ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОНЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Телекоммуникация инжиниринги»

ТЕХНОЛОГИИ СЕТЕЙ СВЯЗИ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

Методическое пособие

для студентов, обучающихся по направлениям образования 5311300 – Телекоммуникации

Ташкент 2014

Авторы Эшмурадов А.М., Садчикова С.А., Норматова Д.Т. Технологии сетей связи следующего поколения. Методическое пособие. /ТУИТ. 207с. Ташкент, 2014

Сети общего пользования нового поколения (NGN) основаны на принципах коммутации пакетов и протоколах, разработанных для передачи данных, и обещают как более низкие цены, так и большую функциональность. Ядром концепции NGN большинства компаний-производителей оборудования служит центральный сервер обработки речевых вызовов и сигнализации, управляющий шлюзами на границах сети передачи данных, основными характеристиками которого являются – поддержка протоколов сигнализации (ISUP, INAP, H.323/SIP, MGCP/H/248), обслуживание вызовов интеллектуальных сетей, наличие API для взаимодействия с ПО третьей стороны (например, для приложений электронной коммерции), реализация Gatekeeper и RADIUS, позволяющая выполнять функции привратника и производить идентификацию удаленных пользователей.

Данное методическое пособие рассчитано для использования в учебном процессе при подготовке специалистов в области телекоммуникаций.

Ташкентский Университет Информационных Технологий, 2014

СОДЕРЖАНИЕ

Введение

Существующие телефонные сети общего пользования (ТфОП) проектировались для обслуживания речевого трафика, т.е. для предоставления традиционных услуг телефонной связи ТфОП. Телеграфные сообщения передавались через отдельную, ранее существовавшую сеть, а системы передачи данных и изображений появились гораздо позже.

Сегодня появились сети общего пользования нового поколения, которые основаны на принципах коммутации пакетов и протоколах, разработанных для передачи данных, и обещают как более низкие цены, так и большую функциональность. Структура обусловлена тем, что именно IP является движущей силой конвергенции сетей связи, информационных технологий и мультимедийных продуктов. На сетевом уровне IP создает единую управляемую приложениями интерактивную сеть, способную обеспечить высокоскоростную пакетную связь абонентскими устройствами проще и дешевле, чем традиционные сети.

Операторам ТфОП в самое ближайшее время понадобятся мультисервисные платформы, сочетающие высокую производительность с экономичностью и гибкостью

Ядром концепции NGN большинства компаний-производителей обрудования служит центральный сервер обработки речевых вызовов и сигнализации, управляющий шлюзами на границах сети передачи данных. Основные характеристики этой платформы — поддержка большинства протоколов сигнализации (ISUP, INAP, H.323/SIP, MGCP/H/248), обслуживание вызовов интеллектуальных сетей, наличие API для взаимодействия с программными продуктами третьей стороны (например, для приложений электронной коммерции), реализация Gatekeeper и RADIUS, позволяющая выполнять функции привратника и производить идентификацию удаленных пользователей и другие.

На территории Республики Узбекистан совместно работают электронные станции и мультисервисное пакетное оборудование различных фирм-производителей коммутационного оборудования. Оборудование разных фирм-производителей имеет общие принципы построения и аппаратной части и ПО.

Данное методическое пособие рассчитано для использования в учебном процессе при подготовке специалистов в области телекоммуникаций.

Методическое пособие рассмотрено и одобрено на заседании кафедры ТИ. Рекомендовано к тиражированию НМС в типографии ТУИТ.

1. КОНВЕРГЕНЦИЯ СЕТЕЙ СВЯЗИ. ОСОБЕННОСТИ СОВРЕМЕННЫХ УСЛУГ СВЯЗИ

1.1. Конвергенция сетей связи

Со времени своего возникновения телекоммуникации базируются на передаче электромагнитных сигналов через транспортную среду, каковой могут быть:

• металлический кабель,
• оптоволокно,
• радиоканал.

Передаваемая в виде электромагнитных сигналов информация может представлять собой:

• речь,
• данные,
• видеоизображение

или любую их комбинацию, называемую мультимедийной информацией.

Эти три источника и три составные части телекоммуникаций в полной мере отражают их современное состояние, причем современность здесь понимается в широком смысле. Передача по сетям связи информации трех перечисленных выше видов благополучно осуществлялась не одно десятилетие.

Однако некоторые события привели к коренному изменению подходов к построению информационных сетей:

- 1996 г. в США трафик передачи данных впервые превысил речевой и продолжает расти (до 30% в год по сравнению с 3% в год для телефонии). То же произошло в Европе в 1999 году.
- Протокол IP получил мировое признание и стал стандартом для передачи мультимедийной информации.
- В сети Интернет рост числа пользователей составляет 5% в месяц.

Речь и данные меняются местами. Традиционные сети передачи данных базировались на магистралях с коммутацией каналов, предназначенных для телефонного трафика. При новом подходе - все наоборот: телефония будет надстраиваться над инфраструктурой сети передачи данных.

Смещение центра тяжести в область передачи данных поставило вопрос о поиске удобного способа встраивания речи в мультимедийный цифровой поток. Причина популярности IP заключается в его восприимчивости к требованиям со стороны не только услуг передачи данных, но и приложений реального времени. Примером может служить технология передачи речевой информации по сетям с маршрутизацией пакетов IP - Voice over IP (VolP) или IP-телефония.

Стандартизация речевых технологий на основе стека TCP/IP и их поддержка лидерами рынка пакетной телефонии обеспечат совместимость оборудования разных производителей и позволят создавать системы, в которых возможны вызовы с аналогового телефонного аппарата, подключенного к порту маршрутизатора, на персональный компьютер, или с персонального компьютера на номер ТфОП.

Internet Protocol будет доминирующим протоколом в сетях следующего поколения, которым предстоит поддерживать передачу речи, данных, факсимиле, видеоинформации и мультимедиа.

Необходимо учесть, что в течение длительного времени ТфОП и IP-сети будут вынуждены существовать параллельно, обеспечивая взаимную прозрачность и объединяя свои усилия в обслуживании разнородного абонентского трафика.

Поэтому необходимо соблюдение основных законов существующей ТфОП - эксплуатационная надежность с тремя девятками после запятой, жесткие нормы качества передачи речи в реальном времени. Важно сохранить все привычные для пользователя действия - набор номера, способ доступа к телефонным услугам и т. д. Абонент не должен ощущать разницы между IP-телефонией и обычной телефонной связью ни по качеству речи, ни по алгоритму доступа. Желательно обеспечить между ТфОП и IP-сетями полную прозрачность передачи пользовательской информации и сигнализации. В отличие от большинства корпоративных сетей связи, сети общего пользования не имеют национальных и ведомственных границ.

Достижения электронной техники за последнее десятилетие привели к настоящему буму в области телекоммуникаций. Связь, находящаяся в статическом состоянии еще с середины 1980-х годов, сегодня превратилась в бурно развивающуюся отрасль, приносящую операторам значительные прибыли.

Пользователи получили доступ к услугам, о которых 10–15 лет назад и не задумывались. E-mail, Интернет, сотовый телефон стали обычными атрибутами повседневной жизни. За короткое время мы так привыкли к практически ежедневному появлению всевозможных новинок, что сами начали выдвигать требования по предоставлению новых услуг и

приложений.

Пользователю уже недостаточно просто поговорить по домашнему телефону. Мы хотим иметь возможность позвонить своим друзьям или коллегам, находясь на улице, в поезде, на корабле, в любой точке земного шара.

Нам уже недостаточно иметь несколько разных номеров, принадлежащих разным сетям (телефонная сеть общего пользования, мобильная сеть, Интернет и т.д.). Мы хотим иметь один персональный номер, который позволял бы однозначно определять нас и направлять входящий звонок к терминалу, подключенному к сети, в которой мы находимся в данный момент.

Но какими бы ни были желания пользователей, а также достижения в науке и технике, ни один оператор связи не будет устанавливать новое оборудование или вводить новые сервисы, если это экономически нецелесообразно. Поэтому потребность операторов сетей связи получать все новые прибыли заставляет их задуматься над созданием сети, которая позволяла бы:

- как можно быстрее и дешевле создавать новые услуги, с тем чтобы постоянно привлекать новых абонентов;
- уменьшать затраты на обслуживание;
- быть независимыми от поставщиков оборудования;
- быть конкурентоспособными (дерегуляция в телекоммуникационной отрасли и достижения в новейших технологиях привели к появлению новых операторов связи и сервис-провайдеров, предлагающих более дешевый и широкий спектр услуг).

1.1.1. Особенности современных услуг связи

Технологической основой информационного общества является Глобальная информационная инфраструктура (ГИИ), которая должна обеспечить возможность недискриминационного доступа к информационным ресурсам каждого жителя планеты. Информационную инфра-структуру составляет совокупность баз данных, средств обработки информации, взаимодействующих сетей связи и терминалов пользователя. Доступ к информационным ресурсам в ГИИ реализуется посредством услуг связи нового типа, получивших название услуг Информационного общества или инфокоммуникационных услуг.

Наблюдаемые в настоящее время высокие темпы роста объемов предоставления инфокоммуникационных услуг позволяют прогнозировать их преобладание в сетях связи в ближайшем будущем.

На сегодняшний день развитие инфокоммуникационных услуг осуществляется, в основном, в рамках компьютерной сети Интернет, доступ к услугам которой происходит через традиционные сети связи.

В то же время в ряде случаев услуги Интернет, ввиду ограниченных

возможностей ее транспортной инфраструктуры не отвечают современным требованиям, предъявляемым к услугам информационного общества.

В связи с этим развитие инфокоммуникационных услуг требует решения задач эффективного управления информационными ресурсами с одновременным расширением функциональности сетей связи. В свою очередь это стимулирует процесс интеграции Интернета и сетей связи.

1.1.2. Особенности инфокоммуникационных услуг

К основным технологическим особенностям, отличающим инфокоммуникационные услуги от услуг традиционных сетей связи, можно отнести следующие:

- инфокоммуникационные услуги оказываются на верхних уровнях модели ВОС (в то время как услуги связи предоставляются на третьем, сетевом уровне);
- большинство инфокоммуникационных услуг предполагает наличие клиентской и серверной частей; клиентская часть реализуется в оборудовании пользователя, а серверная – на специальном выделенном узле сети, называемом узлом служб;
- инфокоммуникационные услуги, как правило, предполагают передачу информации мультимедиа, которая характеризуется высокими скоростями передачи и несимметричностью входящего и исходящего информационных потоков;
- для предоставления инфокоммуникационных услуг зачастую необходимы сложные многоточечные конфигурации соединений;
- для инфокоммуникационных услуг характерно разнообразие прикладных протоколов и возможностей по управлению услугами со стороны пользователя;
- для идентификации абонентов инфокоммуникационных услуг может использоваться дополнительная адресация в рамках данной инфокоммуникационной услуги.

Большинство инфокоммуникационных услуг являются "приложениями", т.е. их функциональность распределена между оборудованием поставщика услуги и оконечным оборудованием пользователя. Как следствие, функции оконечного оборудования также должны быть отнесены к составу инфокоммуникационной услуги, что необходимо учитывать при их регламентации.

Бизнес-модель, определяющая участников процесса предоставления инфокоммуникационных услуг и их взаимоотношения, также отличается от модели традиционных услуг электросвязи, в которой было представлено всего лишь три основных участника: оператор, абонент и пользователь.

Новая деловая модель предполагает наличие поставщика услуг, который предоставляет инфокоммуникационные услуги абонентам и

пользователям. При этом сам поставщик является потребителем услуг переноса, предоставляемых оператором сети связи.

На рынке могут также присутствовать дополнительные виды поставщиков услуг: поставщики информации, брокеры, ритейлеры и т.д. Поставщик информации предоставляет информацию поставщику услуг для распространения. Брокер предоставляет информацию о поставщиках услуг и их потенциальных абонентах, содействует пользователям в поиске поставщиков, оказывающих требуемые услуги. Ритейлер выступает как посредник между абонентом и поставщиком с целью адаптации услуги к индивидуальным требованиям абонента.

К инфокоммуникационным услугам предъявляются такие требования, как:

- мобильность услуг;
- возможность гибкого и быстрого создания новых услуг;
- гарантированное качество услуг.

Большое влияние на требования к инфокоммуникационным услугам оказывает процесс конвергенции, приводящий к тому, что инфокоммуникационные услуги становятся доступными пользователям вне зависимости от способов доступа.

1.1.3. Требования к сетям связи

Принимая во внимание рассмотренные особенности инфокоммуникационных услуг, могут быть определены следующие требования к *перспективным сетям связи*:

- мультисервисность, под которой понимается независимость технологий предоставления услуг от транспортных технологий;
- широкополосность, под которой понимается возможность гибкого и динамического изменения скорости передачи информации в широком диапазоне в зависимости от текущих потребностей пользователя;
- мультимедийность, под которой понимается способность сети передавать многокомпонентную информацию (речь, данные, видео, аудио) с необходимой синхронизацией этих компонент в реальном времени и использованием сложных конфигураций соединений;
- интеллектуальность, под которой понимается возможность управления услугой, вызовом и соединением со стороны пользователя или поставщика услуг;
- инвариантность доступа, под которой понимается возможность организации доступа к услугам независимо от используемой технологии;
- многооператорность, под которой понимается возможность участия нескольких операторов в процессе предоставления услуги и разделение их ответственности в соответствии с областью деятельности.

Кроме того, при формировании требований к перспективным сетям связи необходимо учитывать особенности деятельности поставщиков услуг. В

частности, современные подходы к регламентации услуг присоединения предусматривают доступ поставщиков услуг, в том числе и не обладающих собственной инфраструктурой, к ресурсам сети общего пользования на недискриминационной основе. При этом к основным требованиям, предъявляемым поставщиками услуг к сетевому окружению, относятся:

- обеспечение возможности работы оборудования в "мультиоператорской " среде, т.е. увеличение числа интерфейсов для подключения к сетям сразу нескольких операторов связи, в том числе на уровне доступа;
- обеспечение взаимодействия узлов поставщиков услуг для их совместного предоставления;
- возможность применения "масштабируемых " технических решений при минимальной стартовой стоимости оборудования.

Существующие сети связи общего пользования с коммутацией каналов (ТфОП) и коммутацией пакетов (СПД) в настоящее время не отвечают перечисленным выше требованиям. Ограниченные возможности традиционных сетей являются сдерживающим фактором на пути внедрения новых инфокоммуникационных услуг.

С другой стороны, наращивание объемов предоставляемых инфокоммуникационных услуг может негативно сказаться на показателях качества обслуживания вызовов базовых услуг существующих сетей связи.

Все это вынуждает учитывать наличие инфокоммуникационных услуг при планировании способов развития традиционных сетей связи в направлении создания сетей связи следующего поколения.

1.2. Понятие сети ССП и ее базовые принципы

В основу концепции построения *сети связи следующего поколения* положена идея о создании универсальной сети, которая бы позволяла переносить любые виды информации, такие как речь, видео, аудио, графику и т. д., а также обеспечивать возможность предоставления неограниченного спектра инфокоммуникативных услуг.

Сеть связи следующего поколения (***ССП***, ***NGN*** – Next Generation Network) – концепция построения сетей связи, обеспечивающих предоставление неограниченного набора услуг с гибкими возможностями по их управлению, персонализации и созданию новых услуг за счет унификации сетевых решений, предполагающая реализацию универсальной транспортной сети с распределенной коммутацией, вынесение функций предоставления услуг в оконечные сетевые узлы и интеграцию с традиционными сетями связи.

Базовым принципом концепции NGN является отделение друг от друга функций переноса и коммутации, функций управления вызовом и функций управления услугами.

ССП, которая потенциально должна объединить существующие сети

связи (телефонные сети общего пользования – ТфОП, сети передачи данных – СПД, сети подвижной связи – СПС), обладает *следующими характеристиками*:

- сеть на базе коммутации пакетов, которая имеет разделенные функции управления и переноса информации, где функции услуг и приложений отделены от функций сети;
- сеть компонентного построения с использованием открытых интерфейсов;
- сеть, поддерживающая широкий спектр услуг, включая услуги в реальном времени и услуги доставки информации (электронная почта), в том числе мультимедийные услуги;
- сеть, обеспечивающая взаимодействие с традиционными сетями электросвязи;
- сеть, обладающая общей мобильностью, т.е. позволяющая отдельному абоненту пользоваться и управлять услугами независимо от технологии доступа и типа используемого терминала и предоставляющая абоненту возможность свободного выбора поставщика услуг.

Сети электросвязи, построенные на основе концепции *ССП*, обладают следующими *преимуществами* перед традиционными сетями электросвязи.

- *Для оператора:*
  - построение одной универсальной сети для оказания различных услуг;
  - повышение среднего дохода с абонента за счет оказания дополнительных мультимедийных услуг;
  - оператор *ССП* может наиболее оптимально реализовывать полосу пропускания для интеграции различных видов трафика и оказания различных услуг;
  - *ССП* лучше приспособлена к модернизации и расширению;
  - *ССП* обладает легкостью в управлении и эксплуатации;
  - оператор *ССП* располагает возможностью быстрого внедрения новых услуг и приложений с различным требованием к объему передаваемой информации и качеству ее передачи.
- *Для пользователя:*
  - абстрагирование от технологий реализации услуг электросвязи (принцип черного ящика);
  - гибкое получение необходимого набора, объема и качества услуг;
  - мобильность получения услуг.

Одной из основных целей построения *ССП*, как уже отмечалось ранее, является расширение спектра предоставляемых услуг.

- услуги службы телефонной связи (предоставление местного телефонного соединения, междугороднего телефонного соединения, международного телефонного соединения);
- услуги служб передачи данных (предоставление выделенного канала

передачи данных, постоянного и коммутируемого доступа в сеть Интернет, виртуальных частных сетей передачи данных);

- услуги телематических служб ("электронная почта ", "голосовая почта ", "доступ к информационным ресурсам ", телефония по IP-протоколу, "аудиоконференция " и "видеоконференция ");
- услуги служб подвижной электросвязи;
- услуги поставщиков информации: видео и аудио по запросу, "интерактивные новости " (для пользователя реализуется возможность просмотра, прослушивания и чтения информации о произошедших за какое-то время событиях), электронный супермаркет (пользователь выбирает товар в "электронном магазине ", получает подробную информацию о его потребительских свойствах, цене и пр.), дистанционное обучение и др.

Таким образом, *ССП* будут поддерживать как уже существующее, так и новое оконечное оборудование, включая аналоговые телефонные аппараты, факсимильные аппараты, оборудование ЦСИС (цифровая сеть с интеграцией служб), сотовые телефоны различных стандартов, терминалы телефонии по IP-протоколу (SIP и H.323), кабельные модемы и т.д.

Услуги *ССП* используют различные способы кодирования и передачи и включают в себя: многоадресную и широковещательную передачу сообщений, передачу чувствительного и нечувствительного к задержкам трафика, услуги обычной передачи данных, услуги реального масштаба времени, диалоговые услуги.

1.3. Классификация услуг для сетей ССП

В настоящее время отсутствует общая классификация услуг для сетей *ССП*. В рамках концепции, когда сеть *ССП* предлагается рассматривать не как отдельную категорию сетей связи, а как инструмент построения и развития существующих сетей, услуги, предоставляемые в рамках фрагмента *ССП*, можно классифицировать следующим образом:

- базовые: услуги, ориентированные на установление соединения с использованием фрагмента *NGN* между двумя оконечными терминалами;
- дополнительные виды обслуживания: услуги, предоставляемые наряду с базовыми и ориентированные на поддержку дополнительных списков возможностей;
- услуги доступа, ориентированные на организацию доступа к ресурсам, и точек присутствия интеллектуальных сетей и сетей передачи данных;
- информационно-справочные услуги: услуги, ориентированные на предоставление информации из баз данных, входящих в структуру *ССП*;
- услуги виртуальных частных сетей: услуги, ориентированные на организацию и поддержание функционирования VPN со стороны

элементов фрагмента *ССП*;
- услуги мультимедиа: услуги, ориентированные на обеспечение и поддержку функционирования мультимедийных приложений со стороны фрагмента *ССП*.

1.3.1. Базовые услуги

Под базовыми видами понимаются:
- услуги местной, междугородной, международной телефонной связи, предоставляемые с использованием (полным или частичным) фрагмента сети на основе *NGN*-технологий. Базовые услуги телефонии в сетях *ССП* могут использовать технологии компрессии речи, при этом качество предоставления базовых услуг должно соответствовать классам "высший " и "высокий ". Базовые услуги телефонии могут быть доступны пользователям, использующим терминалы сетей ТфОП, СПС и H.323, SIP-терминалы;
- услуги по передаче факсимильных сообщений между терминальным оборудованием пользователей. Услуга может предоставляться пользователям, использующим терминалы сетей ТфОП и СПС. Услуга e-fax не относится к данному классу;
- услуги по организации модемных соединений между терминальным оборудованием пользователей. Услуга может предоставляться пользователям, использующим терминалы сетей ТфОП и СПС. Услуга доступа в сети IP не относится к данному классу;
- услуга доставки информации "64 кбит/с без ограничений " и базирующиеся на ней услуги предоставления связи, определенные для технологии ISDN для установления соединений между терминальным оборудованием пользователей. Услуга может предоставляться пользователям, использующим терминалы ISDN.

Задачей сетевого фрагмента *ССП* при предоставлении базовых услуг является установление и поддержание соединения с требуемыми параметрами.

1.3.2. Дополнительные виды обслуживания (ДВО)

Предоставление базовых услуг может сопровождаться дополнительными видами обслуживания, которые расширяют возможности пользователя по получению информации о соединении, тональных уведомлений, а также позволяют изменять конфигурацию соединения. В сетевом фрагменте *ССП* пользователям могут быть доступны следующие дополнительные виды обслуживания:
- идентификации вызывающей линии (CLIP);

- запрет идентификации вызывающей линии (CLIR);
- предоставление идентификации подключенной линии (COLP);
- переадресация вызова при отсутствии ответа (Call Forwarding No Reply);
- переадресация вызова при занятости (Call Forwarding Busy);
- безусловная переадресация вызова (Call Forwarding Unconditional);
- идентификация злонамеренного вызова (MOD);
- индикация ожидающего вызова/сообщения (Call/Message Waiting);
- завершение вызова (Call Completion);
- парковка и перехват вызовов (Call Park/Pick-up);
- удержание вызова (Call Hold);
- замкнутая группа пользователей (CUG);
- конференц-связь с расширением (CONF);
- другие.

Следует отметить, что в зависимости от используемого типа подключения и терминального оборудования, а также от возможностей Softswitch список и алгоритмы предоставления услуг могут отличаться.

В настоящий момент наиболее специфицированными являются дополнительные виды обслуживания для пользователей сетей ISDN. Спецификации ряда ДВО для пользователей сетей на основе H.323 и SIP-протоколов находятся в процессе разработки в международных организациях. Также следует отметить, что фрагмент ССП для проходящих через него вызовов должен обеспечивать поддержку ДВО, инициированных в других сетях.

