

того затраты на приобретение КСМ могут быть скомпенсированы или даже перекрыты за счет подключения новых абонентов.

Перспектива — цифровая АТС

Однако и это еще не все возможности развития. Существует возможность перехода к полностью цифровой АТС.

На этом этапе демонтируются МКС, а также заменяются абонентские комплекты, вместо которых теперь будут использоваться РСЛ с формирователями цифровых потоков (для каждого абонента), и цифровой коммутатор заменяется более мощным. Контроллер АТС доработок не требует — в нем заменяется лишь ПО. Однако стоимость этого этапа достаточно высока. Чудес не бывает — в результате мы опять пришли к стоимости цифровой АТС. Это вполне естественно, поскольку нами реализована струк-

тура цифровой АТС, а элементная база и там, и здесь примерно одинакова. Однако затраты на переоборудование АТС производятся поэтапно, т. е. не требуются больших разовых капиталовложений.

Возможно, есть резон задуматься о целесообразности перехода к полностью цифровой АТС, поскольку реальный выигрыш при этом незначителен, а стоимость его довольно высока.

Доступ к Интернету

Отдельной проблемой является необходимость обеспечения высокоскоростного доступа к сети Интернет. Технические решения для такого доступа (мосты Ethernet-E1) существуют у разных фирм. Однако здесь возникает новая проблема — нехватка канальных интервалов для передачи потока Ethernet, особенно в потоках E1/2. Существует немало трактов, где свободны всего 2 — 3

интервала (или они отсутствуют вообще), поэтому о высокой скорости Интернета даже для нескольких пользователей говорить не приходится. Увеличение числа канальных интервалов требует замены оконечного оборудования ИКМ/15 на ИКМ/30, что приводит к дополнительным вложениям. В этом случае покупка недорогой каналообразующей аппаратуры КСМ-ИКМ, специально разработанной для КСМ, позволит заметно снизить расходы.

Таким образом, можно с уверенностью сказать, что пути эффективного и экономичного решения проблемы устаревших АТСК 50/200, которые выводят их на современный уровень, есть. При этом в соответствии с законом “О связи” обеспечиваются повременный учет соединений, предоставление универсальной услуги и закрытая 10-значная нумерация — и это без серьезных затрат на цифровую АТС.

Телекоммуникационные сети последующих поколений в свете документов МСЭ-Т, или еще раз о NGN

И.И. ВЛАСОВ, технический директор ООО “ВИЛКОМ ХОЛДИНГ”, М.М. ПТИЧНИКОВ, руководитель курсов “Технологическая связь” УИЦ Госакадемии нефти и газа им. И.М. Губкина

Характеризуя современное состояние телекоммуникационных сетей, в первую очередь, можно определить его, как время их коренной реконструкции. Сейчас вряд ли кто-нибудь отважится точно определить, как сети будут выглядеть в будущем, сколько поколений технологий передачи и соответствующей аппаратуры предстоит еще освоить. Но многие приметы будущего, кажется, видны уже сегодня: открытая конкуренция операторов в связи с развитием свободных рынков услуг, взрывной рост цифрового трафика, например, из-за увеличения использования сети Интернет, повышение спроса на новые мультимедийные

услуги, рост потребности в общей мобильности связи, конвергенция сетей и услуг связи и т. д. Для практической реализации всего перечисленного необходимо иметь мощные сети передачи и коммутации пакетов, высокоскоростные линии доступа и многое другое.

Появился и соответствующий термин, определяющий следующее поколение телекоммуникационных сетей, — Next Generation Networks (NGN). В отечественной литературе принято обозначение “сеть последующих поколений” (СПП). СПП считают новым конкретным шагом в реализации концепции глобальной информационной инфраструктуры (ГИИ).

Цель СПП состоит в предоставлении всех элементов, требуемых для возможной функциональной совместимости и способности сетей, чтобы обеспечивать глобальную поддержку приложений в телекоммуникационной сети при сохранении подхода с разделением транспортных, услуг и применений.

Рекомендации МСЭ-Т Y.2001 — Y.2004 содержат целый ряд определений и характеристик функций СПП и ее архитектуры.

