого абонента Б, терминал абонента А с помощью протокола RSVP занимает ресурс связи с маршрутизатором MPLS, необходимый ему для гарантированной передачи речевого трафика реального времени с соответствующим стандартам качеством.

Дело в том, что терминал абонента А далеко не всегда имеет прямой доступ к сети MPLS. Подключение к ней может идти по каналам обычной (public) сети Интернет, которая гарантированного качества обслуживания не обеспечивает. Именно здесь мы и будем использовать протокол RSVP.

Далее, в случае использования сигнализации ОКС-7, коммутатор Softswitch формирует сигнальное сообщение IAM в сторону вызываемой станции (которая, кстати, может находиться в зоне действия другого Softswitch, и тогда сначала сообщениями будут обмениваться коммутаторы Softswitch, а уж потом эти сообщения будут транслироваться на АТС).

Происходит обмен стандартными сообщениями ОКС-7 между Softswitch и вызываемой станцией. Получив от вызываемой станции сообщение ANM об ответе вызываемого абонента, Softswitch транслирует это сообщение в сторону вызывающего абонента А.

Между найденным Softswitch шлюзом VoIP и ближайшим к нему маршрутизатором MPLS устанавливается RSVP-соединение. Таким образом, образуется цепочка VoIP терминал – маршрутизаторы IP/MPLS – шлюз VoIP – АТС – терминал ТфОП, и на всем ее протяжении действуют механизмы обеспечения гарантированного качества обслуживания. Затем начинается передача речевого трафика между абонентами с использованием протоколов RTP/RTCP. После завершения соединения, цепочка разрушается. Для этого абоненты (абонент А через Softswitch и абонент Б через АТС) информируют друг друга об окончании разговора, после чего резервирование RSVP отменяется.

На самом деле все будет выглядеть гораздо сложнее. И при резервировании ресурсов, и при обмене сигнальными сообщениями, и при установлении речевого соединения должны выполняться разнообразные действия, передаваться команды, запросы, ответы, но здесь и не ставилась задача детально расписать сценарий установления соединения. Просмотрев описания протоколов и механизмов (о каждом немало написано в самых разных источниках – рекомендациях, книгах, статьях), читатель легко сможет сделать это сам.

Вместо заключения

Изложенное выше оставляет открытым самый главный вопрос, на который нужно ответить: насколько предложенный симбиоз технологий MPLS и RSVP позволяет решить проблемы характерного для IP-сетей тяжелого наследия "best effort", которое свалится на абонентов телефонной сети, развращенных нормой потерь по вызовам порядка одного процента и привыкших к задержкам в получении сигнала "Ответ станции", сравнимым со временем, которое тратится на то, чтобы поднести телефонную трубку к уху?

Окончательный ответ на этот вопрос требует аналитического исследования и определенных количественных оценок. И кое-что в этом направлении уже сделано. Существуют формулы и механизмы для определения задержек в сети с RSVP, подобные результаты получены и для технологии MPLS. Но, по имеющимся данным, аналогичных количественных оценок для MPLS и RSVP вместе не существует (однако многие, включая и автора данной статьи, над этим усердно работают).

Что же касается гипотетической конвергентной К-сети, то на самом деле она вовсе не гипотетическая, а как раз самая реальная. Гипотетической же сегодня, наоборот, является мультисервисная М-сеть, существующая, в основном, на картинках проспектов Lucent, Siemens, Alcatel. Рассмотренная в статье К-сеть полностью удовлетворяет заданным нами условиям.

Возможно, когда-нибудь проект такой сети с комбинированным использованием RSVP-подхода для доступа и MPLS-подхода для транспорта будет реализован. Или будет придумано что-то более удачное. В любом случае нельзя останавливаться на месте. Ни у кого не вызывает сомнения, что мультисервисные сети будут строиться и в самом ближайшем будущем, и что технологии MPLS и RSVP помогут решить главную для этих сетей проблему – обеспечить гарантированное качество обслуживания.