1.3.3. Услуги доступа

Услугами доступа, поддерживаемыми со стороны сетевого фрагмента *ССП*, являются:

- услуги доступа в сети IP по коммутируемому соединению с поддержкой процедур точки доступа и авторизации со стороны фрагмента *NGN*; применяются как для поддержки WWW, E-mail, FTP-приложений, так и для доступа к сетям IP-телефонии;
- услуги доступа к ресурсам ИСС с реализацией функции SSP в сетевом фрагменте *NGN*. Реализованный SSP на ЕСЭ РФ должен как минимум обеспечивать поддержку следующих видов услуг ИСС:
  - "Бесплатный вызов ";
  - "Телеголосование ";
  - "Вызов с дополнительной оплатой ";
  - "Вызов по предоплаченной карте ".
- услуги доступа к информационно-справочным ресурсам с поддержкой точки доступа и авторизации доступа со стороны фрагмента *ССП* (функция Service Node при доступе к внешним ресурсам).

1.3.4. Информационно-справочные услуги

К информационно-справочным относятся услуги предоставления информации со стороны элементов фрагмента *ССП*. В отличие от услуги доступа к информационно-справочным ресурсам, в данном случае предоставление предполагает включение сервера услуги в состав фрагмента *ССП* и использование API-интерфейсов между Softswitch и сервером приложений.

1.3.5. Услуги VPN

Фрагментом *ССП* может поддерживаться предоставление следующих видов услуг виртуальных частных сетей:

- виртуальная частная сеть (VPN) на основе коммутируемых соединений с поддержкой адресного пространства VPN со стороны Softswitch. В этом случае задачей Softswitch является анализ номера входящего/исходящего абонента с принятием решения о возможности установления соединения в соответствии с политикой VPN. После принятия положительного решения об установлении соединения обрабатывается во фрагменте *ССП* как обычный вызов;
- виртуальная частная сеть на основе постоянных соединений внутри фрагмента *NGN* с обработкой адресной информации со стороны гибкого коммутатора. В этом случае для виртуальной частной сети изначально резервируется транспортный ресурс во фрагменте *NGN*. Обслуживание вызовов VPN осуществляется гибким коммутатором в рамках выделенного для VPN транспортного ресурса;
- виртуальная частная сеть на основе постоянных соединений без обработки сигнальной информации вызова гибким коммутатором. В этом случае VPN использует фрагмент *NGN* только как транспортный ресурс. Обработкой сигнальной информации, относящейся к вызову, занимаются внешние к фрагменту устройства.

1.3.6. Услуги мультимедиа

Мультимедийные услуги можно рассматривать с двух позиций:

- с позиции абонентов услуг связи;
- с позиции поставщика услуг (оператора связи).

С точки зрения абонентов, мультимедийная услуга связи представляет собой возможность сети обеспечить функционирование специфических мультимедийных пользовательских приложений. Фактически абоненту безразлично, на базе какой сети предоставляется мультимедийная услуга, т. е. услуга не зависит от технологической платформы сети.

Мультимедийное пользовательское приложение представляет собой приложение, одновременно поддерживающее несколько "единиц "

представления аудиовизуальной информации и предоставляющее абонентам общее информационное пространство в рамках одного сеанса связи. В качестве примеров мультимедийных приложений можно привести следующие: совместная работа с документами и графикой, "белая доска ", дистанционное обучение, телемедицина и др.

Оператор связи рассматривает мультимедийную услугу связи как перенос комбинации двух или более "единиц " представления аудиовизуальной информации (т. е. видео, звука, текста) между абонентами (группами абонентов) в рамках сетевой инфраструктуры и с учетом состава и возможностей используемого оборудования. Таким образом, возможность предоставления той или иной мультимедийной услуги полностью зависит от технологической платформы сети.

Европейский институт стандартизации в области связи (ETSI) ввел понятие "широкополосных мультимедийных услуг ". Под такими услугами понимаются услуги связи, предоставление которых осуществляется на базе широкополосных сетей связи, способных обеспечить перенос информации (контента) в виде непрерывных потоков пакетов/ячеек в режиме реального времени.

Классификацию мультимедийных услуг связи и приложений можно производить с различных точек зрения и с использованием различных критериев.

В качестве примера классификации, отражающей точку зрения оператора сети B-ISDN, можно привести рекомендацию ITU-T I.211. Суть подхода заключается в том, что услуги связи предоставляются абонентам с помощью определенных служб B-ISDN. Согласно рекомендации, в зависимости от способов связи между терминальным оборудованием абонентов и в соответствии с возможными пользовательскими приложениями все службы делятся на интерактивные и распределительные, каждая из которых, в свою очередь, включает несколько классов служб.

Контрольные вопросы

1. Каковы особенности инфокоммуникационных услуг?
2. Каковы основные требования, предъявляемые поставщиками услуг к сетевому окружению?
3. Каков базовый принцип NGN?
4. Что означает термин мультисервисность?
5. Что подразумевается под понятием широкополосность?
6. Что означает термин мультимедийность?
7. Что подразумевается под понятием интеллектуальность?
8. Что означает термин инвариантность доступа?
9. Что подразумевается под понятием многооператорность?
10. Как вы понимаете «передача голоса по IP-телефонии».
11. В чем отличие сети Интернет от сети ТфОП?

2. IP-ТЕЛЕФОНИЯ

2.1. Сеть Интернет и протокол IP
2.2. Разница понятий IP-телефония, Voice over IP – VoIP, Интернет-телефония
2.3. Принципы пакетной передачи речи
2.4. Виды соединений в сети IP-телефонии
2.5. Принцип пакетной передачи речи на примере сценария IP-телефонии "компьютер-компьютер".
2.6. Пакетная обработка речи - Протоколы RTP и RTCP
2.7. Типы речевых кодеков
2.8. Основные характеристики рассмотренных кодеков

2.1. Сеть Интернет и протокол IP

Универсальная сеть Интернет строится на основе семейства протоколов TCP/IP и включает в себя протоколы 4-х уровней коммуникаций (рис. 2.1).

Прикладной:	Telnet, FTP, E-mail и т.д.
Транспортный:	TCP, UDP
Сетевой:	IP, ICMP, IGMP
Сетевой интерфейс:	Драйвер устройства и сетевая плата

Рис. 2.1. Четыре уровня стека протоколов TCP/IP

Уровень сетевого интерфейса отвечает за установление сетевого соединения в конкретной физической сети - компоненте сети Интернет, к которой подсоединен компьютер. На этом уровне работают драйвер устройства в операционной системе и соответствующая сетевая плата компьютера.

Сетевой уровень - основа стека протоколов TCP/IP. Именно на этом уровне реализуется принцип межсетевого соединения, в частности маршрутизация пакетов по сети Интернет. Протокол IP - основной протокол сетевого уровня, позволяющий реализовывать межсетевые соединения. Он используется обоими протоколами транспортного уровня - TCP и UDP. Протокол IP определяет базовую единицу передачи данных в сети Интернет - IP-дейтаграмму, указывая точный формат всей информации, проходящей, но сети TCP/IP. Программное обеспечение уровня IP выполняет функции маршрутизации, выбирая путь данных по соединениям физических сетей. Для определения маршрута поддерживаются специальные таблицы; выбор осуществляется на основе адреса сети, к которой подключен компьютер-адресат. Протокол IP определяет маршрут отдельно для каждого пакета

данных, не гарантируя надежной доставки в нужном порядке. Он задает непосредственное отображение данных на нижележащий физический уровень передачи и реализует тем самым высокоэффективную доставку пакетов.

На сетевом уровне протокол IP реализует ненадежную службу доставки пакетов по сети от системы к системе без установления соединения (connectionless packet delivery service). Это означает, что будет выполнено все необходимое для доставки пакетов, однако эта доставка не гарантируется. Пакеты могут быть потеряны, переданы в неправильном порядке, продублированы и т.д. Протокол IP не обеспечивает надежности коммуникации. Не имеется механизма подтверждений ни между отправителем и получателем, ни между хост-компьютерами. Не имеется контроля ошибок для поля данных только контрольная сумма для заголовка. Не поддерживается повторная передача, нет управления потоком. Обнаруженные ошибки могут быть оглашены посредством протокола ICMP (Internet Control Message Protocol).

Надёжную передачу данных реализует следующий уровень, транспортный, на котором два основных протокола, TCP и UDP, осуществляют связь между машиной-отправителем пакетов и машиной-адресатом.

Наконец, прикладной уровень - это приложения типа клиент-сервер, базирующиеся на протоколах нижних уровней. В отличие от протоколов остальных трех уровней, протоколы прикладного уровня занимаются деталями конкретного приложения и «не интересуются» способами передачи данных по сети. Среди основных приложений TCP/IP, имеющихся практически в каждой его реализации, - протокол эмуляции терминала Telnet, протокол передачи файлов FTP, протокол электронной почты SMTP, протокол управления сетью SNMP, используемый в системе World Wide Web (WWW) протокол передачи гипертекста HTTP и др.

Поскольку в Интернет детали физических соединений скрыты от приложений, прикладной уровень совершенно «не заботится» о том, что клиент приложения работает в сети Ethernet, а сервер подключен к сети Token Ring. Между конечными системами может быть несколько десятков маршрутизаторов и множество промежуточных физических сетей различных типов, но приложение будет воспринимать этот конгломерат как единую физическую сеть. Это и обуславливает основную силу и привлекательность технологии Интернет и I протокола IP.

На базе протокола IP строится не только сеть Интернет, но и любые другие сети передачи данных (локальные, корпоративные), которые могут иметь или не иметь выход на глобальную сеть Интернет. Универсальность и гибкость сетей на базе протокола IP дает возможность применять их не только для передачи данных, но и другой мультимедийной информации. С недавних пор IP-сети стали использовать для передачи речевых сообщений.

2.2. Разница понятий IP-телефония, Voice over IP – VoIP, Интернет-телефония

В технической литературе используются три основных термина для обозначения технологии передачи речи по сетям с пакетной коммутацией на базе протокола IP (Internet Protocol):

- IP-телефония (IP Telephony);
- голос по IP-сетям (Voice over IP - VoIP);
- Интернет-телефония (Internet Telephony).

Под IP-телефонией будем понимать технологию, позволяющую использовать любую сеть с пакетной коммутацией на базе протокола IP (например - сеть Интернет) в качестве средства организации и ведения международных, междугородных и местных телефонных разговоров и передачи факсов в режиме реального времени.

За рубежом технология передачи голосовой информации с использованием протокола IP имеет устоявшееся название Voice over IP (VoIP). В отношении сервисов и технологий между IP-телефонией и VoIP нет никакой разницы. Различные производители могут предпочитать один или другой термин либо использовать их в равной степени. С точки же зрения сетевых решений «IP-телефония», безусловно, - термин более содержательный, так как она реализуется не только на уровне каналов передачи (как глобальных, так и локальных), но и на уровне абонентского оборудования и, что немаловажно, учрежденческих автоматических телефонных станций (УАТС). Последнее действительно означает фактическую интеграцию телефонии в ее привычном понимании и IP-сетей.

Интернет-телефония - это частный случай IP-телефонии, когда в качестве каналов передачи пакетов телефонного трафика либо от абонента к оператору, либо на магистрали (либо на обоих названных участках) используются обычные каналы сети Интернет.

2.3. Принципы пакетной передачи речи

«Классические» телефонные сети основаны на технологии коммутации каналов (рис.2.2), которая для каждого телефонного разговора требует выделенного физического соединения. Следовательно, один телефонный разговор представляет собой одно физическое соединение телефонных каналов. В этом случае аналоговый сигнал шириной 3,1 кГц передается на ближайшую АТС, где он мультиплексируется по технологии временного разделения с сигналами, которые поступают от других абонентов, подключенных к этой АТС. Далее групповой сигнал передается по сети межстанционных каналов. Достигнув АТС назначения, сигнал де-мультиплексируется и доходит до адресата. Основным недостатком телефонных сетей с коммутацией каналов является неэффективное

использование полосы канала — во время пауз в речи канал не несет никакой полезной нагрузки.

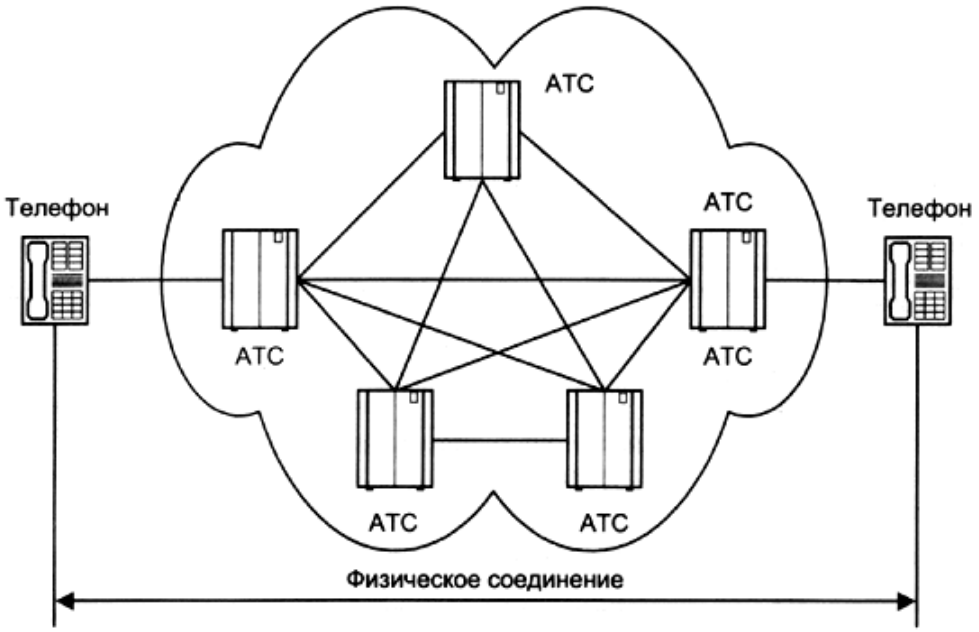


Рис. 2.2. Соединение в «классической» телефонной сети

Переход от аналоговых к цифровым технологиям стал важным шагом для возникновения - современных цифровых телекоммуникационных сетей. Одним из таких шагов в развитии цифровой телефонии стал переход к пакетной коммутации. В сетях пакетной коммутации по каналам связи передаются единицы информации, которые не зависят от физического носителя. Такими единицами могут быть пакеты, кадры или ячейки (в зависимости от протокола), но в любом случае они передаются по разделяемой сети (рис.2.3), более того - по отдельным виртуальным каналам, не зависящим от физической среды. Каждый пакет идентифицируется заголовком, который может содержать информацию об используемом им канале, его происхождении (т.е. об источнике или отправителе) и пункте назначения (о получателе или приемнике).

В сетях на основе протокола IP все данные - голос, текст, видео, компьютерные программы или информация в любой другой форме - передаются в виде пакетов. Любой компьютер и терминал такой сети имеет свой уникальный IP-адрес, и передаваемые пакеты маршрутизируются к получателю в соответствии с этим адресом, указываемом в заголовке. Данные могут передаваться одновременно между многими пользователями и процессами по одной и той же линии. При возникновении проблем IP-сети могут изменять маршрут для обхода неисправных участков. При этом протокол IP не требует выделенного канала для сигнализации. Процесс передачи голоса по IP-сети состоит из нескольких этапов.

На первом этапе осуществляется оцифровка голоса. Затем оцифрованные данные анализируются и обрабатываются с целью

уменьшения физического объема данных, передаваемых получателю. Как правило, на этом этапе происходит подавление ненужных пауз и фонового шума, а также компрессирование.

На следующем этапе полученная последовательность данных разбивается на пакеты и к ней добавляется протокольная информация - адрес получателя, порядковый номер пакета на случай, если они будут доставлены не последовательно, и дополнительные данные для коррекции ошибок. При этом происходит временное накопление необходимого количества данных для образования пакета до его непосредственной отправки в сеть.

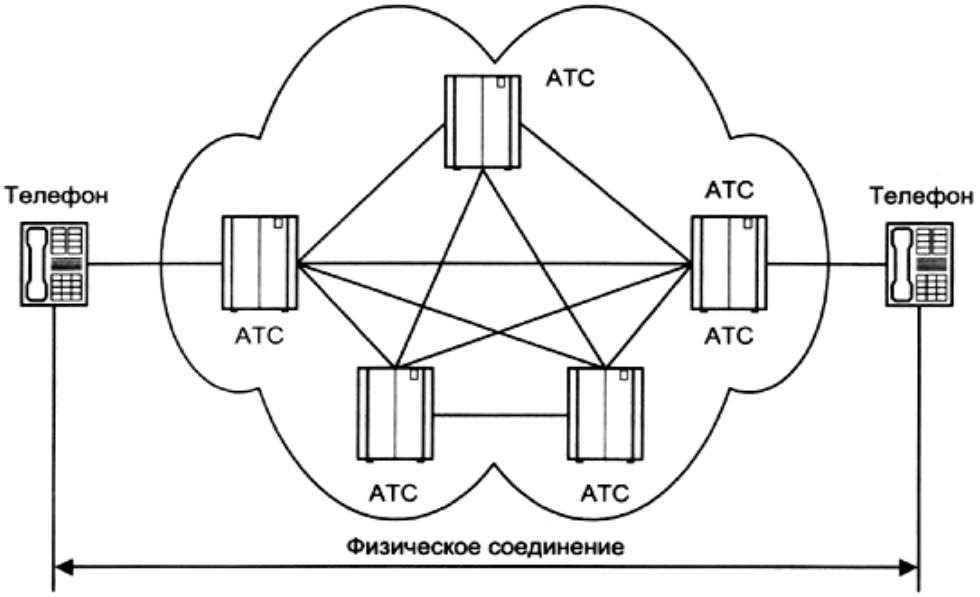


Рис. 2.3. Соединение в сети с коммутацией пакетов

Извлечение переданной голосовой информации из полученных пакетов также происходит в несколько этапов. Когда голосовые пакеты приходят на терминал получателя, то сначала проверяется их порядковая последовательность. Поскольку IP-сети не гарантируют время доставки, то пакеты со старшими порядковыми номерами могут прийти раньше, более того, интервал времени получения также может колебаться. Для восстановления исходной последовательности и синхронизации происходит временное накопление пакетов. Однако некоторые пакеты могут быть вообще потеряны при доставке, либо задержка их доставки превышает допустимый разброс. В обычных условиях приемный терминал запрашивает повторную передачу ошибочных или потерянных данных. Но передача голоса слишком критична ко времени доставки, поэтому в этом случае либо включается алгоритм аппроксимации, позволяющий на основе полученных пакетов приблизительно восстановить потерянные, либо эти потери просто игнорируются, а пропуски заполняются данными случайным образом.

Полученная таким образом (не восстановленная) последовательность данных декомпрессируется и преобразуется непосредственно в аудио-сигнал, несущий голосовую информацию получателю.

Таким образом, с большой степенью вероятности, полученная информация не соответствует исходной (искажена) и задержана (обработка на передающей и приемной сторонах требует промежуточного накопления). Однако в некоторых пределах избыточность голосовой информации позволяет мириться с такими потерями.

Операторы сетей с пакетной коммутацией получают преимущества, присущие разделяемой инфраструктуре электросвязи по самой её природе. Проще говоря, они могут продать больше, чем в действительности имеют, основываясь на статистическом анализе работы сети. Поскольку предполагается, что абоненты не будут круглосуточно и ежедневно задействовать всю оплаченную полосу, можно обслужить больше абонентов, не расширяя магистральную инфраструктуру. Оборот и прибыль при этом увеличиваются.

Иными словами, абонент, оплативший полосу 64 кбит/с, использует канал в среднем лишь на 25%. Следовательно, оператор способен продать имеющийся у него ресурс в четыре раза большему числу пользователей, не перегружая свою сеть. Такой сценарий выгоден обеим сторонам - и клиенту, и продавцу, — поскольку оператор увеличивает свои доходы и уменьшает абонентскую плату за счет снижения издержек. Это выигрышное решение уже признано в мире передачи данных, а теперь начинает использоваться и на рынке телефонии.

В настоящее время в IP-телефонии существует два основных способа передачи голосовых пакетов по IP-сети:

- через глобальную сеть Интернет (Интернет - телефония);
- используя сети передачи данных на базе выделенных каналов (IP-телефония).

В первом случае полоса пропускания напрямую зависит от загруженности сети Интернет пакетами, содержащими данные, голос, графику и т.д., а значит, задержки при прохождении пакетов могут быть самыми разными. При использовании выделенных каналов исключительно для голосовых пакетов можно гарантировать фиксированную (или почти фиксированную) скорость передачи. Ввиду широкого распространения сети Интернет особый интерес вызывает реализация системы Интернет-телефонии, хотя следует признать, что в этом случае качество телефонной связи оператором не гарантируется.

Для того, чтобы осуществить междугородную (международную) связь с помощью телефонных серверов, организация или оператор услуги должны иметь по серверу в тех местах, куда и откуда планируются звонки. Стоимость такой связи на порядок меньше стоимости телефонного звонка по обычным телефонным линиям. Особенно велика эта разница для международных переговоров.

Общий принцип действия телефонных серверов Интернет-телефонии таков: с одной стороны, сервер связан с телефонными линиями и может соединиться с любым телефоном мира. С другой стороны, сервер связан с

Интернетом и может связаться с любым компьютером в мире. Сервер принимает стандартный телефонный сигнал, оцифровывает его (если он исходно не цифровой), значительно сжимает, разбивает на пакеты и отправляет через Интернет по назначению с использованием протокола IP. Для пакетов, приходящих из сети на телефонный сервер и уходящих в телефонную линию, операция происходит в обратном порядке. Обе составляющие операции (вход сигнала в телефонную сеть и его выход из телефонной сети) происходят практически одновременно, что позволяет обеспечить полнодуплексный разговор. На основе этих базовых операций можно построить много различных конфигураций. Например, звонок «телефон-компьютер» или «компьютер-телефон» может обеспечивать один телефонный сервер. Для организации связи телефон (факс) - телефон (факс) нужно два сервера.

Основным сдерживающим фактором на пути масштабного внедрения IP-телефонии является отсутствие в протоколе IP механизмов обеспечения гарантированного качества услуг, что делает его пока не самым надежным транспортом для передачи голосового трафика. Сам протокол IP не гарантирует доставку пакетов, а также время их доставки, что вызывает такие проблемы, как «рваный голос» и просто провалы в разговоре. Сегодня эти проблемы решаются: организации по стандартизации разрабатывают новые протоколы, производители выпускают новое оборудование, но на этом уровне дела с совместимостью и стандартизацией обстоят уже не так хорошо, как с «упаковкой» речи в пакеты. Заметим, что если в рамках частной корпоративной сети некоторая потеря качества голосовой связи при сильной загруженности ресурсов вполне терпима при условии, что средний показатель будет вполне удовлетворительным, то в случае сети общего пользования все намного серьезнее.