Основополагающими характеристиками СПП являются:

передача с пакетной коммутацией;

разделение функций управления между пропускной способностью ка-

нала-носителя, вызовом-сеансом, а также приложением-услугами;

развязка между предоставлением услуг и транспортировкой информации и предоставление открытых интерфейсов;

поддержка широкого спектра услуг, приложений и механизмов на основе унифицированных блоков обслуживания (включая услуги в реальном масштабе времени, в потоковом режиме, в автономном режиме и мультимедийные услуги);

возможности широкополосной передачи со сквозной функцией качества обслуживания (QoS);

взаимодействие с существующими сетями с помощью открытых интерфейсов;

универсальная мобильность, т. е. возможность для пользователя или других подвижных объектов осуществлять связь и иметь доступ к услугам вне зависимости от изменений местоположения или технических условий. Степень доступности обслуживания может зависеть от ряда факторов, включая возможности сети доступа, соглашения об уровне обслуживания между домашней сетью пользователя и транспортной сетью (если это применимо) и т. д. Мобильность допускает возможность обеспечения электросвязи как в сочетании с непрерывным предоставлением услуг, так и без такой возможности;

неограниченный доступ пользователей к разным поставщикам услуг;

разнообразие схем идентификации;

единые характеристики обслуживания;

сближение услуг фиксированной и подвижной связи;

независимость функций обслуживания от используемых технологий транспортировки;

поддержка различных технологий "последней мили";

выполнение всех регламентных требований, в том числе для аварийной связи, защиты информации, СОРМ и т. д.

СПП должна предоставлять возможности (инфраструктуру, протоколы и т. д.) для создания, развертывания и управления всеми

возможными видами услуг (известными или пока еще нет). Сюда входят услуги, использующие передачу аудио, видео, аудиовизуальной информации со всеми типами ее кодирования; услуги передачи данных: диалоговые, с адресацией конкретному устройству, групповой адресацией и вещанием; услуги передачи сообщений в реальном масштабе времени и с регулированием задержки.

При построении СПП особое внимание уделяется вопросам обеспечения требований заказчика поставщиками услуг, причем некоторые из поставщиков будут предлагать своим клиентам возможность реализации своих собственных услуг. СПП должна иметь интерфейсы программирования приложений (API), чтобы поддерживать создание, предоставление и управление услугами.

Одной из основных характеристик СПП является развязка транспортировки и услуг, т. е. возможность предлагать их отдельно и развивать независимо. Поэтому в архитектуре СПП существует четкое разделение функций обслуживания и функций транспортировки. СПП позволяет предоставлять как существующие, так и новые услуги вне зависимости от используемой сети и типа доступа.

В СПП функциональные объекты, обеспечивающие структуру, сеансы связи, среду передачи, ресурсы, доставку услуг, защиту и т. д., могут быть рас-

пределены по инфраструктуре существующих и новых сетей. При их пространственном разделении они должны поддерживать связь через открытые интерфейсы. Поэтому важным моментом для СПП является идентификация опорных точек. Для обеспечения связи между взаимодействующими функциональными объектами необходимо стандартизировать протоколы.

Взаимодействие между СПП разных операторов и между СПП и существующими сетями, такими как коммутируемая телефонная сеть общего пользования, цифровая сеть с интеграцией служб и глобальная система подвижной связи, обеспечивается с помощью шлюзов.

СПП поддерживает как существующие, так и перспективные оконечные устройства, включая аналоговые телефонные и факсимильные аппараты, аппаратуру приема — передачи данных, кабельные модемы, мобильные телефоны, оконечные устройства систем ра-

IDW СЕРИЯ



Однопарные соединители абонентской проводки



www.belconn.com
Эксклюзивный дистрибьютор в РФ и СНГ
ЗАО "СТР"
 тел./факс: (812) 329-22-03, 329-22-04
 www.str-telecom.ru

диодоступа общего пользования, ПК и т. д.

Предусматривается передача каналов ТЧ в инфраструктуру СПП в реальном масштабе времени, обеспечение качества обслуживания (гарантированная ширина полосы, задержка, целостность пакетов и т. д.), а также защита информации. Сеть СПП должна обеспечивать в своей инфраструктуре унифицированные механизмы защиты информации от внешних атак и от неразрешенного пользования услугами.

Функциональная архитектура разделяет СПП на ряд объектов, каждый из которых предоставляет свои функции и связан стандартными интерфейсами.

При построении СПП ее функциональная архитектура должна обеспечивать:

- возможность использования обобщенных методов эталонного моделирования для определения дополнительных стандартов, необходимых для поддержки совместимых с СПП услуг связи в пределах домена оператора или между доменами операторов;

- определение межсетевых функций взаимодействия для поддержки устаревших (“не знакомых с СПП”) оконечных устройств;

- поддержку сквозных услуг, управление вызовами и мобильность пользователя в неоднородных сетях;

- функциональное определение “знакомых с СПП” оконечных устройств на основе видов программного обеспечения, способов резервирования, согласования версий и управления.

Необходимо также определить, как различным сетевым оконечаниям прийти к согласию по вопросу сквозного качества обслуживания (QoS) для того или иного вызова, а также как использовать параметры протокола верхнего уровня для управления нижним уровнем и QoS для уровней транспортировки и доступа.

Механизмы QoS в СПП лучше всего разделить на два типа: “вертикальный” механизм связывания функций QoS верхнего и нижнего

уровней (например, дифференцированные услуги и т. д.) и “горизонтальный” механизм нижнего уровня, который должен связывать управление QoS нижнего уровня между различными доменами и сетями. При этом необходимо определить:

- класс QoS для телефонии по сетям с пакетной коммутацией;

- принципы определения класса сквозного QoS для мультимедийных систем и метод идентификации классов QoS отдельных мультимедийных составляющих;

- технические требования к способу использования механизма QoS нижнего уровня для обеспечения QoS верхнего уровня сети;

- управление QoS нижнего уровня между доменами;

- восприятие QoS конечным пользователем.

Один из наиболее важных ключевых аспектов для СПП заключается в разделении управления обслуживанием и предоставления услуг в базовой сети и в расширении управления обслуживанием для телефонии и мультимедийных систем.

Требуемые платформы обслуживания должны обеспечивать открытые интерфейсы с применением API и/или прокси-серверов для использования внешних поставщиков услуг. Создаваемые при этом услуги должны быть доступны конечным пользователям при их перемещении из сети в сеть, и, естественно, сквозные услуги должны быть доступны для пользователей, подключенных к разным сетям с различными поставщиками услуг.

Для организации платформы обслуживания СПП должна обеспечивать:

- определение принципов и структуры управления обслуживанием, включая как интерфейсы открытого доступа к услугам, так и стыки прокси-серверов;

- расширение механизмов поддержки процесса предоставления услуг в нескольких сетях, включая как услуги роуминга, так и взаимосвязанность услуг;

- разработку механизмов определения присутствия пользова-

телей и управления настройкой и профилем услуг в соответствии с требованиями пользователей;

- влияние мобильности пользователя на платформы обслуживания.

В отношении вопросов управления сетью необходимо обеспечить:

- расширение архитектуры общего управления базовой сетью и основных услуг по управлению сетью и интерфейсами в соответствии с требованиями СПП (отказы, конфигурация, учет/оплата, эксплуатационные характеристики, защита, управление клиентами, управление трафиком и маршрутизацией);

- введение и применение новых концепций архитектуры и новых технологий, например, языка маркировки электросвязи (tML).

Вопросы защиты информации в СПП взаимосвязаны, с одной стороны, с архитектурой, QoS, управлением сетью, мобильностью, а с другой — с организацией выставления счетов и их оплаты.

Одна из наиболее существенных проблем, с которыми сталкиваются при проектировании стандартов защиты для СПП, заключается в том, что сети больше нельзя считать едиными системами с хорошо известными интерфейсами. Большая часть работы по стандартизации защиты СПП должна основываться на руководствах и принципах, согласующихся с интерфейсами API, чтобы можно было построить защищенную сеть из заданного комплекта конкретных компонентов СПП.