С точки зрения масштабируемости (если отвлечься от проблем с неконтролируемым ухудшением качества при росте нагрузки на сеть) IP-телефония представляется вполне законченным решением. Во-первых, поскольку соединение на базе протокола IP может начинаться (и заканчиваться) в любой точке сети от абонента до магистрали. Соответственно, IP-телефонию в сети можно вводить участок за участком, что, кстати, на руку и с точки зрения миграции, так как ее можно проводить «сверху вниз», «снизу вверх» или по любой другой схеме. Для решений IP-телефонии характерна определенная модульность: количество и мощность различных узлов - шлюзов, gatekeeper («привратников» - так в терминологии VoIP именуются серверы обработки номерных планов) - можно наращивать практически независимо, в соответствии с текущими потребностями. Естественно, проблемы наращивания ресурсов собственно сетевой инфраструктуры мы сейчас не учитываем, поскольку узлы самой сети могут быть независимы от системы IP-телефонии, а могут и совмещать в себе их функции.

2.4. Виды соединений в сети IP-телефонии

Сети IP-телефонии предоставляют возможности для вызовов четырех основных типов:

- «От телефона к телефону» (рис.2.4).

Вызов идет с обычного телефонного аппарата к АТС, на один из выходов которой подключен шлюз IP-телефонии, и через IP-сеть доходит до другого шлюза, который осуществляет обратные преобразования.

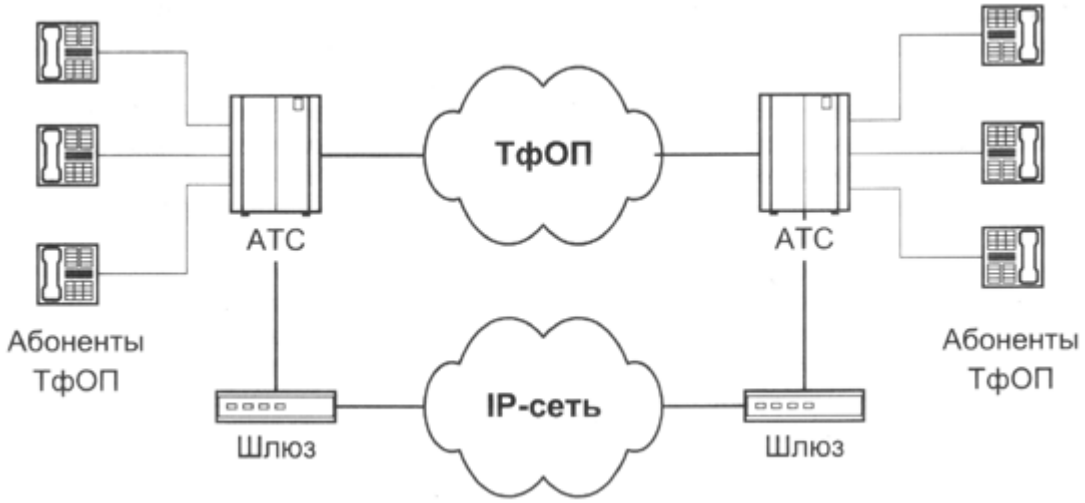


Рис. 2.4. Схема связи «телефон-телефон»

Сценарий «телефон-телефон» в значительной степени отличается от остальных сценариев IP-телефонии своей социальной значимостью, поскольку целью его применения является предоставление обычным абонентам ТфОП альтернативной возможности междугородной и международной телефонной связи. В этом режиме современная технология IP-телефонии предоставляет виртуальную телефонную линию через IP-доступ.

Как правило, обслуживание вызовов по такому сценарию IP-телефонии выглядит следующим образом. Поставщик услуг IP-телефонии подключает свой шлюз к коммутационному узлу или станции ТфОП, а по сети Интернет или по выделенному каналу соединяется с аналогичным шлюзом, находящимся в другом городе или другой стране.

Типичная услуга IP-телефонии по сценарию «телефон-телефон» использует стандартный телефон в качестве интерфейса пользователя, а вместо междугородного компонента ТфОП использует либо частную IP-сеть/lntranet, либо сеть Интернет. Благодаря маршрутизации телефонного трафика по IP-сети стало возможным обходить сети общего пользования и, соответственно, не платить за междугородную/международную связь операторам этих сетей.

Следует отметить, что сама идея использовать альтернативные транспортные механизмы для обхода сети ТфОП не является новой.

Достаточно вспомнить статистические мультиплексоры, передачу речи по сети Frame Relay или оборудование передачи речи по сети АТМ.

Как показано на рис.2.4, поставщики услуг IP-телефонии предоставляют услуги «телефон-телефон» путём установки шлюзов IP-телефонии на входе и выходе IP-сетей. Абоненты подключаются к шлюзу поставщика через ТфОП, набирая специальный номер доступа. Абонент получает доступ к шлюзу, используя персональный идентификационный номер (PIN) или услугу идентификации номера вызывающего абонента (Calling Line Identification). После этого шлюз просит ввести телефонный номер вызываемого абонента, анализирует этот номер и определяет, какой шлюз имеет лучший доступ к нужному телефону. Как только между входным и выходным шлюзами устанавливается контакт, дальнейшее установление соединения к вызываемому абоненту выполняется выходным шлюзом через его местную телефонную сеть.

Полная стоимость такой связи будет складываться для пользователя из расценок ТфОП на связь с входным шлюзом, расценок Интернет-провайдера на транспортировку и расценок удалённой ТфОП на связь выходного шлюза с вызванным абонентом.

Одним из алгоритмов организации связи по сценарию «телефон-телефон» является выпуск поставщиком услуги своих телефонных карт. Имея такую карту, пользователь, желающий позвонить в другой город, набирает номер данного поставщика услуги, затем в режиме донабора вводит свой идентификационный номер и PIN-код, указанный на карте. После процедуры аутентификации он набирает телефонный номер адресата.

Возможны и другие алгоритмы реализации этого сценария: вместо телефонной карты может использоваться информация об альтернативном счете. Счет для оплаты может быть выслан абоненту и после разговора, аналогично тому, как это делается при междугородном соединении в ТфОП.

- «От компьютера к телефону» (рис. 2.5).

Мультимедийный компьютер, имеющий программное обеспечение IP-телефонии, звуковую плату (адаптер), микрофон и акустические системы, подключается к IP-сети или к сети Интернет, и с другой стороны шлюз IP-. телефонии имеет соединение через АТС с обычным телефонным аппаратом.

Следует отметить, что в соединениях I и 2 типов вместо телефонных аппаратов могут быть включены факсимильные аппараты, и в этом случае сеть IP-телефонии должна обеспечивать передачу факсимильных сообщений.

Рассмотрим несколько подробнее пример упрощенной архитектуры системы IP-телефонии по сценарию «телефон-компьютер». При попытке вызвать справочно-информационную службу, используя услуги пакетной телефонии и обычный телефон, на начальной фазе абонент А вызывает

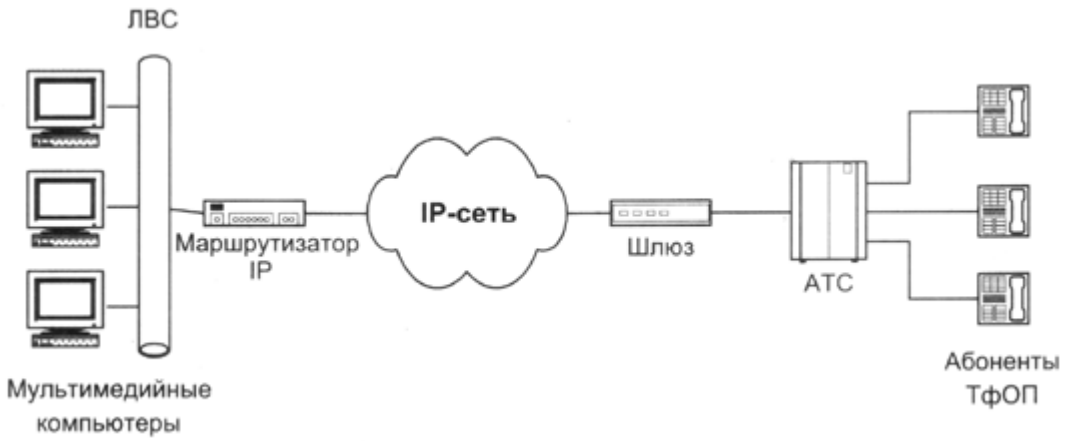


Рис. 2.5. Схема связи «компьютер-телефон»

близлежащий шлюз IP-телефонии. От шлюза к абоненту А поступает запрос ввести номер, к которому должен быть направлен вызов (например, номер службы), и личный идентификационный номер (PIN) для аутентификации и последующего начисления платы, если это служба, вызов которой оплачивается вызывающим абонентом. Основываясь на вызываемом номере, шлюз определяет наиболее доступный путь к данной службе. Кроме того, шлюз активизирует свои функции кодирования и пакетизации речи, устанавливает контакт со службой, ведет мониторинг процесса обслуживания вызова и принимает информацию о состояниях этого процесса (например, занятость, посылка вызова, разъединение и т.п.) от исходящей стороны через протокол управления и сигнализации. Разъединение с любой стороны передается противоположной стороне по протоколу сигнализации и вызывает завершение установленных соединений и освобождение ресурсов шлюза для обслуживания следующего вызова.

Для организации соединений от службы к абонентам используется аналогичная процедура. Популярными программными продуктами для этого варианта сценария IP-телефонии «компьютер-телефон» являются IDT Net2Phone и DotDialer, организующие вызовы к обычным абонентским телефонным аппаратам в любой точке мира.

Эффективность объединения услуг передачи речи и данных является основным стимулом использования IP-телефонии по сценариям «компьютер-компьютер» и «компьютер-телефон», не нанося при этом никакого ущерба интересам операторов традиционных телефонных сетей.

- «От компьютера к компьютеру» (рис. 2.6).

В этом случае соединение устанавливается через IP-сеть между двумя мультимедийными компьютерами, оборудованными аппаратными и программными средствами для работы с IP-телефонией.

Для поддержки сценария «компьютер - компьютер» поставщику услуг Интернет желательно иметь отдельный сервер (привратник), преобразующий

имена пользователей в динамические адреса IP. Сам сценарий ориентирован на пользователя, которому сеть нужна, в основном, для передачи данных, а

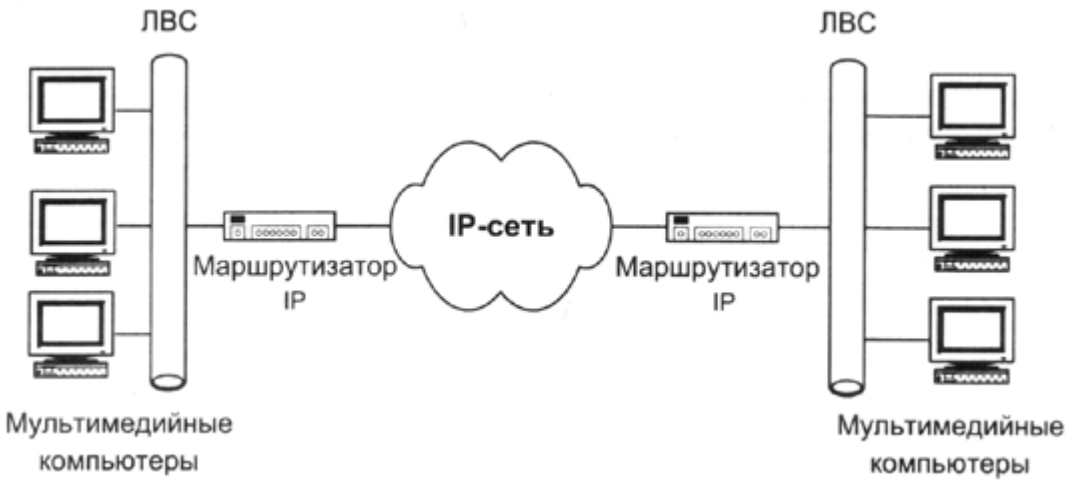


Рис. 2.6. Упрощённая схема связи «компьютер-компьютер»

программное обеспечение IP-телефонии требуется лишь иногда для разговоров с коллегами. Эффективное использование телефонной связи по сценарию «компьютер-компьютер» обычно связано с повышением продуктивности работы крупных компаний, например, при организации виртуальной презентации в корпоративной сети с возможностью не только видеть документы на Web-сервере, но и обсуждать их содержание с помощью IP-телефона. При этом между двумя IP-сетями могут использоваться элементы ТфОП, а идентификация вызываемой стороны может осуществляться как на основе E.164, так и на основе IP-адресации. Наиболее распространенным программным обеспечением для этих целей является пакет Microsoft NetMeeting, доступный для бесплатной загрузки с узла Microsoft.

- «От WEB браузера к телефону» (рис. 2.7).

С развитием сети Интернет стал возможен доступ и к речевым услугам. Например, на WEB-странице некоторой компании в разделе «Контакты» размещается кнопка «Вызов», нажав на которую можно осуществить речевое соединение с представителем данной компании без набора телефонного номера. Стоимость такого звонка для вызывающего пользователя входит в стоимость работы в сети Интернет.

Рис. 2.7. Схема связи «WEB-браузер - телефон»

Рассмотренные выше сценарии сведены в таблице 2.1.

Таблица 2.1

Варианты межсетевого взаимодействия

Сценарий	Входящая сеть	Транзитная сеть	Исходящая сеть	Примечание
«компьютер - компьютер»	IP	IP	IP	Рис.2.6 рис.2.8
	IP	ТфОП	IP	
«компьютер - телефон»	IP	ТфОП	ТфОП	Рис.2.5
	ТфОП	IP	IP	
	ТфОП	ТфОП	IP	
	IP	IP	ТфОП	
«телефон - телефон»	ТфОП	IP	ТфОП	Рис.2.4
	ТфОП	ТфОП	ТфОП	

2.5. Принцип пакетной передачи речи на примере сценария IP-телефонии "компьютер-компьютер".

Рассмотрим представленный на рис.2.8 сценарий установления соединения «компьютер-компьютер» более подробно.

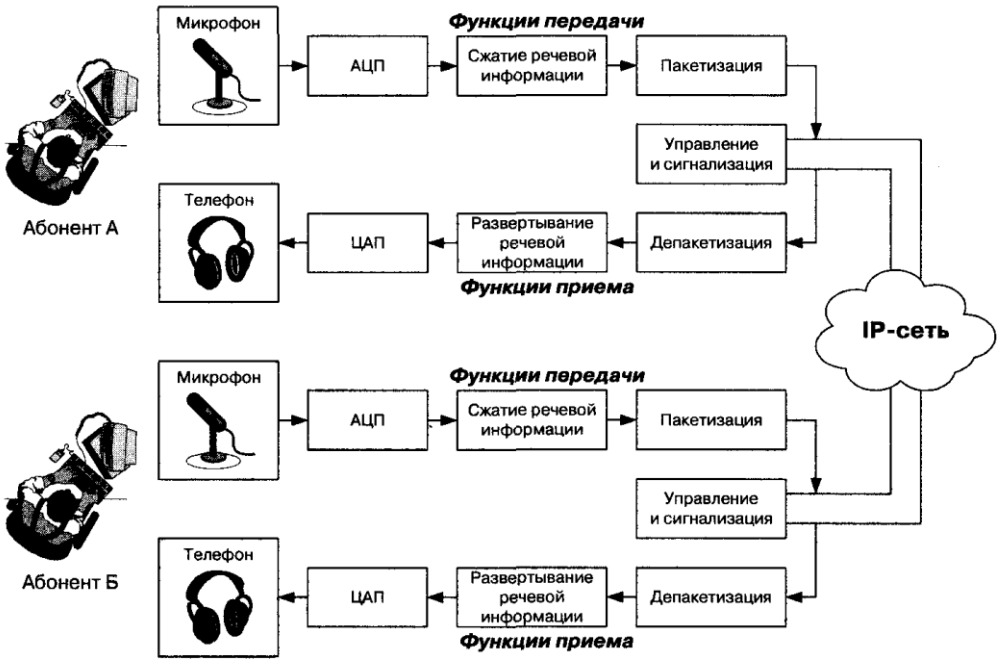


Рис.2.8. Сценарий IP-телефонии "компьютер-компьютер"

Для проведения телефонных разговоров друг с другом абоненты А и Б должны иметь доступ к Интернет или к другой сети с протоколом IP. Предположим, что такая IP-сеть существует, и оба абонента подключены к ней. Рассмотрим возможный алгоритм организации связи между этими абонентами.

1. Абонент А запускает свое приложение IP-телефонии, поддерживающее протокол H.323.
2. Абонент Б уже заранее запустил свое приложение IP-телефонии, поддерживающее протокол H.323.
3. Абонент А знает доменное имя абонента В элемент системы имен доменов - Domain Name System (DNS), вводит это имя в раздел «кому позвонить» в своем приложении IP-телефонии и нажимает кнопку Return.
4. Приложение IP-телефонии обращается к DNS-серверу (который в данном примере реализован непосредственно в персональном компьютере абонента А) для того, чтобы преобразовать доменное имя абонента Б в IP-адрес.
5. Сервер DNS возвращает IP-адрес абонента Б.
6. Приложение IP-телефонии абонента А получает IP-адрес абонента Б и отправляет ему сигнальное сообщение H.225 Setup.
7. При получении сообщения H.225 Setup приложение абонента Б сигнализирует ему о входящем вызове.
8. Абонент Б принимает вызов и приложение IP-телефонии отправляет ответное сообщение H.225 Connect.
9. Приложение IP-телефонии у абонента А начинает взаимодействие с приложением у абонента Б в соответствии с рекомендацией H.245.
10. После окончания взаимодействия по протоколу H.245 и открытия

логических каналов абоненты А и Б могут разговаривать друг с другом через IP-сеть.

2.6. Пакетная обработка речи - Протоколы RTP и RTCP

В сетях на основе протокола IP все данные - голос, текст, видео, компьютерные программы или информация в любой другой форме - передаются в виде пакетов. Процесс передачи голоса по IP-сети состоит из нескольких этапов:

- оцифровка голоса (АЦП)
- анализ и обработка оцифрованные данные с целью уменьшения физического объема данных (подавление ненужных пауз и фонового шума, компрессирование)
- упаковка данных в формат RTP пакетов (разбивка данных на пакеты, добавка протокольная информация - адрес получателя, порядковый номер пакета, дополнительные данные для коррекции ошибок)
- временное накопление необходимого количества данных

Извлечение переданной голосовой информации из полученных пакетов также происходит в несколько этапов.

- проверка порядковой последовательности пакетов
- временное накопление пакетов.
- включение алгоритма аппроксимации для восстановления потерянных пакетов
- декомпрессия данных
- преобразование оцифрованных данных в аудио-сигнал (ЦАП)

Приложения, обеспечивающие передачу речевой и видеоинформации, используют сервис транспортного уровня без установления соединений (например, UDP). При этом каждое приложение может обеспечивать формирование полезной нагрузки пакетов специфическим образом, включая необходимые для функционирования поля и данные. Однако, данные разной природы (речь, видео) имеют общие особенности, которые требуют обеспечения вполне определенной функциональности при их передаче по сети. Это позволяет сформировать некий общий транспортный уровень, объединяющий функции, общие для потоковых данных разной природы, и используемый всеми соответствующими приложениями, придав протоколу этого уровня статус стандарта. Комитетом IETF был разработан протокол транспортировки информации в реальном времени – Real-time Transport Protocol (RTP), который стал базисом практически для всех приложений, связанных с интерактивной передачей речевой и видеоинформации по сети с маршрутизацией пакетов.

Характерные для IP-сетей временные задержки и вариация задержки пакетов (джиттер) могут серьезно исказить информацию, чувствительную к

задержке, например, речь и видеоинформацию, сделав ее абсолютно непригодной для восприятия. Отметим, что вариация задержки пакетов гораздо сильнее влияет на субъективную оценку качества передачи, чем абсолютное значение задержки.

Уже длительное время ведется работа по созданию методов уменьшения джиттера и задержек. Именно протокол RTP позволяет компенсировать негативное влияние джиттера на качество речевой и видеоинформации. В то же время, он не имеет собственных механизмов, гарантирующих своевременную доставку пакетов или другие параметры качества услуг, -это осуществляют нижележащие протоколы. Он даже не обеспечивает все те функции, которые обычно предоставляют транспортные протоколы, в частности функции исправления ошибок и управления потоком. Обычно протокол RTP базируется на протоколе UDP и использует его функции, но может работать и поверх других транспортных протоколов.

Существует несколько серьезных причин, по которым транспортный протокол TCP плохо подходит для передачи чувствительной к задержкам информации. Во-первых, это алгоритм надежной доставки пакетов. Пока отправитель повторно передаст пропавший пакет, получатель будет ждать, результатом чего может быть недопустимое увеличение задержки. Во-вторых, алгоритм управления при перегрузке в протоколе TCP далеко не оптимален для передачи речи и видеоинформации. При обнаружении потерь пакетов протокол TCP уменьшает размер окна, а затем будет его медленно увеличивать. Однако передача речевой и видеоинформации осуществляется на вполне определенных, фиксированных скоростях, которые нельзя мгновенно уменьшить, не ухудшив качество предоставляемых услуг. Правильной реакцией на перегрузку для информационных потоков этих типов было бы изменение метода кодирования, частоты видеокадров или размера видеоизображения.

Основной функцией протокола RTCP является организация обратной связи приемника с отправителем информации для отчета о качестве получаемых данных. Протокол RTCP передает сведения (как от приемника, так и от отправителя) о числе переданных и потерянных пакетов, значении джиттера, задержке и т.д. Эта информация может быть использована отправителем для изменения параметров передачи, например для уменьшения коэффициента сжатия информации с целью улучшения качества ее передачи.

2.7. Типы речевых кодеков

Одним из важных факторов эффективного использования пропускной способности IP-канала, является выбор оптимального алгоритма кодирования/декодирования речевой информации — кодека.

Все существующие сегодня типы речевых кодеков по принципу действия можно разделить на три группы:

1. Кодеки с импульсно-кодовой модуляцией ИКМ и адаптивной дифференциальной импульсно-кодовой модуляцией АДИКМ, появившиеся в конце 50-х годов и использующиеся сегодня в системах традиционной телефонии. В большинстве случаев, представляют собой сочетание АЦП/ЦАП.

2. Кодеки с вокодерным преобразованием речевого сигнала возникли в системах мобильной связи для снижения требований к пропускной способности радиотракта. Эта группа кодеков использует гармонический синтез сигнала на основании информации о его вокальных составляющих — фонемах. В большинстве случаев, такие кодеки реализованы как аналоговые устройства.

3. Комбинированные (гибридные) кодеки сочетают в себе технологию вокодерного преобразования/синтеза речи, но оперируют уже с цифровым сигналом посредством специализированных DSP. Кодеки этого типа содержат в себе ИКМ или АДИКМ кодек и реализованный цифровым способом вокодер.