Архитектура защиты для СПП должна обеспечивать исчерпывающую нисходящую и сквозную защиту сети и может применяться для элементов сети, услуг и приложений, чтобы обнаруживать, предупреждать и устранять уязвимые моменты в защите. Для этого необходимо произвести разработку исчерпывающей архитектуры защиты для сетей СПП, подготовку руководств по эксплуатационной защите СПП, развитие стратегии эксплуатационной защиты СПП, соответствующие протоколы и интерфейсы API для защиты СПП.

Общие требования пользователя к мобильности (о ней уже говорилось выше) должны включать возможности:

- изменения точки доступа и/или типа оконечного устройства;

- получения доступа к сети из любой ее точки;

- постоянного получения услуг с учетом ограничений, возникающих в конкретных ситуациях;

- подключения пользователя к сетевым функциям, а также к услугам и приложениям, включая те, которые предоставляются третьей стороной.

Для обеспечения мобильности необходимо обеспечить как поддержку персональной мобильности, так и поддержку мобильности оконечного устройства или обе указанные функции одновременно.

Главным вопросом при этом является обеспечение возможности развития более прозрачной стационарной и мобильной беспроводной широкополосной связи путем применения различных технологий доступа. Для этого необходимо обеспечить согласованный подход к использованию разных систем доступа, систем подвижной связи и стационарных систем, снизить затраты на развертывание и эксплуатацию сети, повысить эффективность использования спектра.

Для обеспечения универсальной мобильности требуется провести дополнительные разработки функций сети на уровне управления в отношении:

- механизмов идентификации и аутентификации;

- функций управления и разрешения доступа;

- определения местоположения объекта сети;

- распределения и управления адресами оконечных устройств и сеансов связи;

- поддержки управления средой пользователя;

- управления профилем пользователя;

- доступа к данным пользователя.

С учетом все возрастающего распределенного характера функций управления в архитектурах СПП возникает необходимость изучения

эталонных моделей управления сетью, включающего такие вопросы, как: ресурсы и QoS при доступе в сеть и в базовую сеть, среда передачи, преобразование кодов, передача информации, управление вызовами и сеансами связи, управление обслуживанием.

Модель архитектуры управления сетью должна учитывать различные требования к функциям управления и определять типовые команды, действующие в опорных точках.

Можно привести следующие примеры группировки функций:

- функции шлюза доступа к среде передачи, сетевого устройства защиты, преобразования адресов сетевых портов (NAPT), усиления стратегии передачи;

- управление ресурсами, включая контроль и обработку запросов на доступ;

- управление сеансами доступа, включая распределение адресов, местоположение пользователя, управление профилем доступа пользователя;

- управление обслуживанием, включая регистрацию пользователя, управление профилем обслуживания пользователя, обработку запросов на услуги, управление взаимодействием услуг.

Модели архитектуры управления сетью должны учитывать функциональные требования к доступу в сеть (интерфейс пользователь — сеть), к интерфейсам между сетями (интерфейс сеть — сеть) и к интерфейсам между сетями и поставщиками услуг/приложений (например, интерфейсы сеть — поставщики).

При учете существующих тенденций и будущего развития требований клиента к услугам, включая связь в реальном и не в реальном времени, проводную и беспроводную, между людьми и между машинами, необходимо в структуре СПП обеспечить функциональную совместимость всевозможных типов систем и сетей. При этом следует учитывать возможности услуг электросвязи, которые должна предоставлять СПП, а также разделение приложений, услуг и сетей. Необходимо также

разработать пригодную архитектуру обслуживания, обеспечивающую бесперебойную связь во всех средах передачи, основанную на интерфейсах, которые должны поддерживать различные модели сети.

Поскольку СПП складывается из соединенных друг с другом различных сетей, используя разнообразный доступ и разные устройства пользователя, и должна обеспечивать бесперебойные возможности вне зависимости от способа доступа и сети, необходимо обратиться к адресации, именованию и нумерации. Отдельных пользователей можно идентифицировать с помощью имени/номеров, используя систему разрешения имени/номера, которая должна иметь возможность перевести данное имя/номер в пригодный для маршрутизации и допустимый адрес, чтобы обеспечить средство транспортировки сообщений. Пользователь, которому требуется получить доступ к другому пользователю, может непосредственно ввести один из выбранных идентификаторов, а затем оконечное устройство или сеть может провести ввод пользователя в адрес точки назначения, используя внутреннюю или внешнюю базу данных сети (например, доступ с помощью механизма перевода системы имен доменов DNS). СПП должна обеспечивать также переносимость имени или номера.

В качестве рабочей сети общего пользования СПП должна удовлетворять высоким требованиям к разрешению имен: система разрешения имени/номера непосредственно связана с работой СПП, поэтому она должна иметь надежность класса несущей. Архитектура должна обеспечивать для нее две возможности:

- во-первых, она не должна быть единственным уязвимым звеном;

- во-вторых, она должна обладать отличным механизмом выравнивания загрузки. Необходимо создать хорошую конфигурацию и организацию во время планирования сети, чтобы обеспечить требования к пропускной способности.

Поскольку система разрешения имени/номера непосредственно связана с работой сетей общего пользования, необходимо, чтобы системы разрешения имени/номера этих сетей не входили в конфликт между собой. Поэтому общие базы данных для перевода имени/номера должны иметь надежные входы, не оказывающие влияния на целостность всей системы, особенно при использовании распределенных систем. Система разрешения имени/номера должна быть специализированной и используемой только данной сетью, необходимо принять определенные меры для ее защиты. Защита, главным образом, осуществляется с помощью определения права доступа пользователей, защиты данных, конфиденциальности данных, синхронизации данных сети и восстановления сети после сбоев в ее работе.

Есть еще один очень важный аспект этой проблемы. Сети последующих поколений должны обеспечивать связь в чрезвычайных ситуациях с целью предоставления преимущественного доступа для представителей соответствующих организаций и приоритетной обработки аварийного трафика. Для этого могут потребоваться определенные специальные меры.

Как же практически реализуются перечисленные выше требования к СПП?

Повторяя определение, данное в рекомендации МСЭ-ТУ.2001, можно сказать следующее: СПП — это гетерогенная мультисервисная сеть, основанная на пакетной коммутации и обеспечивающая предоставление неограниченного спектра телекоммуникационных услуг. Такая сеть должна поддерживать передачу разнородного трафика с различными требованиями к качеству обслуживания и обеспечивать соответствующие запросы оператора и абонентов. На первый взгляд, мы бесконечно далеко ушли в этом определении от традиционных сетей, настолько далеко, что здесь не осталось места привычной нам телефонии. Однако, это не так. Ключевое слово здесь — услуга или сервис. Это всеобъемлющее понятие вклю-

чает в себя различные виды трафика, в том числе и телефонию, точнее — канал ТЧ в составе услуги Triple Play, т. е. телефон, данные и видеoinформация, передаваемые по одной абонентской линии.

Наиболее распространенная модель СПП состоит из четырех уровней: доступа, транспортного, управления, услуг.

Транспортный уровень — это основа СПП. От используемых на нем технологий во многом зависит качество работы всей сети следующего поколения и количество предоставляемых сервисов.

Наиболее дешевое решение — это сети IP, построенные на базе коммутаторов и маршрутизаторов Ethernet. Именно по этой причине оно достаточно часто встречается в небольших сетях. Такие сети просты в проектировании и эксплуатации, легко наращиваются и модернизируются, однако имеют ряд недостатков, ограничивающих их применение в СПП в качестве транспортной среды. Основной из них — недостаточная адаптированность к пропуску разнородного трафика, особенно потоков, используемых наиболее востребованными приложениями (VoIP, VideoIP). При использовании сетей IP очень сложно обеспечить требуемое качество работы таких приложений. Единственный выход — это увеличение пропускной способности магистралей, но и это не всегда приводит к положительному результату.

Сети ATM более адаптированы к применению в СПП, прежде всего, благодаря наличию встроенных механизмов обеспечения заданного качества сервиса, возможности адаптации к разнородному трафику данных, гибкого перераспределения полосы пропускания между различными сервисами. Эта достаточно дорогая технология применяется, прежде всего, в больших сетях, что обусловлено ее надежностью и гибкостью. В качестве транспортной среды передачи технология ATM часто использует SDH. Такое сочетание позволяет добиться необходимой надежности и управляемости сети.