На рис.2.10 представлена усредненная субъективная оценка качества кодирования речи для вышеперечисленных типов кодеков. В голосовых шлюзах IP-телефонии понятие кодека подразумевает не только алгоритма кодирования/декодирования, но и их аппаратную реализацию. Большинство кодеков, используемых в IP-телефонии, описаны рекомендациями семейства «G» стандарта H.323 (рис.2.11).

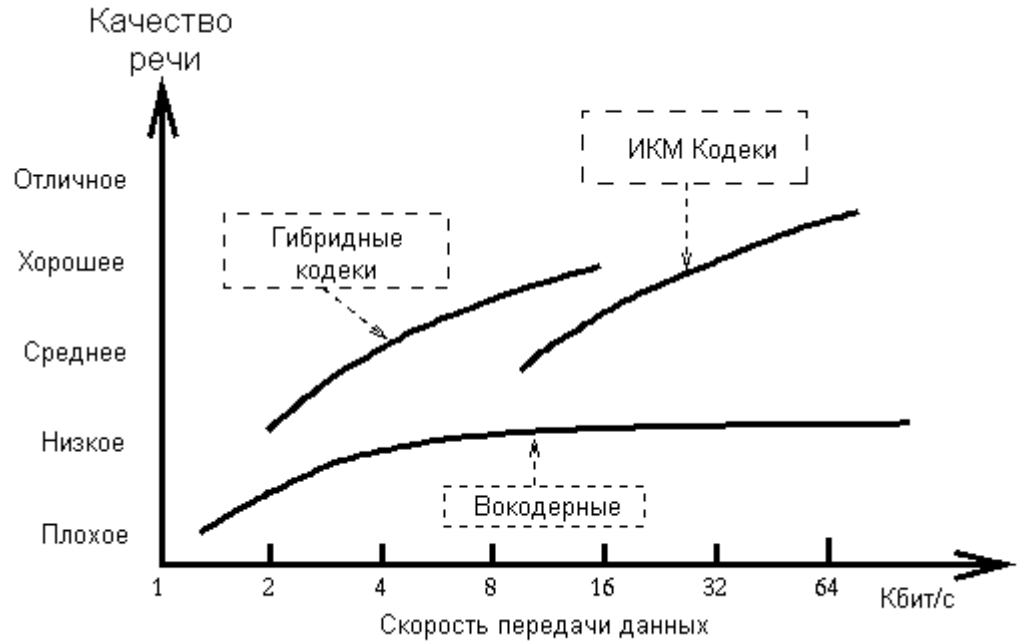


Рис.2.10. Усредненная субъективная оценка качества кодирования речи для различных типов кодеков

Все методы кодирования, основанные на определенных предположениях о форме сигнала, не подходят при передаче сигнала с резкими скачками амплитуды. Именно такой вид имеет сигнал,

генерируемый модемами или факсимильными аппаратами, поэтому аппаратура, поддерживающая сжатие,должна автоматически распознавать сигналы факс-аппаратов и модемов и обрабатывать их иначе, чем голосовой трафик. Многие методы кодирования берут свое начало от метода кодирования с линейным предсказанием LPC

Рис.2.11. Кодеки семейства H.323

(Linear Predictive Coding). В качестве входного сигнала в LPC используется последовательность цифровых значений амплитуды, но алгоритм кодирования применяется не к отдельным цифровым значениям, а к определенным их блокам. Для каждого такого блока значений вычисляются

его характерные параметры: частота, амплитуда и ряд других. Именно эти значения и передаются по сети. При таком подходе к кодированию речи, во-первых, возрастают требования к вычислительным мощностям специализированных процессоров, используемых для обработки сигнала, а во-вторых, увеличивается задержка при передаче, поскольку кодирование применяется не к отдельным значениям, а к некоторому их набору, который перед началом преобразования следует накопить в определенном буфере.

Важно, что задержка в передаче речи связана не только с необходимостью обработки цифрового сигнала (эту задержку можно уменьшать, увеличивая мощность процессора), но и непосредственно с характером метода сжатия. Метод кодирования с линейным предсказанием LPC позволяет достигать очень больших степеней сжатия, которым соответствует полоса пропускания 2,4 или 4,8 кбит/с, однако качество звука здесь сильно страдает. Поэтому в коммерческих приложениях он не используется, а применяется в основном для ведения служебных переговоров. Более сложные методы сжатия речи основаны на применении LPC в сочетании с элементами кодирования формы сигнала. В этих алгоритмах используется кодирование с обратной связью, когда при передаче сигнала осуществляется оптимизация кода. Закодировав сигнал, процессор пытается восстановить его форму и сличает результат с исходным сигналом, после чего начинает варьировать параметры кодировки, добиваясь наилучшего совпадения. Достигнув такого совпадения, аппаратура передает полученный код по линиям связи; на противоположном конце происходит восстановление звукового сигнала. Ясно, что для использования такого метода требуются еще более серьезные вычислительные мощности.

Одной из самых распространенных разновидностей описанного метода кодирования является метод LD CELP (Low-Delay Code-Excited Linear Prediction). Он позволяет достичь удовлетворительного качества воспроизведения при пропускной способности 16кбит/с. Алгоритм применяется к последовательности цифр, получаемых в результате аналого-цифрового преобразования голосового сигнала с 16-разрядным разрешением. Пять последовательных цифровых значений кодируются одним 10-битовым блоком — это и дает те самые 16 кбит/с. Для применения этого метода требуются большие вычислительные мощности; в частности, в марте 1995 г. ITU принял новый стандарт — G.723, который предполагается использовать при сжатии речи для организации видеоконференций по телефонным сетям. Этот стандарт представляет собой часть более общего стандарта H.324, описывающего подход к организации таких видеоконференций. Цель — организация видеоконференций с использованием обычных модемов. Основой O.723 является метод сжатия речи MP-MLQ (Multipulse Maximum Likelihood Quantization). Он позволяет добиться весьма существенного сжатия речи при сохранении достаточно высокого качества звучания. В основе метода лежит описанная выше процедура оптимизации; с помощью различных усовершенствований можно сжимать речь до уровня 4,8; 6,4; 7,2 и

8,0 кбит/с. Структура алгоритма позволяет на основе программного обеспечения изменять степень сжатия голоса в ходе передачи. Вносимая кодированием задержка не превышает 20мс. Повышая эффективность использования полосы пропускания, механизмы сжатия речи в то же время могут привести к ухудшению ее качества и увеличению задержек.

Далее рассмотрены некоторые основные кодеки, используемые в шлюзах IP-телефонии операторского уровня.

Кодек G.711. Рекомендация G.711, утвержденная МККТТ в 1984г., описывает кодек, использующий ИКМ преобразование аналогового сигнала с точностью 8 бит, тактовой частотой 8 кГц и простейшей компрессией амплитуды сигнала. Скорость потока данных на выходе преобразователя составляет 64 кбит/с (8 битх8 кГц). Для снижения шума квантования и улучшении преобразования сигналов с небольшой амплитудой при кодировании используется нелинейное квантование по уровню согласно специальному псевдо-логарифмическому закону: А-закон для европейской системы ИКМ-30/32 или μ- закон для североамериканской системы ИКМ-24.

Первые ИКМ кодеки с нелинейным квантованием появились уже в 60г.г. XXв. Кодеки G.711 широко распространен в системах традиционной телефонии с коммутацией каналов, Несмотря на то, что рекомендация G.711 в стандарте H.323 является основной и первичной, в шлюзах IP-телефонии данный кодек применяется редко из-за высоких требований к полосе пропускания и задержкам в канале передачи. Использование G.711 в системах IP-телефонии обосновано лишь в тех случаях, когда требуется обеспечить максимальное качество кодирования речевой информации при небольшом числе одновременных разговоров.

Кодек G.726. Один из старейших алгоритмов сжатия речи ADPCM - адаптивная дифференциальная ИКМ (стандарт G.726 был принят в 1984г.). Этот алгоритм дает практически такое же качество воспроизведения речи, как и ИКМ, однако для передачи информации при его использовании требуется полоса всего в 16-32 кбит/с. Метод основан на том, что в аналоговом сигнал передающем речь, невозможны резкие скачки интенсивности. Поэтому, если кодировать не саму амплитуду сигнала, а ее изменение по сравнению с предыдущим значением, то можно обойтись меньшим числом разрядов. В ADPCM изменение уровня сигнала кодируется четырехразрядным числом, при этом частота измерения амплитуды сигнала сохраняется неизменной. Процесс преобразования не вносит существенной задержки и требует от DSP 5,5-6,4 MIPS (Million Instructions Per Second). Кодек может применяться совместно с кодеком G.711 для снижения скорости кодирования последнего. Кодек предназначен для использования в системах видеоконференций.

Кодек G.723.1. Рекомендация G.723.1 описывает гибридные кодеки, использующие технологию кодирования речевой информации, сокращенно называемую — MP-MLQ (Multy-Pulse — Multy Level quantization — множественная импульсная, многоуровневая квантизация), данные кодеки

можно охарактеризовать, как комбинацию АЦП/ЦАП и вокодера. Своим возникновением гибридные кодеки обязаны системам мобильной связи. Применение вокодера позволяет снизить скорость передачи данных в канале, что принципиально важно для эффективного использования радиотракта и IP-канала. Основной принцип работы вокодера — синтез исходного речевого сигнала посредством адаптивной замены его гармонических составляющих соответствующим набором частотных фонем и согласованными шумовыми коэффициентами. Кодек О.723 осуществляет преобразование аналогового сигнала в поток данных со скоростью 64 кбит/с (ИКМ), а затем при помощи многополосного цифрового фильтра/вокодера выделяет частотные фонемы, анализирует их и передает по IP-каналу информацию только о текущем состоянии фонем в речевом сигнале. Данный алгоритм преобразования позволяет снизить скорость кодированной информации до 5,3-6,3 кбит/с без видимого ухудшения качества речи. Кодек имеет две скорости и два варианта кодирования: 6,3 кбит/с с алгоритмом MP-MLQ и 5,3 кбит/с с алгоритмом CELP. Первый вариант предназначен для сетей с пакетной передачей голоса и обеспечивает лучшее качество кодирования по сравнению с вариантом CELP, но менее адаптирован к использованию в сетях со смешанным типом трафика (голос/данные).

Процесс преобразования требует от DSP 16,4-16,7 MIPS и вносит задержку 37мс. Кодек G.723.1 широко применяется в голосовых шлюзах и прочих устройствах IP-телефонии. Кодек уступает по качеству кодирования речи кодеку G.729a, но менее требователен к ресурсам процессора и пропускной способности канала.

Кодеки G.729. Семейство включает кодеки G.729, G.729 Аппех А, G.729 Аппех В (содержит VAD , и генератор комфортного шума). Кодеки G.729 сокращенно называют CS-ACELP Conjugate Structure - Algebraic Code Excited Linear Prediction — сопряженная структура с управляемым алгебраическим кодом линейным предсказанием. Процесс преобразования использует DSP 21,5 MIPS и вносит задержку 15 мс. Скорость кодированного речевого сигнала составляет 8 кбит/с. В устройствах VoIP данный кодек занимает лидирующее положение, обеспечивая наилучшее качество кодирования речевой информации при достаточно высокой компрессии.

Кодек G.728. Гибридный кодек, описанный в рекомендации G.728 в 1992 г. относится к категории LD-CELP - Low Delay - Code Excited Linear Prediction - кодек с управляемым кодом линейным предсказанием и малой задержкой. Кодек обеспечивает скорость преобразована 16 кбит/с, вносит задержку при кодировании от 3 до 5 мс и для реализации необходим процессор с быстродействием более 40 MIPS. Кодек предназначен для использования, в основном, в системах видеоконференций. В устройствах IP-телефонии данный кодек применяется достаточно редко.

2.8. Основные характеристики рассмотренных кодеков

Основные характеристики рассмотренных кодеков приведены в табл.2.2.

Скорость передачи, которую предусматривают имеющиеся сегодня узкополосные кодеки, лежит в пределах 1.2-64кбит/с. Естественно, что от этого параметра прямо зависит качество воспроизводимой речи. Существует множество подходов к проблеме определения качества. Наиболее широко используемый подход оперирует оценкой MOS (Mean Opinion Score), которая определяется для конкретного кодека как средняя оценка качества большой группой слушателей по пятибалльной шкале. Для прослушивания экспертам предъявляются разные звуковые фрагменты - речь, музыка, речь на фоне различного шума и т.д. Оценки интерпретируют следующим образом:

- 4-5 - высокое качество; аналогично качеству передачи речи в ISDN, или еще выше;
- 3.5-4 - качество ТфОП (toll quality); аналогично качеству речи, передаваемой с помощью кодека АДИКМ при скорости 32кбит/с. Такое качество обычно обеспечивается в большинстве телефонных разговоров. Мобильные сети обеспечивают качество чуть ниже toll quality;
- 3-3.5 - качество речи, по-прежнему, удовлетворительно, однако его ухудшение явно заметно на слух;
- 2.5-3 - речь разборчива, однако требует концентрации внимания для понимания. Такое качество обычно обеспечивается в системах связи специального применения (например, в вооруженных силах).

В рамках существующих технологий качество ТфОП (toll quality) невозможно обеспечить при скоростях менее 5 Кбит/с.

Таблица.2.2.

Основные характеристики кодеков (данные компании CISCO Systems)

Кодек	Тип кодека	Скорость кодирования	Размер кадра	Оценка
G.711	ИКМ	64 Кбит/с	0,125 мс	4,1
G.726	АДИКМ	32 Кбит/с	0,125 мс	3,85
G.728	LD – CELP	16 Кбит/с	0,625 мс	3,61
G.729	CS – ACELP (без VAD)	8 Кбит/с	10 мс	3,92
G.729	2-х кратное кодирование	8 Кбит/с	10 мс	3,27
G.729	3-х кратное кодирование	8 Кбит/с	10 мс	2,68
G.729a	CS – ACELP	8 Кбит/с	10 мс	3,7
G.723.1	MP – MLQ	6,3 Кбит/с	30 мс	3,9
G.723.1	ACELP	5,3 Кбит/с	30 мс	3,65

Количественными характеристиками ухудшения качества речи являются единицы QDU (Quantization Distortion Units): 1 QDU соответствует ухудшению качества при оцифровке с использованием стандартной

процедуры ИКМ; значения QDU для основных методов компрессии приведены в табл.2.3.

Таблица 2.3.

Значения QDU для основных методов компрессии

Метод компрессии	QDU
ADPCM 32 кбит/с	3,5
ADPCM 24 кбит/с	7
LD-CELP 16 кбит/с	3,5
CS-CELP 8 кбит/с	3,5

Дополнительная обработка речи всегда ведет к дальнейшей потере качества. Согласно рекомендациям МСЭ-Т, для международных вызовов величина QDU не должна превышать 14, причем передача разговора по международным магистральным каналам ухудшает качество речи, как правило, на 4 QDU. Следовательно, при передаче разговора по национальным сетям должно теряться не более 5 QDU. Поэтому для качественной передачи речи процедуру компрессии/декомпрессии желательно применять в сети только один раз. В некоторых странах это является обязательным требованием регулирующих органов по отношению к корпоративным сетям, подключенным к сетям общего пользования. Подавление пауз (silence suppression) — важная функция АТМ-коммутаторов. Суть технологии подавления пауз заключается в определении различия между моментами активной речи и молчания в период. В результате применения этой технологии генерация ячеек происходит только в активного разговора. Поскольку в процессе типичного разговора по телефону тишина составляет до 60% времени, происходит двукратная оптимизация по количеству данных, должны быть переданы по линии. Объединение технологии сжатия речи и подавления пауз речи в коммутаторах приводит к уменьшению потока данных в канале до восьми раз.

Современные продукты для IP-телефонии применяют самые разные кодеки, стандартные и нестандартные. Конкурентами являются кодеки GSM (13,5 кбит/с) и кодеки МСЭ-Т серии G, использование которых предусматривается стандартом Н.323 для связи по IP-сети. Единственным обязательным для применения кодеком в Н.323-совместимых продуктах остается стандарт G.711: выдаваемые им массивы данных составляют от 56 до 64 кбит/с. В качестве дополнительных высокопроизводительных кодеков стандарт Н.323 рекомендует G.723 и G,729 — последние способны сжимать оцифрованную 16-разрядную ИКМ- речь длительностью 10 мс всего в 10 байт. Стандарт G.729 уже получил широкое распространение в передачи голоса по IP; его поддерживают значительное число производителей продуктов для IP-телефонии.

Контрольные вопросы

1. Какие виды соединений могут быть реализованы в сети IP-телефонии?
2. В чём разница понятий IP-телефония (IP Telephony), голос по IP-сетям (Voice over IP - VoIP), Интернет-телефония (Internet Telephony)?
3. На какие этапы делится пакетная обработка речи?
4. Какие функции выполняет маршрутизатор в схеме «компьютер-телефон»?
5. Какую роль выполняет хост в IP-телефонии?
6. Каково назначение шлюза в IP-телефонии?
7. Что подразумевается под «web-браузером» в схеме «web-браузер-телефон»?
8. В чем отличие сети Интернет от сети ТфОП?
9. Какие преимущества имеет технология IP-телефония?
10. Каково назначение протокола RTP?
11. Назначение протокола RTCP?
12. На какие группы можно разделить речевые кодеки?
13. Какие основные кодеки используются в шлюзах IP-телефонии?
14. Что такое DSP?
15. Что такое MIPS?
16. Что такое VAD?
17. Что такое генератор комфортного шума?
18. Что такое оценка MOS?
19. Что означает величина 1 QDU?

3. АРХИТЕКТУРА СЕТИ NGN, ОСНОВНЫЕ ТЕХНОЛОГИИ ДЛЯ ПОСТРОЕНИЯ УРОВНЕЙ

3.1. Общие подходы к построению мультисервисных сетей связи

Общие подходы к построению мультисервисных сетей связи нашли отражение в концепции перспективных сетей связи следующего поколения - NGN.

Базовым принципом концепции NGN является отделение друг от друга функций переноса и коммутации, функций управления вызовом и функций управления услугами. Фирмы-производители при разработке оборудования NGN вводят разное количество уровней. Например, при начальных разработках фирмы Lucent и HUAWEI вводили четыре слоя, а фирма Alcatel – 6. Фирма Alcatel определяла следующие слои архитектуры NGN:

- уровень доступа,
- уровень шлюзов (поддерживает стыковку с сетями подвижной связи, ТфОП и другими),
- уровень транспорта,
- уровень управления,
- уровень приложений,
- уровень эксплуатационного управления.

Все слои построены на открытых элементах и взаимодействуют друг с другом на основе открытых интерфейсов. Разнообразные услуги доставляются по общей транспортной сети, которая построена по технологии IP, к многочисленным сетям доступа, а управление услугами оператор осуществляет с общей плоскости управления независимо от сетей доступа. Преимущества IP-транспорта особенно сказываются в случае, когда оператор хочет ввести новые услуги. Уровень шлюзов отвечает за стыковку различных сетей (подвижных, фиксированных, широкополосного доступа и т.д.) с пакетной транспортной сетью. На уровне управления оборудование программной коммутации управляет вызовами для того, чтобы обеспечить связность абонентов и доставить услуги к терминалам пользователей. Также оборудование программной коммутации подключает нужные услуги конечным пользователям со слоя приложений, которому принадлежат все новые мультимедийные услуги. И, наконец, венчает эту слоистую структуру уровень эксплуатационного управления.

В настоящее время наибольшее распространение получила четырехуровневая архитектура ССП.

2.2. Функциональная модель сетей NGN

Функциональная модель сетей NGN состоит из 4 уровней

Рис. 3.1. Архитектура сети следующего поколения

- уровень управления услугами;
- уровень управления коммутацией;
- транспортный уровень;
- уровень доступа.

Уровень управления услугами содержит функции управления логикой услуг и приложений и представляет собой распределенную вычислительную среду, обеспечивающую:

- предоставление инфокоммуникационных услуг;
- управление услугами;
- создание и внедрение новых услуг;
- взаимодействие различных услуг.

Данный уровень позволяет реализовать специфику услуг и применять одну и ту же программу логики услуг вне зависимости от типа транспортной сети и способа доступа. Наличие этого уровня позволяет также вводить на сети электросвязи любые новые услуги без вмешательства в функционирование других уровней.

Уровень управления может включать множество независимых подсистем ("сетей услуг"), базирующихся на различных технологиях, имеющих своих абонентов и использующих свои, внутренние системы адресации.

Операторам связи требуются механизмы, позволяющие быстро и гибко развертывать, а также изменять услуги в зависимости от индивидуальных потребностей пользователей.

Такие механизмы предусмотрены открытой сервисной архитектурой OSA (Open Services Access) – основной концепцией будущего развития сетей электросвязи в части внедрения и оказания новых дополнительных услуг.

При создании систем на основе OSA должны присутствовать следующие

ключевые моменты:

- открытая среда для создания услуг;
- открытая платформа управления услугами.

На протяжении нескольких лет различными организациями предлагалось несколько вариантов реализации концепции OSA, пока в 1998 г. не был сформирован консорциум Parlay Group, который занимается созданием спецификаций открытого API (Application Programming Interface), позволяющего управлять сетевыми ресурсами и получать доступ к сетевой информации.

Архитектура Parlay является одной из практических реализаций концепции OSA (рис. 3.2). Как показано на рисунке, разные сети связи имеют различные сетевые элементы:

- в сети подвижной электросвязи второго поколения входят SGSN (Serving GPRS Support Node) и MSC (Mobile Switching Center);
- в телефонную сеть общего пользования входит SSP (Service Switching Point) коммутатор услуг в ТфОП;
- в сети подвижной электросвязи третьего поколения входит S-CSCF (Serving Call Session Control Function);
- ведомственные АТС.

Каждый из этих элементов выходит на шлюз (Gateway) по своему протоколу, а задача шлюза по концепции OSA/Parlay состоит в том, чтобы свести все протоколы к единым интерфейсам API. Тогда приложения можно писать без учета особенностей нижележащих сетей, и следует только строго придерживаться интерфейсов API.