В свою очередь, развитие технологии Ethernet привело к появлению нового транспорта — PoS (Pocket over SDH/SONET) или New-GenSDH. По сути, это симбиоз двух хорошо знакомых технологий — Ethernet и SDH/SONET. Такая технология имеет все преимущества системы передачи SDH, характеризующейся высочайшей надежностью и управляемостью, и сети IP, позволяющей предоставлять все необходимые услуги передачи пакетного трафика.

Наращивание скоростей передачи до 1 или 10 Гбит/с подразумевает использование оптических технологий и создание так называемого Optical Ethernet. О разработке такого относительно недорогого оборудования уже заявили многие компании-производители. Однако, даже с учетом огромной полосы пропускания этих каналов такая IP-сеть методологически несет в себе все недостатки младших Ethernet.

Дальнейшее совершенствование IP-сетей привело к созданию MPLS. Технология MPLS изначально задумывалась как средство снижения нагрузки на маршрутизаторы и адаптации IP-сетей к разнородному трафику данных. Она давала пути сопряжения сетей IP и ATM и закономерно стала одной из основных технологий транспортного уровня СПП. Это произошло, прежде всего, благодаря реализованным на ее основе приложениям управления трафиком, организации виртуальных частных сетей, быстрого восстановления соединений, обеспечения качества обслуживания. Сегодня большинство производителей оборудования СПП так или иначе декларируют поддержку технологии MPLS.

Второй уровень — уровень доступа. Доступ в общем случае — это все то оборудование, которое связывает сеть СПП с традиционными цифровыми сетями PDH и SDH и даже с небольшими локальными сетями передачи данных: от цифровых абонентских линий до пограничных шлюзов и конверторов сигнализации. Естественно, нельзя забывать и об абонентах сети.

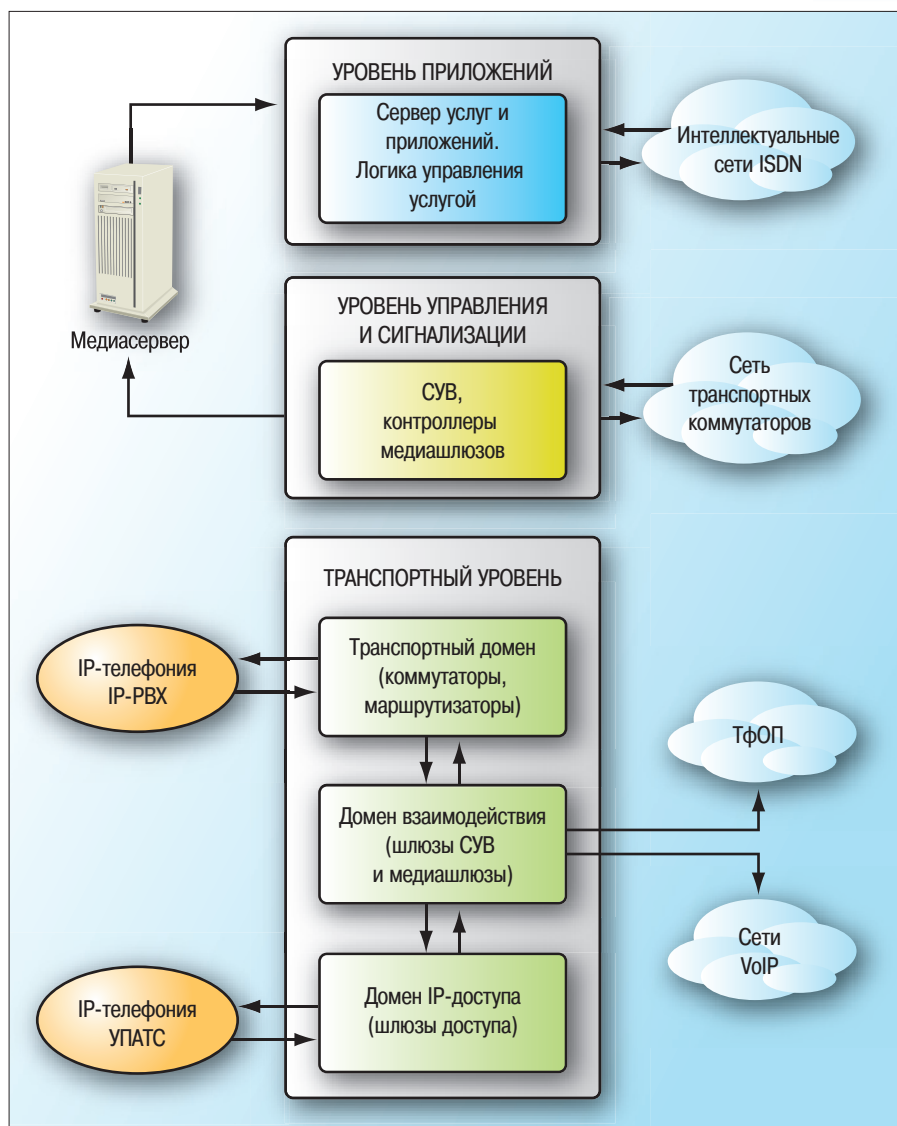
Можно различить несколько способов их включения в сеть следующего поколения. Наиболее интересный из них — это непосредственное подключение пользователей к пакетной сети посредством IP-терминалов или IP-телефонов. Такое подключение наиболее “удобно” с точки зрения построения СПП, предоставления мультимедийного трафика, управления ресурсами сети.

Однако в силу многих технологических трудностей, связанных с невозможностью непосредственно довести до абонента сеть Ethernet или MPLS, операторы часто не могут оказать такой услуги. IP-телефонами чаще всего пользуются корпоративные абоненты, постоянно работающие в локальной сети, интегрированной в СПП. Остальные пользователи подключаются к предлагаемому услугам через широкополосную сеть доступа.

Техника такого подключения может быть разной: DSL-системы, использующие медные кабельные пары, системы цифрового КТВ, активно развивающиеся сейчас системы радиодоступа, оптические технологии доступа, например PON. Объединяет их одно — они предоставляют абоненту в качестве интерфейса IP-подключение, т. е. дают возможность использовать интеллектуальный терминал с доступом к большому количеству услуг.

Гораздо сложнее ситуация с подключением абонентов существующих сетей PDH и SDH. Единственный возможный вариант для них — это включение в СПП через шлюзы стандартной телефонии. Естественно, при этом абоненты “старой” сети не могут получить всего перечня услуг, доступного IP-абонентам, но все же некоторые услуги сети нового поколения становятся им доступны.

Все многообразие устройств, транслирующих и коммутирующих трафик, преобразующих информацию, заложенную в пакеты, в стандартную телефонную сигнализацию и каналы ТЧ, сопрягающих цифровые сети различной природы, терминирующих на себе различные виды трафика, управ-



Обобщенная структура СПП

ляется одним мощным узлом. Это и есть третий уровень СПП — управляющий. Основная функция третьего уровня — это управление соединением абонента А с абонентом Б. Занимается этим специализированный сервер соединений.

Большая мощность и производительность подобных серверов — это необходимое условие бесперебойной работы сети. Кроме того, необходимо учитывать такие специфические факторы IP-сетей, как необходимость обеспечения параметров QoS VoIP-сети, разделение маршрутов потоков голоса и данных, управление маршрутизацией при наличии довольно пестрого спектра сетевых устройств — маршрутизаторов, конверторов сигнализации, пограничных контроллеров, шлюзов, прокси-сер-

веров, абонентских терминалов, мультиплексоров и контроллеров широкополосного абонентского доступа различной природы. Добавьте сюда необходимость обеспечения параметров надежности, соответствующих системам операторского класса.

Последним уровнем СПП принято считать уровень приложений. Его задача — это обеспечение всего спектра услуг, доступного на сетях следующего поколения. В большинстве случаев для реализации уровня приложений выделяются отдельные серверы и базы данных.

На рисунке приведена обобщенная структура СПП, представляющая составные части сети нового поколения и базирующаяся на пакетной передаче.