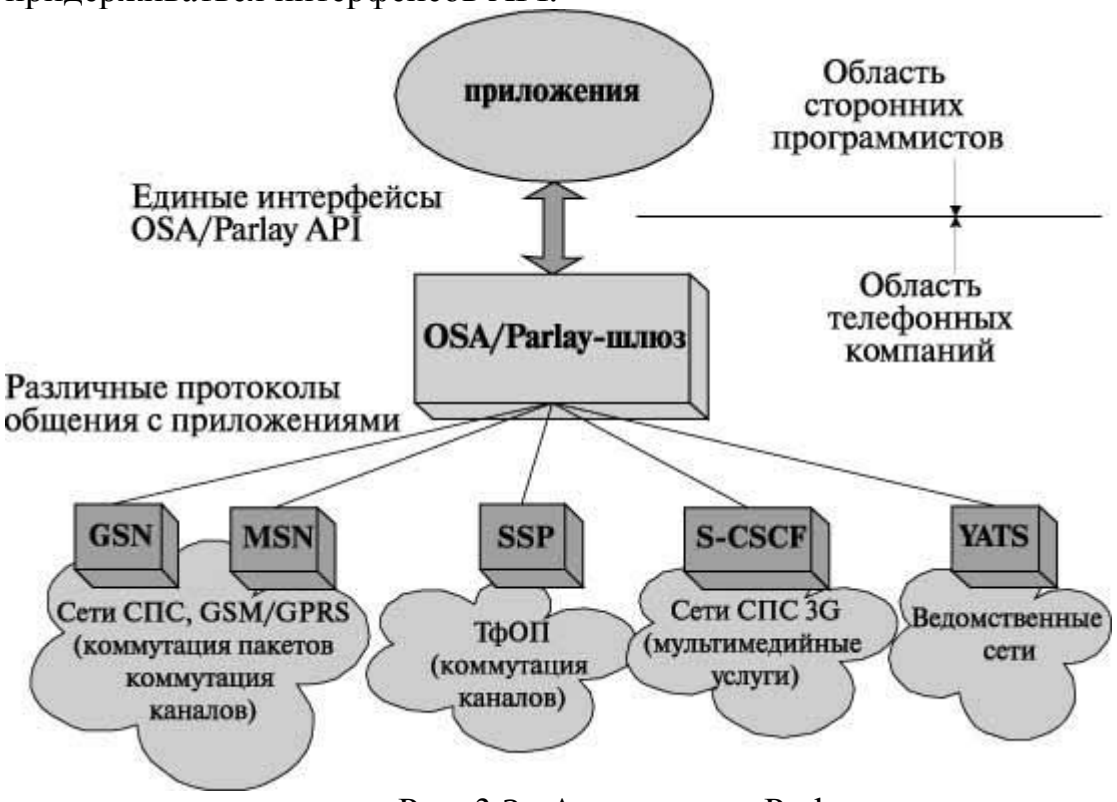


Рис. 3.2. Архитектура Parlay

Оказалось, что концепция Parlay является слишком сложной для массового привлечения сторонних программистов. Выяснилось, что для оказания 80% услуг требуется лишь 20% возможностей Parlay-шлюза. Следовательно, для подавляющего большинства программистов требование освоить весь набор Parlay-интерфейсов является чрезмерно завышенным. По мере уменьшения разнообразия возможностей сети растет число разработчиков приложений, что весьма важно для освоения прибыльного рынка приложений. Эти рассуждения иллюстрирует рис. 3.3, где показаны слева четыре набора функций сети:

Рис. 3.3. Зависимость возможностей сети от количества разработчиков приложений

1. Наибольшие возможности дает использование протоколов (INAP, CAMEL, SIP и др.), как это делается до сих пор, но при этом сообщество разработчиков является минимальным.
2. Значительное упрощение дают открытые интерфейсы API: JAIN, Parlay, OSA, а также собственные интерфейсы (Proprietary APIs).
3. Еще больше программистов разрабатывают web-услуги, используя простые языки скриптов: XML, VXML, CPML, WDSL.
4. Замысел Parlay X состоит в еще большем упрощении программирования web-услуг.

Приложения могут быть написаны на языках C++, Java, Visual Basic, PHP и др. Для разработки приложений Parlay X основным языком программирования является язык XML. В качестве транспортных средств чаще всего используются:

CORBA – универсальный объектно-ориентированный протокол взаимодействия распределенных систем;

SOAP – упрощенный протокол общения распределенных объектов, основан на языке XML, используется в сочетании с протоколом HTTP.

Самой перспективной на сегодняшний день объектной технологией является SOAP/XML, так как она наиболее универсальна, основывается на международных стандартах и имеет обширную поддержку со стороны различных производителей программного обеспечения. Эта технология чаще всего используется для создания web-сервисов и для обеспечения их взаимодействия с клиентским процессом.

Задача уровня управления коммутацией — обработка информации сигнализации, маршрутизация вызовов и управление потоками. Данный

уровень поддерживает логику управления, которая необходима для обработки и маршрутизации трафика.

Функция установления соединения реализуется на уровне элементов базовой сети под внешним управлением оборудования программного коммутатора (Softswitch). Исключением являются АТС с функциями контроллера шлюзов (MGC – Media Gateway Controller), которые сами выполняют коммутацию на уровне элемента транспортной сети.

В случае использования на сети нескольких Softswitch они взаимодействуют посредством соответствующих протоколов (как правило, семейство SIP-T) и обеспечивают совместное управление установлением соединения. Softswitch должен осуществлять:

- обработку всех видов сигнализации, используемых в его домене;
- хранение и управление абонентскими данными пользователей, подключаемых к его домену непосредственно или через оборудование шлюзов доступа;
- взаимодействие с серверами приложений для оказания расширенного списка услуг пользователям сети.

Более подробно Softswitch будет рассмотрен в следующих лекциях.

Задача транспортного уровня — коммутация и прозрачная передача информации пользователя. В ССП операторы получат возможность наращивать объемы услуг, что в свою очередь приведет к росту требований к производительности и емкости сетей транспортного уровня. Основными требованиями к таким сетям являются:

- высокая надежность оборудования узлов;
- поддержка функций управления трафиком;
- хорошая масштабируемость.

Надежность выходит на первое место, так как ССП должны обеспечивать передачу разнородного трафика, в том числе чувствительного к задержкам, который ранее передавался с помощью классических систем передачи с временным разделением каналов иерархий SDH или PDH. В ряде случаев создаваемые транспортные сети будут заменять собой часть инфраструктуры существующих традиционных сетей передачи. Конечно, они должны соответствовать требованиям технических нормативных правовых актов, предъявляемым к заменяемой сети.

МСЭ-Т определяет следующие требования к возможностям транспортного уровня:

- поддержка соединений в реальном времени и соединений, нечувствительных к задержкам;
- поддержка различных моделей соединений: "точка-точка ", "точка-многоточие ", "многоточие-многоточие ", "многоточие-точка ";
- гарантированные уровни производительности, надежности, доступности, масштабируемости.

Транспортный уровень ССП рассматривается как уровень, составными

частями которого являются сеть доступа и базовая сеть.

Под сетью доступа понимается системно-сетевая инфраструктура, которая состоит из абонентских линий, узлов доступа и систем передачи, обеспечивающих подключение пользователей к точке агрегации трафика (к сети ССП или к традиционным сетям электросвязи). Для организации уровня доступа могут использоваться различные среды передачи. Это может быть медная пара, коаксиальный кабель, волоконно-оптический кабель, радиоканал, спутниковые каналы либо любая их комбинация.

Особенностью инфраструктуры ССП является использование универсальной базовой сети, базирующейся на технологиях пакетной коммутации.

Базовая сеть – это универсальная сеть, реализующая функции транспортировки и коммутации. В соответствии с данными функциями базовая сеть представляется в виде трех уровней (рис. 3.4):

- технология коммутации пакетов;
- технологии формирования тракта;
- среда передачи сигналов.

Нижний уровень модели – среда передачи сигналов. Этот уровень должен быть реализован на кабелях с оптическими волокнами (ОВ) или на цифровых радиорелейных линиях (РРЛ).

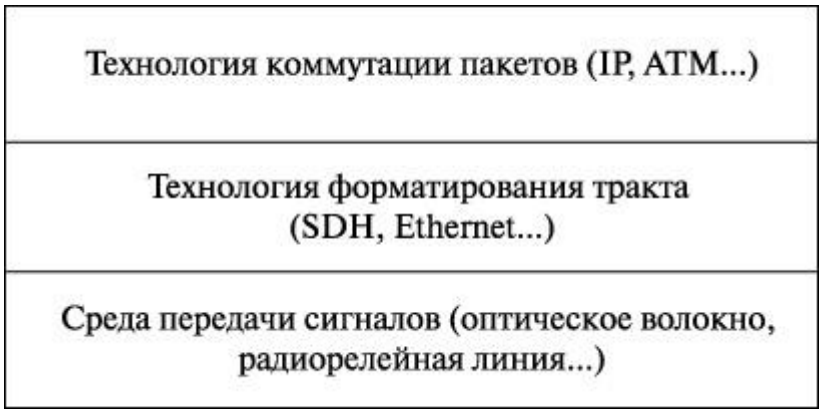


Рис. 3.4. Модель базовой сети

Сегодня при выборе технологической основы перспективной считается IP, ввиду того, что:

- использование технологии IP/MPLS в среде Ethernet позволяет повысить масштабируемость и качество обслуживания до уровня, необходимого для транспортных сетей, а спецификации MPLS RSVP-TE Fast Reroute обеспечивает восстанавливаемость трактов в пределах 50 мс. Это означает, что сети Ethernet приобретают характеристики и надежность SDH или ATM;
- количество приложений, использующих протокол IP, будет возрастать, соответственно доля трафика IP будет увеличиваться, и, как следствие, неизбежны проблемы технологии ATM, связанные с дополнительными

накладными расходами полосы пропускания при передаче IP-трафика, вследствие чего происходит увеличение стоимости реализации сетевых решений на базе ATM.

Архитектура сети электросвязи, построенной в соответствии с концепцией ССП, представлена на рис. 3.5.

В состав транспортной сети NGN могут входить:

- транзитные узлы, выполняющие функции переноса и коммутации;
- оконечные (граничные) узлы, обеспечивающие доступ абонентов к мультисервисной сети;
- контроллеры сигнализации, выполняющие функции обработки информации сигнализации, управления вызовами и соединениями;
- шлюзы, позволяющие осуществить подключение традиционных сетей связи (ТФОП, СПД, СПС).

Контроллеры сигнализации могут быть вынесены в отдельные устройства, предназначенные для обслуживания нескольких узлов коммутации. Использование общих контроллеров позволяет рассматривать их как единую систему коммутации, распределенную по сети. Такое решение не только упрощает алгоритмы установления соединений, но и является наиболее экономичным для операторов и поставщиков услуг, так как позволяет заменить дорогостоящие системы коммутации большой емкости небольшими, гибкими и доступными по стоимости даже мелким поставщикам услуг.

Назначением транспортной сети является предоставление услуг переноса.

Доступ к ресурсам базовой сети осуществляется через граничные узлы, к которым подключается оборудование сети доступа или осуществляется связь с существующими сетями. В последнем случае граничный узел выполняет функции межсетевого шлюза.

К уровню доступа относятся:

- шлюзы;
- сеть доступа (сеть электросвязи, обеспечивающая подключение оконечных терминальных устройств пользователя к оконечному узлу транспортной сети);
- оконечное абонентское оборудование.

К технологиям построения сетей доступа относятся:

- беспроводные технологии (Wi-Fi, WiMAX);
- технологии на основе систем кабельного телевидения (DOCSIS, DVB);
- технологии xDSL;
- оптоволоконные технологии (пассивные оптические сети (PON)).

С развитием технологий электросвязи становится все проблематичней провести четкую грань между транспортным уровнем и уровнем доступа. Так, например, цифровой абонентский мультиплексор доступа (DSLAM) может быть отнесен и к тому, и к другому уровню.

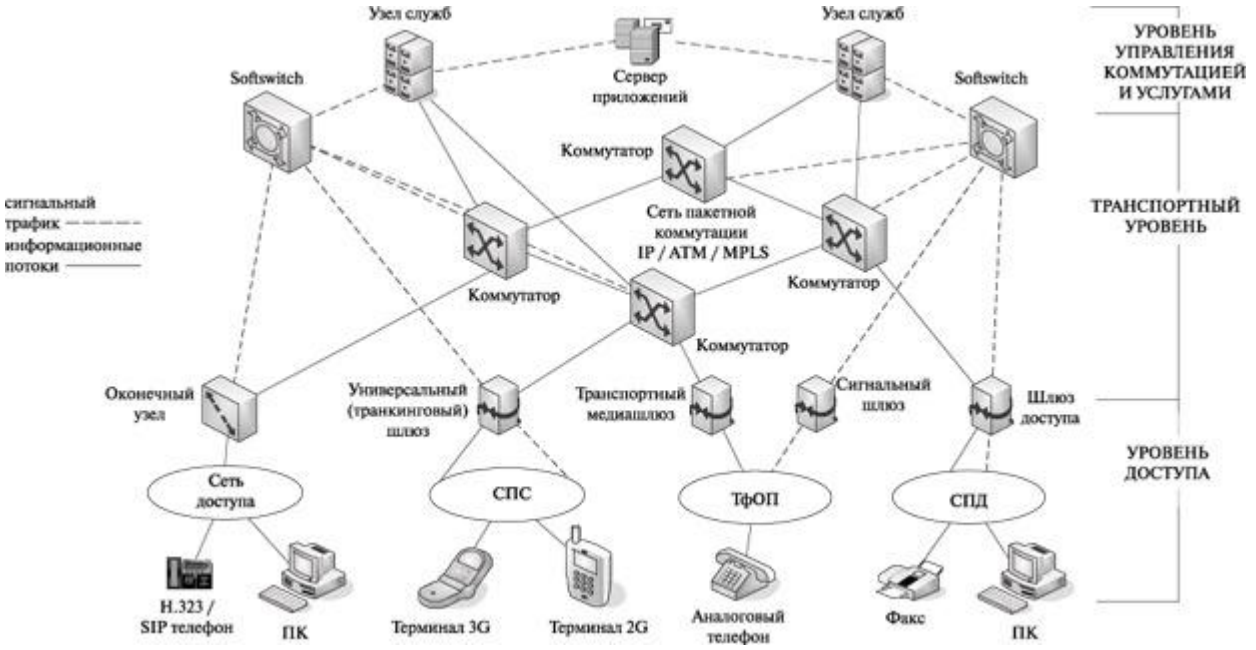


Рис. 3.5. Архитектура сети электросвязи, построенной в соответствии с концепцией ССП

Инфокоммуникационные услуги предполагают взаимодействие поставщиков услуг и операторов связи, которое может обеспечиваться на основе функциональной модели распределённых (региональных) баз данных, реализуемых в соответствии с Рекомендацией МСЭ-Т X.500. Доступ к базам данных организуется с использованием протокола LDAP (Lightweight Directory Access Protocol).

Вышеуказанные базы данных позволяют решить следующие задачи:

- создание абонентских справочников;
- автоматизация взаиморасчётов между операторами связи и поставщиками услуг;
- обеспечение взаимодействия между операторами связи в процессе предоставления услуг ИСС;
- обеспечение взаимодействия терминалов с различными функциональными возможностями на разных концах соединения.

Эти базы данных могут использоваться также поставщиками услуг для организации платных информационно-справочных услуг.

Концепция NGN во многом опирается на технические решения, уже разработанные международными организациями стандартизации. Так, взаимодействие серверов в процессе предоставления услуг предполагается осуществлять на базе протоколов, специфицированных IETF (MEGACO), ETSI (TIPHON), Форумом 3GPP2 и т.д. Для управления услугами будут использованы протоколы H.323, SIP и подходы, применяемые в интеллектуальных сетях связи.

Контрольные вопросы

1. Что является базовым принципом концепции ССП?
2. Основные преимущества NGN
3. Модель базовой сети NGN
4. Что содержит уровень управления услугами?
5. Какой уровень позволяет реализовать специфику услуг и применять одну и ту же программу логики услуг вне зависимости от типа транспортной сети и способа доступа?
6. Какой уровень поддерживает логику управления, которая необходима для обработки и маршрутизации трафика?
7. Какие технологии используются на уровне доступа?
8. Что должен осуществлять программный коммутатор (Softswitch)?
9. Что является задачей транспортного уровня?
10. Какой протокол является основным транспортным протоколом для мультимедийных приложений?

4. ТЕХНОЛОГИИ ДЛЯ ПОСТРОЕНИЯ ТРАНСПОРТНОГО УРОВНЯ (ATM И IP)

4.1. Транспортный уровень

Транспортный уровень сети NGN строится на основе пакетных технологий передачи информации. Основными используемыми технологиями являются ATM и IP. Как правило, в основу транспортного уровня мультисервисной сети ложатся существующие сети ATM или IP. т. е. сеть NGN может создаваться как наложенная на существующие транспортные пакетные сети. Подробно вопрос использования существующих транспортных сетей рассмотрен в гл.2.5 (Семенов А.В. Сети нового поколения. СПб: Наука и техника, 2005 [1]).

Сети, базирующаяся на технологии ATM, имеющей встроенные средства обеспечения качества обслуживания, могут использоваться при создании NGN практически без изменений. Использование в качестве транспортного уровня NGN существующих сетей IP потребует реализации в них дополнительной функции обеспечения качества обслуживания. В случае, если на маршрутизаторе/коммутаторе ATM/IP реализуется функция коммутации под внешним управлением, то в них должна быть реализована функция управления со стороны гибкого коммутатора с реализацией протоколов H.248/MGCP (для IP) или BICC (для ATM).

Типовая структура транспортной сети представлена на рис.4.1. Описание и функциональные требования к элементам транспортного уровня даны в гл.2.1 [1]. Классификация и определения интерфейсов между элементами транспортного уровня, а также принципы построения пакетных транспортных сетей приведены в гл.2.5 [1].

4.2. Построение транспортных пакетных сетей

Транспортная сеть является опорной, поэтому к ней предъявляются высокие требования по обеспечению надежности, производительности и управляемости. В состав транспортной сети NGN могут входить:

- транзитные узлы, выполняющие функции переноса и коммутации:
- оконечные (граничные) узлы, обеспечивающие доступ абонентовк

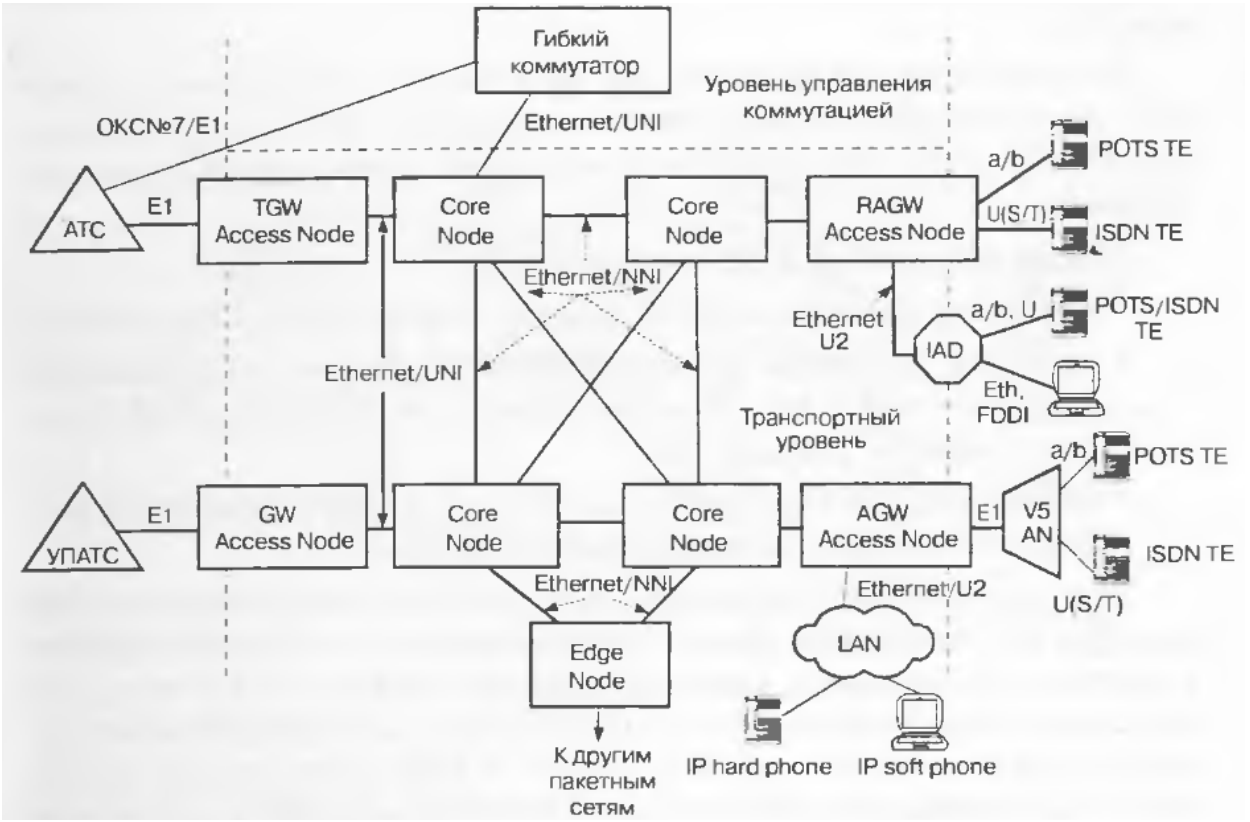


Рис.4.1. Структура транспортного уровня фрагмента NGN

мультисервисной сети:

- контроллеры сигнализации, выполняющие функции обработки информации сигнализации, управления вызовами и соединениями;
- шлюзы, позволяющие осуществить подключение традиционныхсетей связи (ТфОП. СПД. СПС).

Рассмотрим использование различных технологий с точки зрения возможности обеспечения качества передачи разнородного трафика.

4.2.1. Использование технологии ATM для построения транспортного уровня

ATM (Asynchronous Transfer Mode — асинхронный режим передачи) является технологией универсальной транспортной сети, предназначенной для предоставления услуг прозрачной передачи различных типов информации. При этом обеспечивается достаточная пропускная способность для каждого из них и гарантируется своевременная доставка чувствительных к задержкам типов трафика. В основе технологии лежит передача данных в виде ячеек фиксированной длины для любого типа трафика, ск прости передачи и способа кадрирования. Длина ячейки составляет 53 байта, 48 из которых отводится под передачу пользовательской информации, остальные 5 — под заголовок, используемый для адресации, контроля ошибок и управления сетью.

В технологии ATM поддерживается передача трафика четырех видов:

- CBR (Constant Bit Rate — с постоянной битовой скоростью) - синхронный, чувствительный к задержкам;
- VBR (Variable Bit Rate — с переменной битовой скоростью). Разделен на два подкласса: rtVBR — в режиме реального времени (чувствительный к задержкам) и nrtVBR — без использования режима реального времени (задержки допустимы):
- ABR (Available Bit Rate — с доступной битовой скоростью) - трафик приложений, нечувствительных к задержкам. Скорость передачи изменяется в зависимости от нагрузки:
- UBR (Unspecified Bit Rate — с неопределенной битовой скоростью) — трафик, передача которого может вестись без обеспечения каких-либо гарантий производительности.

Основу эталонной модели протокола ATM составляют три уровня архитектуры ATM: физический, уровень ATM и уровень адаптации ATM. соответствующие трем нижним уровням модели OSI (рис.4.2).

	Модель OSI	Модель ATM
3	Сетевой уровень	Уровень адаптации ATM
2	Канальный уровень	Уровень ATM
1	Физический уровень	Физический уровень

Рис.4.2. Сетевые модели ATM и OSI

На физическом уровне осуществляется физическая передача информации по сети ATM. Стандарты ATM для физического уровня описывают, какие кабельные системы должны использоваться в сетях ATM и с какими скоростями может работать ATM при каждом типе кабеля. Наиболее часто используются скорости передачи 155 Мбит/с (кабели «витая пара» категории 5, экранированная «витая пара» типа 1, оптоволоконный кабель) и 622 Мбит, с (оптоволоконный кабель).

Уровень ATM предназначен для пересылки ячеек с физического уровня на уровень адаптации ATM и обратно с генерацией или отделением заголовка ячеек, а также для управления трафиком и установления соединении.

Уровень адаптации ATM (AAL — ATM Adaptation Layer) обеспечивает интерфейс между уровнем ATM и протоколами более высокого уровня. Основной функцией уровня AAL является преобразование форматов данных в соответствии с требованиями различных приложений. Он также обеспечивает синхронизацию, упорядочивание, тактирование и обнаружение, исправление ошибок. В табл.4.1 приведены основные характеристики четырех основных уровней адаптации ATM.

Все протоколы, за исключением AAL 5, добавляют служебную информацию к 48 байтам данных в ячейке ATM. Служебная информация

Таблица 4.1

Основные характеристики четырех основных уровней адаптации АТМ

Уровень адаптации	AAL1	AAL2	AAL5 AAL3/4	
Ориентация на соединение	Ориентированы на соединение			Не ориентированы на соединение
Задержка	Чувствительны к		нечувствительны к задержке	
Скорость	Постоянна	Переменная		
Тип трафика	Голос	Пакетное видео	IP	Независящие от времени данные с переменной

включает в себя специальные команды обработки ячеек, которые используются для обеспечения различных скоростей передачи трафика, в результате чего размер ячейки для передачи пользовательских данных уменьшается.

Уровень AAL1 используется для пересылки аудио- и видеоинформации в режиме реального времени и определяет метод передачи непрерывного сигнала ячейками АТМ.

Уровень AAL2 обеспечивает передачу данных с переменной скоростью в реальном времени. В передаваемые ячейки вместе с данными включается информация синхронизации. Размер полезных данных пользователя составляет 45 байтов.

Уровень AAL3/4 поддерживает передачу информации с переменной скоростью как при ориентированной на соединение, так и при не ориентированной на соединение модели обмена данными. Размер полезной информации составляет 44 байта.

Уровень AAL5 обеспечивает максимальную эффективность передачи данных различных протоколов, в частности, протоколов IP и FR. Размер полезной информации составляет 48 байтов.

Основной транспортной единицей АТМ является виртуальный канал (VC). выделяемый логически. Виртуальный канал АТМ — это соединение между двумя конечными станциями АТМ, которое устанавливается на время их взаимодействия. Виртуальный канал является двунаправленным. Объединение группы виртуальных каналов, следующих на каком-то участке сети в обшем направлении, называется виртуальным путем (VP). Виртуальный путь существует постоянно, независимо от того, установлено ли соединение. Физический тракт передачи может содержать несколько виртуальных путей и каналов.

Различают постоянные и коммутируемые виртуальные соединения. Постоянные соединения являются аналогами традиционных арендованных каналов и трактов. Коммутатор может осуществлять коммутацию виртуальных путей и каналов или только коммутацию виртуальных путей

(кроссовый коммутатор).

Имеются три типа виртуальных каналов:

- постоянные виртуальные каналы (permanent virtual circuit — PVC);
- коммутируемые виртуатьные каналы (switched virtual circuit — SVC);
- интеллектуальные постоянные виртуальные каналы (smart permanent virtual circuits — SPVC).

PVC - это постоянное соединение между двумя конечными станциями, которое устанавливается вручную в процессе конфигурирования сети. PVC включает в себя конечные станции, среду передачи и все коммутаторы, расположенные между конечными станциями. После установки PVC для него резервируется определенная часть полосы пропускания, и двум конечным станциям не требуется устанавливать или сбрасывать соединение.

SVC устанавливается по мере необходимости всякий раз, когда конечная станция пытается передать данные другой конечной станции. Через произвольный промежуток времени SVC сбрасывается. SVC устанавливается динамически. Стандарты передачи сигналов уровня ATM определяют процесс установки, поддержания и сбрасывания соединения, использование конечной станцией при установлении соединения параметров QoS. а также способ управления трафиком.

SPVC - это гибрид PVC и SVC. Подобно PVC. SPVC устанавливается вручную на этапе конфигурирования сети. При этом задаются только конечные станции. Для каждой передачи сеть определяет, через какие коммутаторы будут передаваться ячейки.

Перед установлением соединения конечная станция запрашивает одну из четырех категорий сервиса. Сеть ATM устанавливает соединение, используя соответствующие параметры трафика и QoS для предотвращения перегрузки сети. Установленные соединения не должны превышать предоставленной им полосы пропускания. Если во время соединения полоса пропускания превышается, то ячейки отбрасываются. При этом в соответствии с установленным коэффициентом потерь определяется, какие ячейки можно отбрасывать. Сеть отказывает в установлении соединении, которые не могут поддерживаться.

Для передачи речи через сеть ATM могут использоваться два метода:

- соединение на сервисном уровне. В этом случае ATM рассматривается как мультисервисная сеть, в которой форматы передачитрафика и сигнализации преобразуются в среду ATM;
- соединение на сетевом уровне. В этом случае сеть ATM применяется как эффективная транспортная среда между узлами сети для прозрачной передачи трафика и сигнализации.

В ATM различают следующие типы интерфейсов:

- «пользователь-сеть» (User-to-Network Interface — UNI), определяющий взаимодействие между конечной станцией и коммутатором. Для интерфейса UNI определены скорости передачи 155,520 Мбит с при

использовании коаксиального кабеля (до100Мбит/с). а также 622,080 Мбит/с и 2 4Я8 320 Мбит/с при использовании оптического волокна (до 2 км). Варианты реализации интерфейса UNI определены в Рекомендации МСЭ-Т 1.361, Спецификациях Форума ATM UNI 3.1. а также в Спецификациях Форума ATM UNI 4.0;

- интерфейс «сеть-сеть» (Network-to-Network Interface), определяющий взаимодействие между коммутаторами ATM сети либо между сетями ATM. Функцией интерфейса является сбор, обновление и синхронизация информации о топологии сети ATM и адресах конечных узлов ATVI. Для интерфейса NNI определены скорости передачи 155,520Мбит/с. 622,080Мбит/с и 2 488,320Мбит/с. Варианты реализации интерфейса NNI определены в Рекомендации МСЭ-Т 1.361, Спецификации Форума ATM PNNI версии 1.0. а также в Спецификации Форума ATM B-ICI.

На рис.4.3 приведена схема взаимодействия оконечной станции сети ATM с коммутатором и место интерфейсов ATM в этом взаимодействии. Данные пользователя поступают на уровень адаптации ATM. В соответствии с типом данных какой-либо из четырех протоколов AAL разбивает их на ячейки. Ячейки передаются на уровень ATM. который добавляет к ним информацию, необходимую для маршрутизации. После этого ячейки передаются на физический уровень, разбивающий их на биты и посылающий через среду передачи коммутатору.

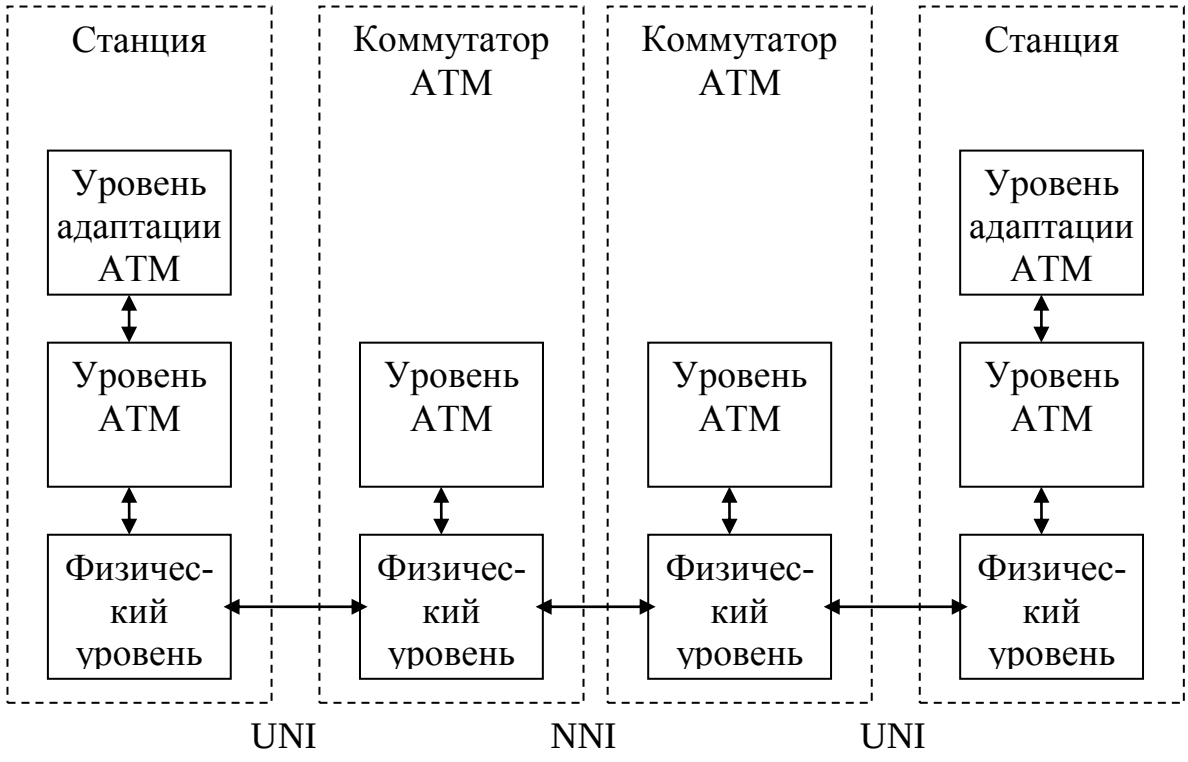


Рис.4.3. Взаимодействие рабочей станции с коммутатором

Ядро ATM-сети строится на основе ATM-коммутаторов. Для организации соединений между узлами сети могут использоваться тракты STM-1 и STM-4 сетей SDH, а также тракты E1 или E3 систем PDH. В качестве оборудования доступа используются ATM мультиплексоры, в функции которых входит концентрация информационных потоков и перенаправление их в ядро сети (примером мультиплексора ATM может служить DSLAM). Для организации доступа пользователей применяются сетевые окончания, содержащие необходимые пользовательские интерфейсы. Пример построения сети ATM приведен на рис.4.4.

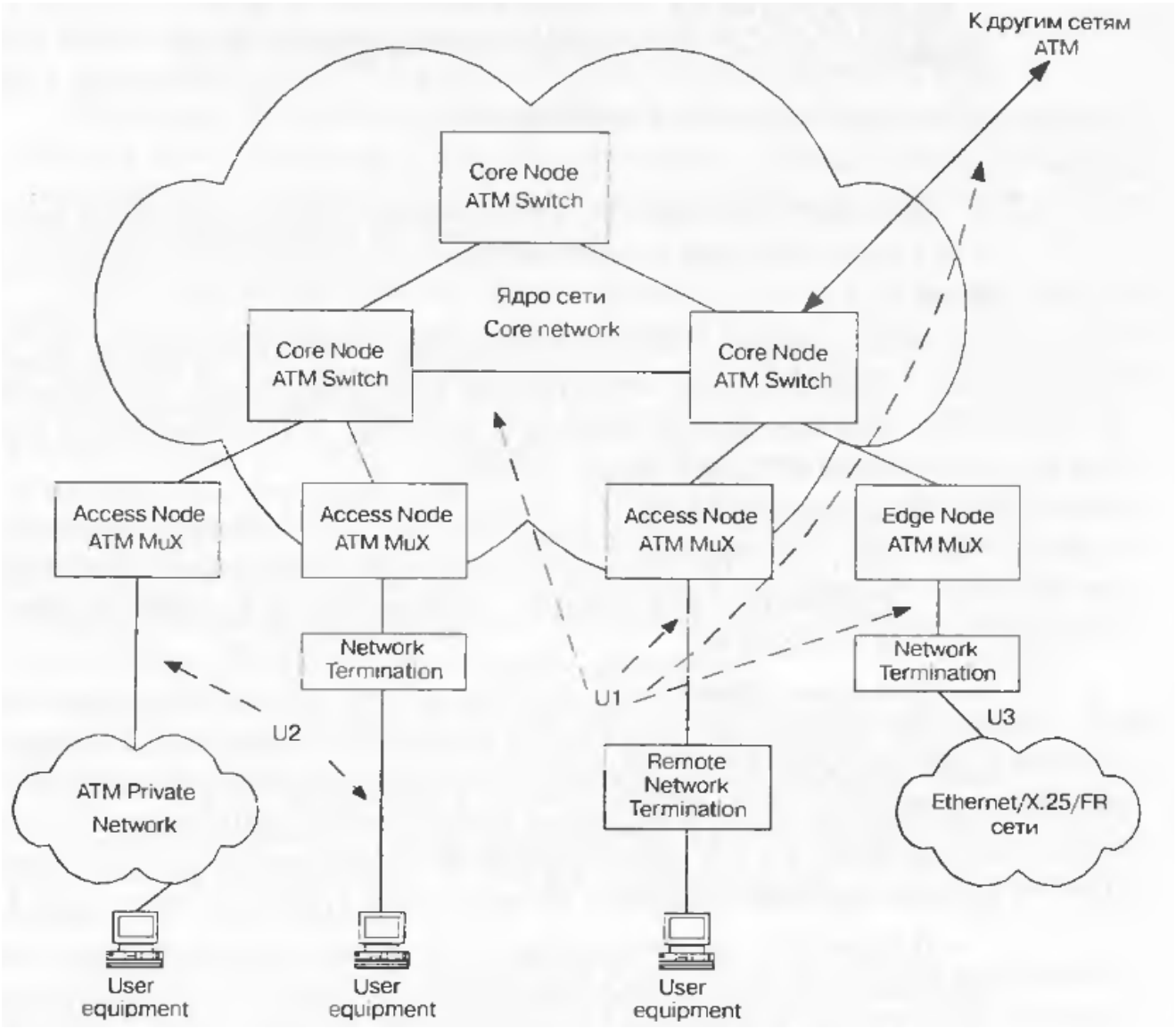


Рис.4.4. Пример построения сети ATM

Взаимодействие узлов сети может осуществляться одним из двух способов (интерфейс U1):

- :в соответствии с требованиями протокола ATM для интерфейса NNI. определенными в Рекомендации МСЭ-Т 1.361. При этом для организации коммутируемых соединений должна использоваться сигнализация B-ISUP

в соответствии с Рекомендациями МСЭ-Т серии Q.27xx;

- в соответствии с требованиями протокола ATM, определенными в Спецификации Форума ATM PNNI версии1.0. При этом для организации коммутируемых соединений должна использоваться сигнатизация. определенная в указанной спецификации.

Подключение абонентов сети ATM должно осуществляться в точках сети, реализующих функции сетевого окончания. Функция сетевого окончания может быть либо реализована в оборудовании оконечного или оконечно-транзитного узла сети ATM. либо вынесена в оборудование. устанавливаемое v абонента.

Сетевое окончание может включать следующие типы интерфейсов для взаимодействия с оконечным оборудованием пользователя (интерфейс U2):

- интерфейс UNI в соответствии с Рекомендацией МСЭ-Т I.361. Для организации коммутируемых соединении должна использоваться сигнализация DSS2 в соответствии с Рекомендациями МСЭ-Т серии Q.29xx:
- интерфейс UNI в соответствии со Спецификациями Форума ATM UNI 3.1. Допускается использование интерфейса UNI Спецификации Форума ATM UNI 4.0.

Для взаимодействия с другими сетями электросвязи (интерфейс U3) сетевое окончание должно поддерживать специализированный интерфейс пользователя, соответствующий стандартному интерфейсу для конкретного протокола передачи информации (например, Ethernet, X.25.I Frame Relay и т. п.). реализующий функцию преобразования формата передаваемой информации и сигнализации в формат протокола ATM.

В частности, оборудование ATM может использоваться для организации постоянных н коммутируемых соединительных линий между узлами ТфОП. В качестве интерфейса физического уровня для взаимодействия оборудования ATM и оборудования ТфОП/ЦСИС могут использоваться каналы E1. Функции преобразования сигнализации должны быть реализованы в соответствующих сетевых окончаниях.

Процесс маршрутизации делится на два этапа: выбор оптимальных маршрутов и непосредственное управление пакетами, осуществляемые раздельно. Выбор маршрутов осуществляется маршрутными серверами в ядре сети, использующими традиционные протоколы маршрутизации (например. OSPF и RIP). Вычисленные маршруты передаются устройствам доступа, поддерживающим распределенную маршрутизацию и осуществляющим непосредственное управление пакетами.

В настоящее время технология ATM более распространена в качестве транспортной технологии, предоставляющей механизмы обеспечения качества передачи на канальном уровне.

4.2.2. Использование технологии IP для построения транспортного уровня

Протокол IP является протоколом сетевого уровня, не ориентированным на соединения и предоставляющим данные для протоколов транспортного уровня TCP (ориентированный на соединения) и UDP (не ориентированный на соединения).

Протокол IP доставляет блоки данных (дейтаграммы) от одного IP-адреса к другому. IP-адрес является уникальным 32-битным идентификатором сетевого интерфейса компьютера. В функции протокола IP входит определение маршрута для каждой дейтаграммы, при необходимости сборка и разборка дейтаграммы на фрагменты, а также отправка источнику дейтаграммы сообщения об ошибке в случае невозможности доставки. Средства контроля корректности данных, подтверждения их доставки, обеспечения правильного порядка следования дейтаграмм, а также функции предварительного установления соединения между компьютерами в IP-протоколе не предусмотрены.

При транспортировке IP-пакетов их порядок может нарушаться. Для обеспечения требуемого качества обслуживания трафика реального времени необходимо сохранение порядка следования пакетов, а также минимизация задержки пакетов и колебаний длительности задержек. Для обеспечения приемлемого голосового потока время задержки должно составлять менее 300-600 мс.

Для реализации механизмов QoS в заголовке IP-пакета предусмотрено поле типа сервиса размером 8 бит (Type of Service — ToS), которое задает характер обработки пакета в процессе его транспортировки.

IP-протокол не подразумевает использования каких-либо определенных протоколов уровня доступа к среде передачи и физическим средам передачи данных. Требования к канальному уровню ограничиваются наличием интерфейса с модулем IP и обеспечением преобразования IP-адреса узла сети, на который передается дейтаграмма, в MAC-адрес. В качестве уровня доступа к среде передачи могут выступать целые протокольные стеки, например. ATM. IPX. X.25 и т.п.

Сеть IP рассматривается как объединение автономных независимых локальных и глобальных сетей, в каждой из которых может использоваться теоретически любая технология канального уровня. Как и в любой сети, в сети IP можно выделить магистральную сеть и сеть доступа. «Границей» магистральной сети являются точки подключения локальных сетей к глобальным. Среди используемых в настоящее время технологий локальных сетей следует выделить следующие:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- Token Ring

- 100VG-ANYLAN
- FDDI/CDDI.

Граничные маршрутизаторы должны поддерживать любое подмножество из перечисленных выше интерфеисов. В табл.4.2 приведены характеристики используемых интерфейсов канального уровня локальных сетей.

Таблица 4.2

Характеристики используемых интерфейсов канального уровня локальных сетей

Технология	Специфи-кация	Среда передачи	Скорость передачи
Ethernet lOBaseT	IEEE 802 3	Неэкранированная витая пара 3 кат	10 Мбит/с
Fast Ethernet 100BaseTX 100BaseFX	IEEE 802.3	Две экранированных витых пары Два оптоволоконных кабеля	100 Мбит/с
Gigabit Ethernet	IEEE 802 3z	Экранированная или неэкранированная витая пара или	1 Гбит/с
Token Ring	IEEE 802 5	Экоанированная или неэкранированная витая пара	4/16 Мбит/с
100VG-ANYLAN	IEEE 802. 12	Четыре неэкранированные витые пары или оптоволоконный кабель	100 Мбит/с
FDDI/CDDI	ISO 93 14	Оптоволокно Экранированная или неэкранированная витая пара	100 Мбит/с

Для соединения сетей используется один из протоколов маршрутизации OSPF или BGP. Архитектура IP-сети приведена на рис.4.5. В настоящее время существуют два основных способа создания магистральных IP-сетей: с помощью IP-маршрутизаторов, соединенных каналами «точка-точка», либо на базе транспортной сети ATM, поверх которой работают IP-маршрутизаторы. В первом варианте в качестве транспорта для передачи IP-пакетов может использоваться один из протоколов канального уровня (SLIP или PPP), во втором — ячейки ATM AAL5. В последнем случае необходимо использование дополнительных управляющих функций для контроля совместной работы IP и ATM.

Структура доступа к IP-сети приведена на рис.4.6. Сервер доступа используется для идентификации, аутентификации и учета трафика пользователей, а также для назначения временных IP-адресов и маршрутизации.

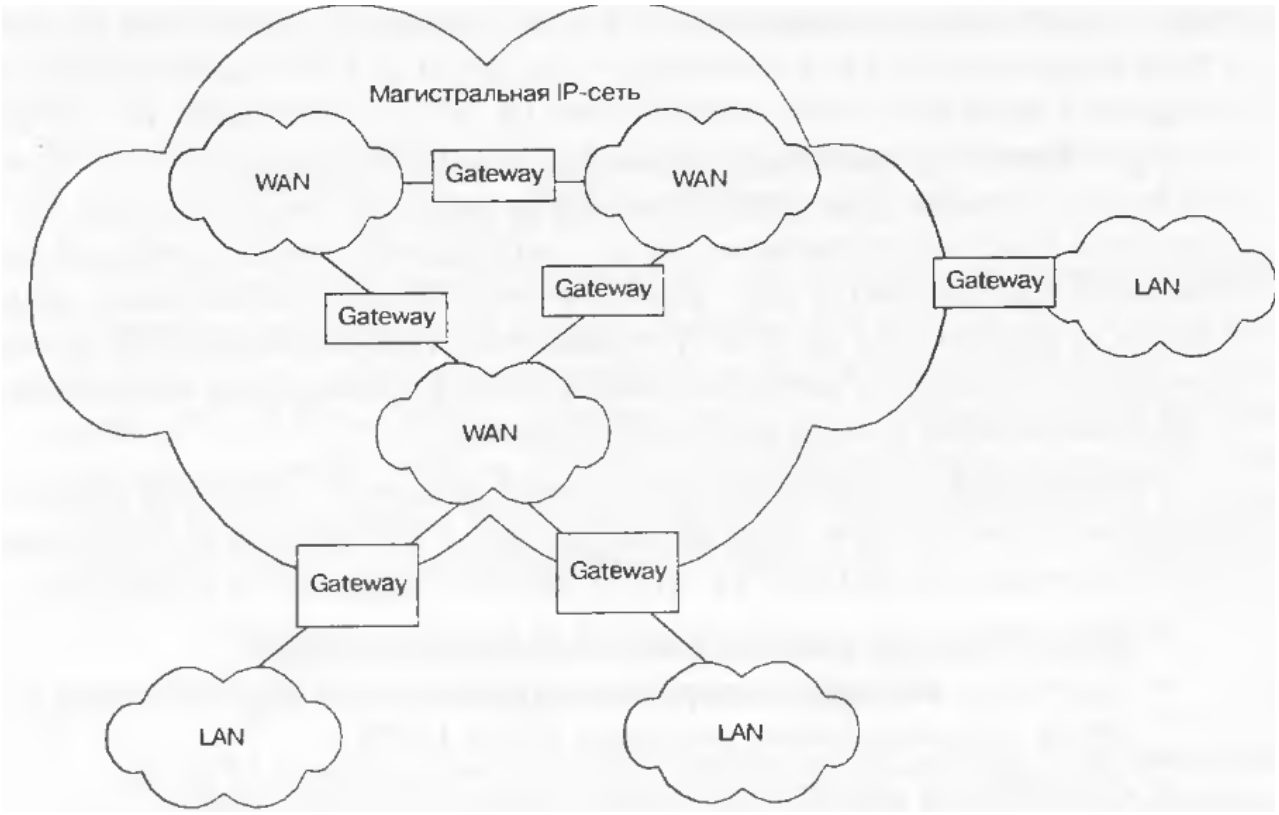


Рис.4.5 Архитектура сети IP

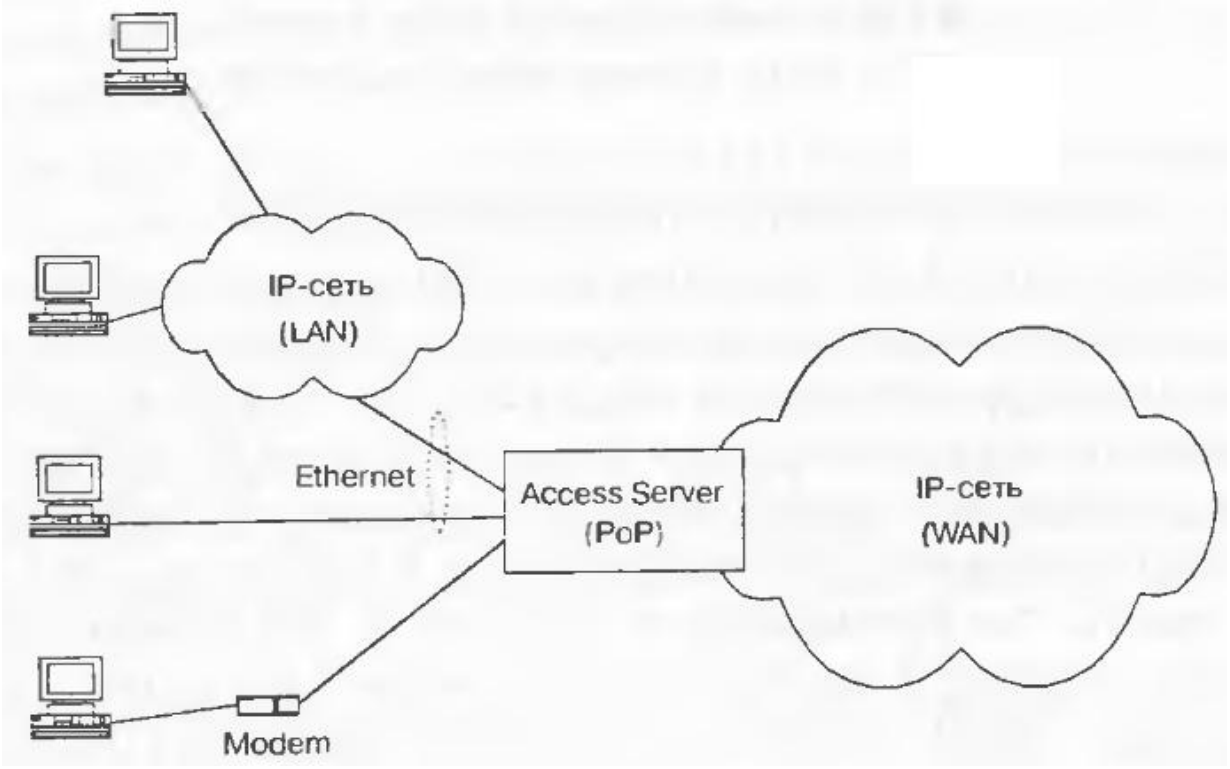


рис.4.6.Структура доступа к IP-сети

IP-протокол изначально не предназначался для передачи голоса, однако его широкая распространенность, возможность наложения практически на любую транспортную сеть, а также высокая степень совместимости решений различных поставщиков привели к тому, что IP-сети стали использоваться как универсальная среда для передачи всех видов трафика. Основным недостатком сетей на основе протокола IP является отсутствие механизмов, которые бы обеспечивали передачу трафика реального времени. Обеспечение качества передачи чувствительного к задержке трафика достигается путем реализации соответствующих механизмов на канальном или транспортном уровне. Реализация услуг мультисервисной сети на базе IP-технологии требует внедрения дополнительной поддержки качества обслуживания, повышения надежности и рационализации использования ресурсов.
Управление качеством обслуживания на уровне IP-протокола реализуется преимущественно в корпоративных сетях, где администратор может контролировать все устройства сети. К методам управления относятся:

- выделение отдельных каналов для передачи голоса:
- настройка маршрутизатора на первоочередное обслуживание па кетов с определенным номером порта UDP;
- ограничение максимально допустимого размера пакета.

4.2.3. Сравнение ATM и IP

ATM - сеть коммутации ячеек, IP- сеть коммутации пакетов
Коммутация ячеек в ATM является более простым и более однородным процессом по сравнению с традиционной маршрутизацией, используемой в сетях IP. Поскольку ячейки ATM всегда имеют одну и ту же длину, значительно меньшую длины кадра IP. они требуют меньшей буферизации. Кроме того, они предсказуемы, поскольку их заголовки всегда находятся на одном и том же месте. В сетях IP маршрутизаторы должны использовать программное обеспечение для правильной обработки ряда изменений в потоке передачи, в частности, для измерения длины пакета, для фрагментирования пакета, для передачи пакетов в правильном порядке и для пересборкн пакетов. В результате коммутатор ATM автоматически обнаруживает заголовки ячеек, и их обработка происходит быстрее.
С другой стороны, поскольку длина пакета IP больше длины ячейки ATM. процент передаваемой полезной нагрузки в сети ATM оказывается значительно меньше, чем в IP. что снижает эффективность работы сети.

ATM - сеть с установлением соединения, IP- без установления соединения
Сети с установлением соединения также могут гарантировать определенное качество обслуживания, поэтому они могут использоваться для передачи различных видов трафика — звука, видео и данных — через одни и те же

коммутаторы. Кроме того, сети с установлением соединения могут лучше управлять сетевым трафиком и предотвращать перегрузку сети, поскольку коммутаторы могут просто сбрасывать те соединения, которые они не способны поддерживать.

Возможность передачи данных разных типов по одному соединению
В АТМ все типы информации могут надежно передаваться через единое сетевое подключение. АТМ использует концепцию категории обслуживания между конечными пользователями АТМ и коммутаторами для того, чтобы получить надежную службу передачи данных.
В сети IP для обеспечения качественной передачи различных типов информации, а также для обеспечения различных категорий обслуживания необходимо использовать дополнительные механизмы на более высоких уровнях..

Возможности масштабирования сети
Теоретически расширение IP-сети ограничено разрядностью IP-адреса. Максимальная скорость магистрали при использовании технологии Gigabit Ethernet составляет 10 Гбит с. На практике обеспечение качества обслуживания в сети IP требует создания управляемой сети с определенной протскной способностью и производительностью маршрхтпзаторов, что накладывает ограничения на масштабируемость.
Существующие стандарты АТМ предусматривают скорости передачи до 2.4 Гбит/с. АТМ поддерживает единый способ передачи данных, позволяющий связывать сети любых размеров и масштабировать их в будущем. Масштабируемость сетей АТМ ограничивается производительностью коммутаторов и возможностью управления сетью.

Распространенность сетей
Развертывание IP-сетей осуществляется, прежде всего, для передачи данных (а не мультисервисного трафика). Благодаря появлению сети Интернет технология IP в настоящее время — наиболее распространенная и быстроразвиваюшаяся технология сетей передачи данных. Это является основной причиной стремления разработчиков создать на базе IP-протокола мультисервнсную сеть, используя для этого уже существующие сети.
Технология АТМ специально создавалась для того, чтобы служить основой широкополосной мультисервпсной сети: ее распространение напрямую связано со стремлением создать подобные сети. Поскольку в настоящее время рынок широкополосных услуг развит в меньшей степени, чем рынок услуг ПД. сети на основе АТМ распространены не столь широко.

Стоимость сети
Цены на оборудование АТМ существенно выше цен на оборудование IP. В то же время качество услуг, предоставляемых АТМ-сетью, также существенно

выше аналогичных показателей IP-сетей. Применение же на сети IP разнообразных средств повышения качества сервиса приводит к существенному удорожанию строительства и эксплуатации сети.
Аналогичные рассуждения касаются и сложности протоколов и управления сетью. Протоколы маршрутизации ATM значительно сложнее, чем в IP. однако внедрение механизмов резервирования полосы пропускания, многоуровневой коммутации, дифференцированного обслуживания приводит к значительному усложнению стека протоколов IP-сети, и его простота перестает быть достоинством.

Отсюда следует сделать вывод, что у каждой технологии существует своя сфера применения, в которой ее качества используются наилучшим образом. Кроме того, возможно, что наилучший результат может дать совместное применение ATM и IP. сочетающее достоинства этих технологий.

4.3. Технологии передачи трафика IP по сетям ATM

В разное время было разработано несколько технологий передачи IP поверх ATM: классический IP поверх ATM (RFC 2225). мультипрото-кольная коммутация поверх ATM (MPOA), мультипротокольная коммутация меток MPLS. Во всех перечисленных технологиях предполагается передача пакета IP в поле блока данных ячеек AAL5. Данный метод инкапсуляции описан в документе IETF RFC 2684 «Мультипротокольная инкапсуляция поверх ATM AAL5». RFC 2684 определяет два метода, применяемых для передачи данных коммутируемых и маршрутизируемых протоколов.

Использование одного виртуального соединения несколькими протоколами. Инкапсуляция осуществляется с использованием заголовка уровня управления звеном данных LLC и заголовка протокола доступа подсети SNAP. Таким образом реализуется свойство самондентификаиии протокола. Применяется при необходимостипередачи информации различных протоколов в одном виртуальном канале. При этом в поле полезной нагрузки необходимо передавать информацию о передаваемом протоколе. Инкапсуляция LLC'SNAP применяется в случаях использования постоянных виртуальных каналов или в случае, когда установка отдельных виртуальных каналов для каждого соединения является нерентабельной.

Выделение отдельного соединения виртуального канала каждому протоколу. Инкапсуляция осуществляется без использования заголовков уровня LLC и SNAP. В данном методе отсутствует необходимость помещения дополнительной информации о передаваемом протоколе в поле полезной нагрузки, что приводит к уменьшению требуемой полосы пропускания и загрузки процессора коммутатора. Выбор данного метода оправдан в тех случаях, когда установка виртуальных каналов происходит быстро и экономично (в небольших сетях). Данный метод инкапсуляции применяется для коммутируемых соединений ATM.

Выбор способа инкапсуляции определяется способом мультиплексирования и может быть реализован при конфигурации (для постоянных соединений) или посредством процедур сигнализации B-ISDN (для коммутируемых соединений).

4.3.1. Classical IP over ATM

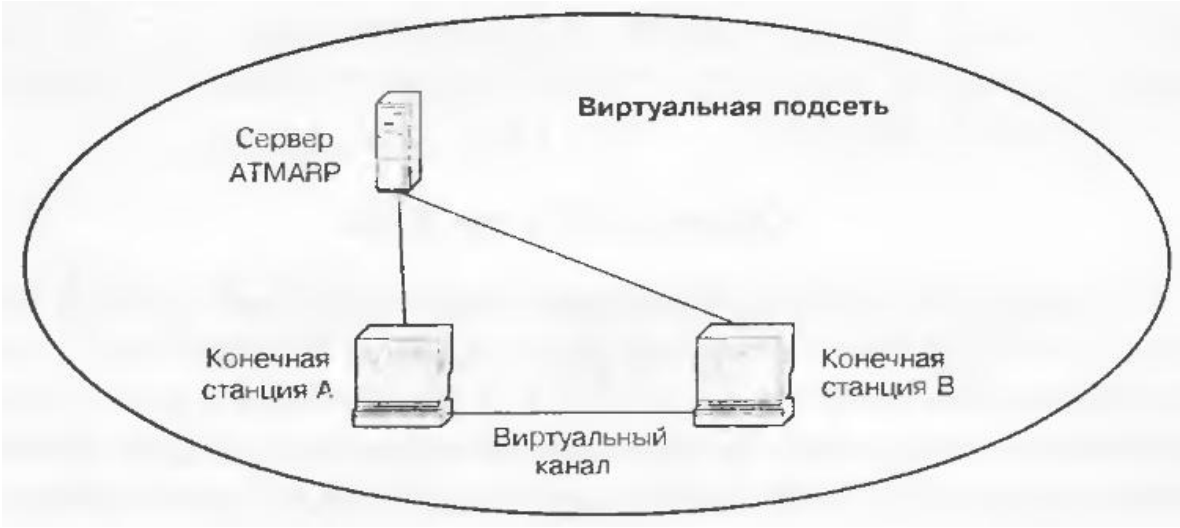
Технология регламентируется документом IETF RFC 2225. описывающим как инкапсуляцию IP-трафика в ячейки ATM на уровне AAL5, так и функции преобразования адресов для постоянных и коммутируемых виртуальных соединений. При реализации данного метода обязательно должна поддерживаться инкапсуляция LLC/SNAP. Спецификация не указывает параметры трафика, качества обслуживания и требуемую категорию услуг CBR. rtVBR. nrtVBR или UBR.

Данная технология предназначена для поддержки протокола IP в одной логической подсети (Logical IP Subnet. LIS) сети ATM. Логическая подсеть представляет собой группу устройств, подключенных к одной сети ATM и использующих единый номер сети/подсети и маску подсети.

В качестве протокола распознавания адреса используются протоколы распознавания адресов ATM ATMARP и InATMARP (инверсный ATMARP). Протокол ATMARP базируется на протоколе ARP. но включает ряд дополнений, необходимых для работы в нешироковещательной сети. Каждая LIS имеет один сервер ATMARP. Основная задача сервера заключается в управлении специальной таблицей, записи которой содержат пары соответствующих IP- и ATM-адресов устройств. Каждое устройство (клиент LIS) в логической подсети настраивается на уникальный ATM-адрес этого сервера.

У каждой конечной станции есть адрес ATMARP-сервера. В какой-то момент клиент посылает ему запрос, и в ответ сервер, послав свой запрос, узнает его IP- и ATM-адреса и добавляет их в свою таблицу, после чего обрабатывается запрос клиента. (В отличие от стандартного ARP. в случае, если адрес не найден, посылается явный отрицательный ответ.) Затем конечная станция (A), получив ATM адрес соседа (конечной станции B), по логической сети устанавливает с ним коммутируемое вирту-атьное соединение и передает данные. Схема взаимодействия узлов по протоколу Classical IP oxer ATM приведена на рис.4.7.

Classical IP over ATM имеет ряд недостатков. Поскольку серверу ATMARP доступна только одна IP-подсеть, узлы IP могут напрямую взаимодействовать только с узлами IP. расположенными в той же подсети. Чтобы посылать пакеты узлу (P. находящемуся в другой виртуальной подсети, передающий узел IP должен направлять их через маршрутизатор. Передающий узел IP использует для соединения с маршрутизатором один



Рмс.4.7. Схема работы протокола Classical IP over ATM

виртуальным канал, а маршрутизатор применяет для соединения с узлом IP. являющимся адресатом, другой виртуальный канал. В этой цепи маршрутизаторы создают «узкое место», поскольку, как правило, работают медленнее коммутаторов. Кроме того. Classical IP over ATM может маршрутизировать только IP-пакеты. Он не решает проблем задержек и перегрузки сети, поскольку не может использовать преимущества качества сервиса сетей ATM. И. наконец. Classical IP over ATM не поддерживает многоадресную рассылку.

Основным достоинством данного стандарта является гибкая конфигурация сети благодаря возможности объединения в одну виртуальную подсеть конечных станций из физически независимых локальных сетей.

4.3.2. MPOA

На основе технологи LANE ATM Forum была разработана технология Multiprotocol over ATM - MPOA (AF-MPOA-0114.000). позволяющая более эффективно работать коммутаторам 3-го уровня различных протоколов (в том числе IP) через ATM. MPOA дает возможность маршрутизировать протоколы типа IP из традиционных ЛВС по коммутируемой ATM-магистрали. Подход MPOA в основном заключается в разделении традиционной роли маршрутизатора на две функции, одна из которых обслуживает непосредственную связь с пользовательскими устройствами, а другая отвечает за сетевой сервис, такой, как определение маршрута. MPOA отделяет пересылку пакетов от других функций маршрутизатора, определяя для пакетов кратчайшие пути, что существенно ускоряет IP-трафик в сети ATM. MPOA состоит из следующих компонентов:

– серверов маршрутизации (Route Servers), которые также называют

серверами MPOA. Они поддерживают таблицы маршрутизации и вычисляют маршруты для оконечных устройств, а также взаимодействуют с традиционными маршрутизаторами и другими серверами маршрутизации. Серверы маршрутизации не обязательно выполнены в виде единого устройства, их функции могут встраиваться в существующие маршрутизаторы и коммутаторы;

- оконечных устройств (Edge Devices), иначе называемых клиентами MPOA. Ими могут служить интеллектуальные коммутаторы, которые пересылают пакеты и ячейки между ЛВС и АТМ. Или сетевые интерфейсные платы, передающие пакеты и ячейки между подключенными к АТМ устройствами и сетями АТМ.
- Вместе серверы маршрутизации и оконечные устройства действуют как распределенные маршрутизаторы: серверы маршрутизации определяют, куда необходимо посылать пакеты, а оконечные устройства их передают.

Когда конечной станции в ЛВС необходимо связаться с подключенным к АТМ устройством, она посылает пакет клиенту MPOA (оконечному устройству), которое запрашивает соответствующий АТМ-адрес у сервера маршрутизации. Если сервер маршрутизации знает АТМ-адрес, то просто выдает запрошенную информацию: в противном случае для определения этого адреса он может, используя один из протоколов маршрутизации, связаться с другими маршрутизаторами — как с традиционными, так и с остальными серверами маршрутизации. Узнав АТМ-адрес, оконечное устройство устанавливает виртуальный канал с соответствующей конечной станцией получателя. На рис.4.8 приведена схема взаимодействия устройств MPOA.

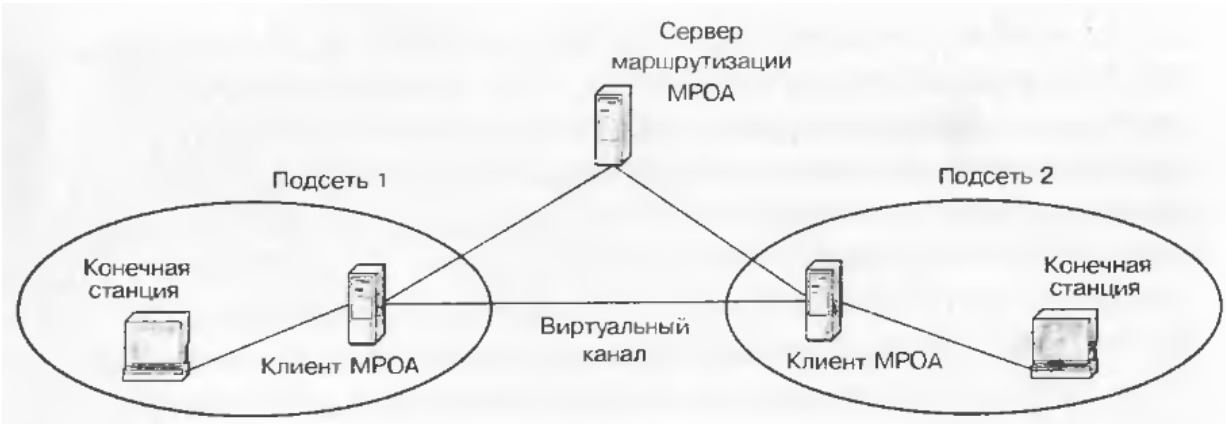


Рис.4.8. Схема работы MPOA

Стандарты MPOA рассчитаны на максимальное использование преимуществ АТМ. в том числе на возможность динамического изменения полосы пропускания сети с использованием прямых коммутируемых виртуальных каналов и гарантированного качества обслуживания.

Поскольку MPOA — это технология сетевого уровня, она имеет доступ к информации сетевого уровня, такой, как характеристики трафика и

параметры качества сервиса ATM. При установлении соединения оконечное устройство может использовать эту информацию для определения оптимального маршрута к конечной станции адресата в зависимости от уровня QoS. запрашиваемого передающей конечной станцией. Кроме того. MPOA предоставляет дополнительные возможности маршрутизации. С помощью MPOA можно осуществлять маршрутизацию между традиционными ЛВС. соединенными ATM-магистралью, создавая таким образом высокоскоростное межсетевое соединение без «узких мест» в виде традиционных маршрутизаторов. Можно также использовать маршрутизацию типа «one-hop» пли «hop-by-hop» для оптимизации коротких и длинных передач.

MPOA позволяет использовать разработанные для [P механизмы. обеспечивающие гарантированное качество услуг, такие как RSVP. в базовой коммутирующей структуре ATM. Технология MPOA позволяет объединить существующие подсети с магистралями ATM без назначения новых адресов IP.

Контрольные вопросы

1. Что является задачей транспортного уровня?
2. Какой протокол является основным транспортным протоколом для мультимедийных приложений?
3. Основные достоинства и недостатки транспортной технологии IP
4. К какому уровню принадлежит протокол IP?
5. Механизм работы протокола UDP
6. Недостатки протокола TCP при передаче мультимедийного трафика, примение протоколов RTP и RTCP
7. Какие уровни составляют сетевую модель ATM?
8. Принцип передачи данных в технологии ATM
9. Что входит в транспортный адрес сетей с маршрутизацией пакетов IP
10. Из каких компонентов состоит MPOA?

5. ОСНОВНЫЕ ПРОТОКОЛЫ, ИСПОЛЬЗУЕМЫЕ В СЕТЯХ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

5.1. Мультипротокольная модель NGN

Softswitch – это устройство управления в сетях следующего поколения. В первую очередь Softswitch управляет обслуживанием вызовов, т.е. установлением и разрушением соединений. Также Softswitch осуществляет координацию обмена сигнальными сообщениями между различными сетями, иначе говоря, Softswitch координирует действия, обеспечивающие соединение с логическими объектами в разных сетях и преобразует информацию в сообщениях таким образом, чтобы они были поняты на обеих сторонах разнородных сетей.

Основные типы сигнализации, которые использует Softswitch:

- сигнализация для управления соединениями;
- сигнализация для взаимодействия различных Softswitch между собой;
- сигнализация для управления транспортными шлюзами.

Основными протоколами сигнализации для управления соединениями

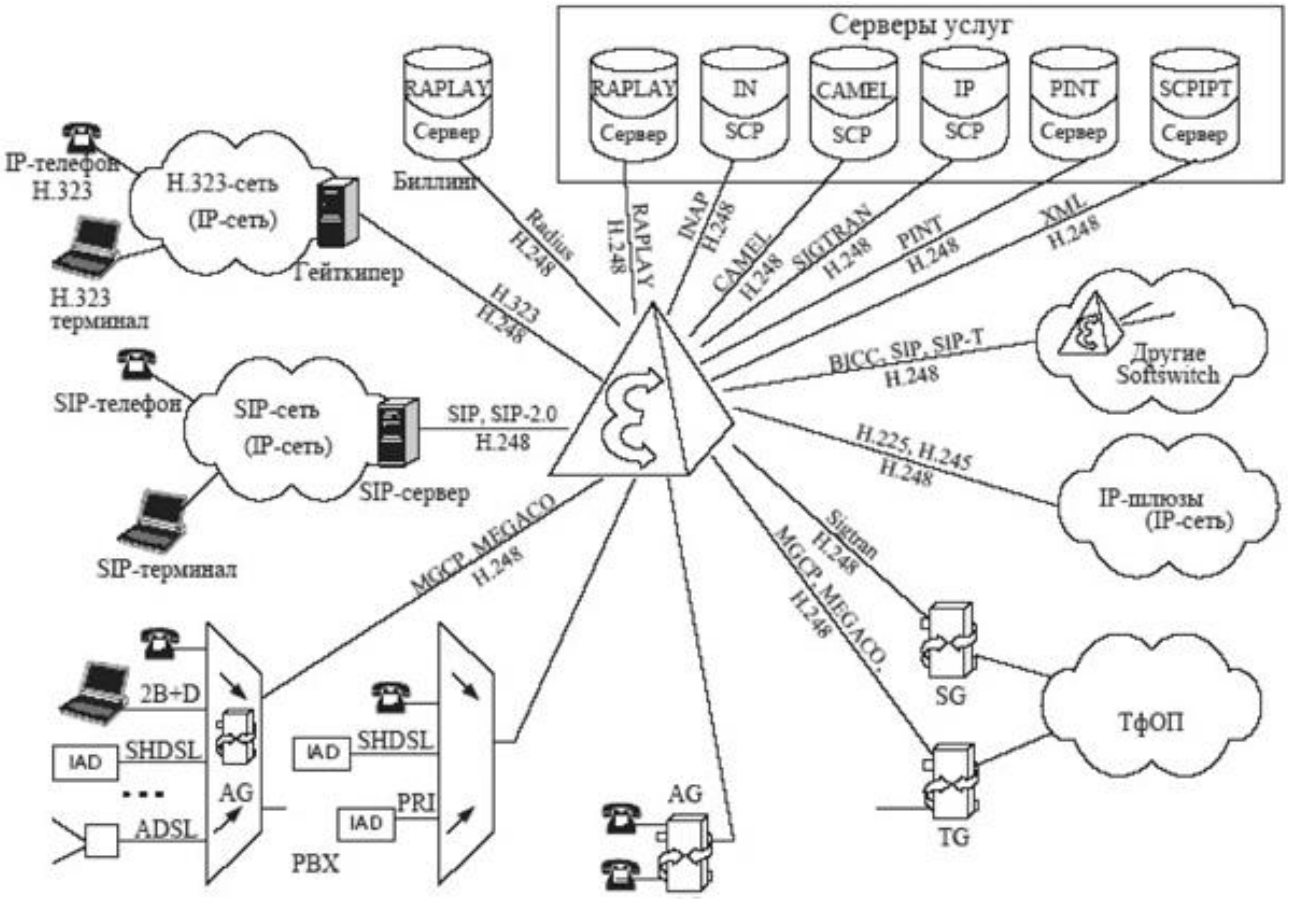


Рис. 5.1. Взаимодействие Softswitch с остальным оборудованием

сегодня являются SIP, ОКС-7, H.323. Также опционально используются:

- абонентская сигнализация E-DDS-1 первичного доступа ЦСИС (цифровая сеть с интеграцией служб, ISDN);
- протокол абонентского доступа через интерфейс V5;
- российская версия сигнализаций R1,R2 – R 1.5.

Основными протоколами сигнализации управления транспортными шлюзами являются MGCP и MEGACO/H.248, а основными протоколами сигнализации взаимодействия между Softswitch — SIP-T и BICC (рис. 5.1).

Характерные для IP-сетей временные задержки и вариация задержки пакетов (джиттер) могут серьезно исказить информацию, чувствительную к задержке, например речь и видеоинформацию, сделав ее абсолютно непригодной для восприятия. Вариация задержки (джиттер) пакетов гораздо сильнее влияет на субъективную оценку качества передачи, чем абсолютное значение задержки.

Протокол RTP позволяет компенсировать негативное влияние джиттера на качество речевой и видеоинформации, но в то же время он не имеет собственных механизмов, гарантирующих своевременную доставку пакетов или другие параметры качества услуг, – это осуществляют нижележащие протоколы. Он даже не обеспечивает все те функции, которые обычно

предоставляют транспортные протоколы, в частности функции исправления ошибок и управления потоком. Обычно протокол RTP базируется на протоколе UDP и использует его функции, но может работать и поверх других транспортных протоколов.

Протокол TCP плохо подходит для передачи чувствительной к задержкам информации. Во-первых, это алгоритм надежной доставки пакетов. Пока отправитель повторно передаст пропавший пакет, получатель будет ждать, результатом чего может быть недопустимое увеличение задержки. Во-вторых, алгоритм управления при перегрузке в протоколе TCP не оптимален для передачи речи и видеоинформации. При обнаружении потерь пакетов протокол TCP уменьшает размер окна, а затем будет его медленно увеличивать, когда как разумнее было бы изменить метод кодирования или размер видеоизображения.

Протокол RTP предусматривает индикацию типа полезной нагрузки и порядкового номера пакета в потоке, а также применение временных меток. Отправитель помечает каждый RTP-пакет временной меткой, получатель извлекает ее и вычисляет суммарную задержку. Разница в задержке разных пакетов позволяет определить джиттер и смягчить его влияние – все пакеты будут выдаваться приложению с одинаковой задержкой.

Доставка RTP-пакетов контролируется специальным протоколом RTCP (Real Time Control Protocol).

Основной функцией протокола RTCP является организация обратной связи приемника с отправителем информации для отчета о качестве получаемых данных. Протокол RTCP передает сведения (как от приемника, так и от отправителя) о числе переданных и потерянных пакетов, значении джиттера, задержке и т.д. Эта информация может быть использована отправителем для изменения параметров передачи, например для

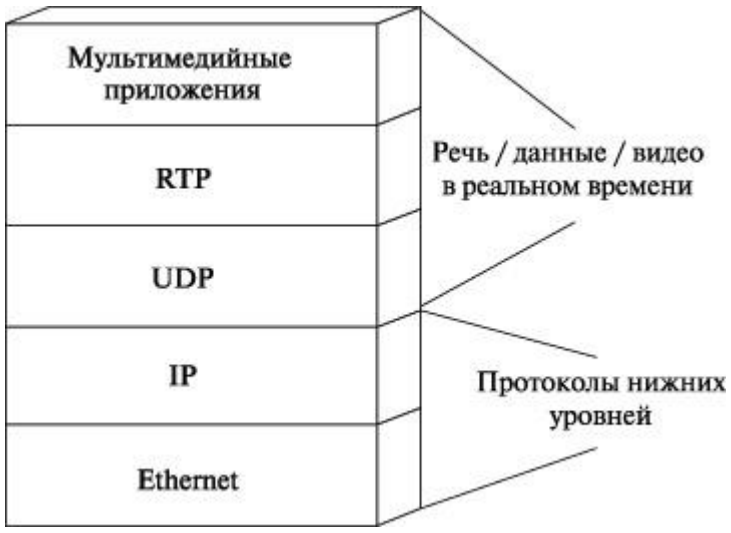


Рис. 5.2. Уровни протоколов RTP/UDP/IP

уменьшения коэффициента сжатия информации с целью улучшения качества

ее передачи.

Протокол передачи пользовательских дейтаграмм – User Datagram Protocol (UDP) – обеспечивает негарантированную доставку данных, т.е. не требует подтверждения их получения; кроме того, данный протокол не требует установления соединения между источником и приемником информации.

5.2. Протоколы RTP и RTCP

Приложения, обеспечивающие передачу речевой и видеоинформации, используют сервис транспортного уровня без установления соединений (например, UDP). При этом каждое приложение может обеспечивать формирование полезной нагрузки пакетов специфическим образом, включая необходимые для функционирования поля и данные. Однако, данные разной природы (речь, видео) имеют общие особенности, которые требуют обеспечения вполне определенной функциональности при их передаче по сети. Это позволяет сформировать некий общий транспортный уровень, объединяющий функции, общие для потоковых данных разной природы, и используемый всеми соответствующими приложениями, придав протоколу этого уровня статус стандарта. Комитетом IETF был разработан протокол транспортировки информации в реальном времени - Realtime Transport Protocol (RTP), который стал базисом практически для всех приложений, связанных с интерактивной передачей речевой и видеоинформации по сети с маршрутизацией пакетов.

Характерные для IP-сетей временные задержки и вариация задержки пакетов (джиттер) могут серьезно исказить информацию, чувствительную к задержке, например, речь и видеоинформацию, сделав ее абсолютно непригодной для восприятия. Отметим, что вариация задержки пакетов гораздо сильнее влияет на субъективную оценку качества передачи, чем абсолютное значение задержки.

Уже длительное время ведется работа по созданию методов уменьшения джиттера и задержек. Именно протокол RTP позволяет компенсировать негативное влияние джиттера на качество речевой и видеоинформации. В то же время, он не имеет собственных механизмов, гарантирующих своевременную доставку пакетов или другие параметры качества услуг, -это осуществляют нижележащие протоколы. Он даже не обеспечивает все те функции, которые обычно предоставляют транспортные протоколы, в частности функции исправления ошибок и управления потоком. Обычно протокол RTP базируется на протоколе UDP и использует его функции, но может работать и поверх других транспортных протоколов.

Существует несколько серьезных причин, по которым транспортный протокол TCP плохо подходит для передачи чувствительной к задержкам информации. Во-первых, это алгоритм надежной доставки пакетов. Пока

отправитель повторно передаст пропавший пакет, получатель будет ждать, результатом чего может быть недопустимое увеличение задержки. Во-вторых, алгоритм управления при перегрузке в протоколе TCP далеко не оптимален для передачи речи и видеоинформации. При обнаружении потерь пакетов протокол TCP уменьшает размер окна, а затем будет его медленно увеличивать. Однако передача речевой и видеоинформации осуществляется на вполне определенных, фиксированных скоростях, которые нельзя мгновенно уменьшить, не ухудшив качество предоставляемых услуг. Правильной реакцией на перегрузку для информационных потоков этих типов было бы изменение метода кодирования, частоты видеокадров или размера видеоизображения.

Протокол RTP предусматривает индикацию типа полезной нагрузки и порядкового номера пакета в потоке, а также применение временных меток. Отправитель помечает каждый RTP-пакет временной меткой, получатель извлекает ее и вычисляет суммарную задержку. Разница в задержке разных пакетов позволяет определить джиттер и смягчить его влияние - все пакеты будут выдаваться приложению с одинаковой задержкой.

Главная особенность RTP - это вычисление средней задержки некоторого набора принятых пакетов и выдача их пользовательскому приложению с постоянной задержкой, равной этому среднему значению. Однако следует иметь в виду, что временная метка RTP соответствует моменту кодирования первого дискретного сигнала пакета. Поэтому, если RTP-пакет, например, с видеоинформацией, разбивается на блоки данных нижележащего уровня, то временная метка уже не будет соответствовать истинному времени их передачи, поскольку они перед передачей могут быть установлены в очередь.

На рис.5.3 представлен основной заголовок RTP-пакета, содержащий ряд полей, которые идентифицируют такие элементы, как формат пакета, порядковый номер, источник информации, границы и тип полезной нагрузки.

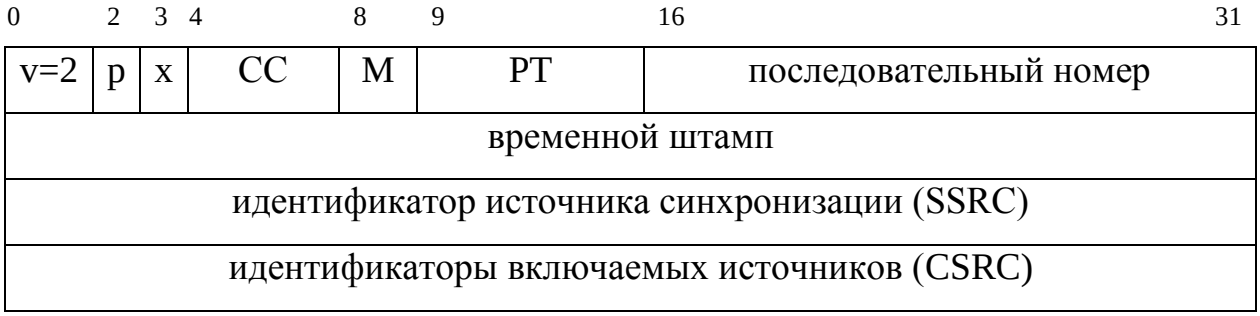


Рис.5.3. Основной заголовок RTP-пакета

V (2 бита) - поле версии протокола. Текущая версия протокола -вторая.

P (1 бит) - поле заполнения. Сигнализирует о наличии заполнения в конце поля полезной нагрузки. Заполнение применяется, когда приложение требует, чтобы размер полезной нагрузки был кратен, например, 32 битам.

X (1 бит) - поле расширения заголовка. Служит для индикации того, что за основным заголовком следует дополнительный заголовок, используемый в экспериментальных расширениях протокола RTP.

CC (4 бита) - поле отправителей. Содержит идентификаторы отправителей, чьи данные находятся в пакете, причем сами идентификаторы следуют за основным заголовком.

M (1 бит) - поле маркера. Обычно используется для указания границ потока данных. Смысл бита маркера зависит от типа полезной нагрузки. В случае передачи видеоинформации он определяет конец кадра. При передаче речевой информации маркер указывает начало периода активности после периода молчания.

PT (7 битов) - поле типа полезной нагрузки. Идентифицирует тип полезной нагрузки и формат данных, включая сжатие и шифрование. В стационарном состоянии отправитель использует только один тип полезной нагрузки в течение сеанса, но он может его изменить в ответ на изменение условий, если об этом сигнализирует протокол управления транспортировкой информации в реальном времени (Real-Time Transport Control Protocol).

Порядковый номер пакета (Sequence Number, 16 битов). Каждый источник начинает нумеровать пакеты с произвольного номера, увеличиваемого затем на единицу с каждым переданным пакетом RTP.

Это позволяет обнаруживать потери пакетов и определять порядок пакетов с одинаковым временным штампом. Несколько последовательных пакетов могут иметь один и тот же штамп, если логически они порождены в один и тот же момент, как, например, пакеты, принадлежащие одному и тому же видеокадру.

Временной штамп (Timestamp, 32 бита). Момент времени, в который был создан первый октет данных полезной нагрузки. Единицы, в которых время указывается в этом поле, зависят от типа полезной нагрузки. Значение определяется по локальным часам отправителя.

Идентификатор SSRC (Synchronization Source Identifier, 32 бита) -поле идентификатора источника синхронизации. Псевдослучайное число, которое уникальным образом идентифицирует источник в течение сеанса и не зависит от сетевого адреса. Это число играет важную роль при обработке порции данных, поступившей от одного источника.

Идентификатор CSRC (Contributing Source Identifier, 32 бита) - список полей идентификаторов источников, участвующих в создании RTP-пакета. Устройство смешивания информации (миксер) вставляет целый список SSRC идентификаторов источников, которые участвовали в построении данного RTP-пакета. Количество элементов в списке: от 0 до 15. Если число участников более 15, выбираются первые 15. Примером может служить речевая конференция, в которой передаются RTP-пакеты с речью всех участников - каждый со своим идентификатором SSRC. Они-то и образуют список идентификаторов CSRC. Вся конференция имеет общий идентификатор SSRC.

Доставка RTP-пакетов контролируется специальным протоколом RTCP (Real Time Control Protocol).

Основной функцией протокола RTCP является организация обратной связи приемника с отправителем информации для отчета о качестве получаемых данных. Протокол RTCP передает сведения (как от приемника, так и от отправителя) о числе переданных и потерянных пакетов, значении джиттера, задержке и т.д. Эта информация может быть использована отправителем для изменения параметров передачи, например для уменьшения коэффициента сжатия информации с целью улучшения качества ее передачи. Более подробное описание протоколов RTP и RTCP можно найти в RFC-1889.

5.3. Протокол UDP

Протокол передачи пользовательских дейтаграмм - User Datagram Protocol (UDP)

- базируется на протоколе IP и предоставляет прикладным процессам транспортные услуги.
- обеспечивает негарантированную доставку данных, т.е. не требует подтверждения их получения;
- не требует установления соединения между источником и приемником информации, т. е. между модулями UDP.

К заголовку IP-пакета протокол UDP добавляет служебную информацию в виде заголовка UDP-пакета (рис.5.4).

Порт отправителя		Порт получателя
Длина		Контрольная сумма
Данные		
…		

Рис.5.4. Формат UDP-пакета

Порт отправителя (Source Port) - поле указывает порт рабочей станции, передавшей дейтаграмму. На этот порт следует адресовать ответную дейтаграмму. Если данное поле не используется, оно заполняется нулями.

Порт получателя (Destination Port) - поле идентифицирует порт рабочей станции, на которую будет доставлен пакет. Наиболее известные порты UDP приведены в Таблице 5.1.

Длина (Length) - это поле информирует о длине UDP-пакета в октетах, включая как заголовок, так и данные. Минимальное значение длины равно восьми.

Контрольная сумма (Checksum) - поле проверки правильности передачи данных заголовка пакета, псевдозаголовка и поля полезной нагрузки пакета. Если данное поле не используется, оно заполняется нулями.

Модуль IP, реализованный в принимающей рабочей станции, передает поступающий из сети IP-пакет модулю UDP, если в заголовке этого пакета указано, что протоколом верхнего уровня является протокол UDP. При получении пакета от модуля IP модуль UDP проверяет контрольную сумму,

Таблица 5.1.

порты UDP

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	CharGen	Returns a string of characters
53	NameServer	Domain Name Service
67	Bootps	Server port to download bootstrap information
68	Bootpc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP trap	Simple Network Management Protocol (trap)

содержащуюся в его заголовке. Если контрольная сумма равна нулю, значит, отправитель ее не подсчитал.

Более подробную информацию о протоколе UDP можно найти в RFC-768.

5.4. Протоколы H.323

5.4.1. Архитектура системы на базе стандарта H.323

Рекомендация H.323 разработана Сектором стандартизации телекоммуникаций Международного союза электросвязи (МСЭ-Т) и содержит описания терминальных устройств, оборудования и сетевых служб, предназначенных для осуществления мультимедийной связи в сетях с коммутацией пакетов (например, в корпоративной интрасети или Интернет).

Терминальные устройства и сетевое оборудование стандарта H.323 могут передавать данные, речь и видеоинформацию в масштабе реального времени. В Рекомендации H.323 не определены: сетевой интерфейс, физическая среда передачи информации и транспортный протокол, используемый в сети. Сеть, через которую осуществляется связь между терминалами H.323, может представлять собой сегмент или множество сегментов со сложной топологией. Терминалы H.323 могут быть интегрированы в персональные компьютеры или реализованы как автономные устройства. Поддержка речевого обмена — обязательная функция для устройства стандарта H.323.

В рекомендации H.323 описываются четыре основных компонента (рис. 5.5.):

- терминал;
- gatekeeper (контроллер зоны);
- шлюз;
- устройство управления многоточечной конференцией (MCU).

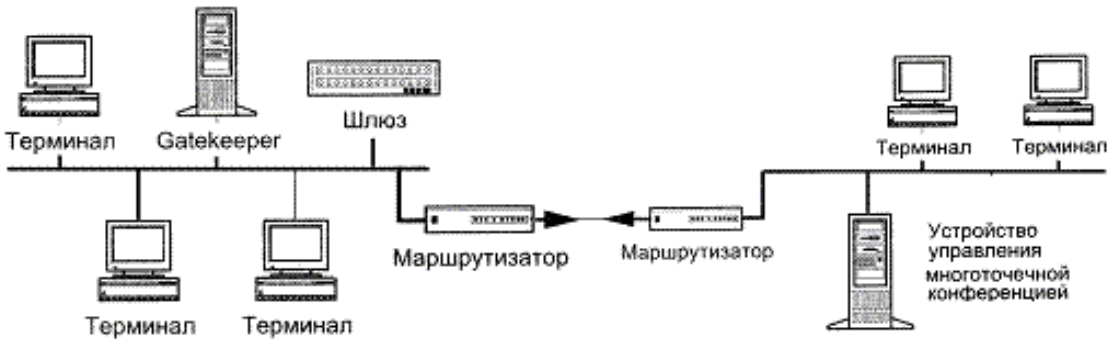


Рис 5.5. Зона H.323

Все перечисленные компоненты организованы в так называемые зоны H.323. Одна зона состоит из gatekeeper и нескольких конечных точек, причем gatekeeper управляет всеми конечными точками своей зоны. Зоной может быть и вся сеть поставщика услуг IP-телефонии или ее часть, охватывающая отдельный регион. Деление на зоны H.323 не зависит от топологии пакетной сети, но может быть использовано для организации наложенной сети H.323 поверх пакетной сети, используемой исключительно в качестве транспорта.

Терминалы H.323

Терминал H.323 представляет собой конечную точку в сети, способную передавать и принимать трафик в масштабе реального времени, взаимодействуя с другим терминалом H.323, шлюзом или устройством управления многоточечной конференцией (MCU).

Для обеспечения этих функций терминал включает в себя:

- элементы аудио (микрофон, акустические системы, телефонный микшер, система акустического эхоподавления);
- элементы видео (монитор, видеокамера);
- элементы сетевого интерфейса;
- интерфейс пользователя.

H.323-терминал должен поддерживать протоколы H.245, Q.931, RAS, RTP/RTCP и семейство протоколов H.450, а также включать в себя аудиокодек G.711. Также немаловажна поддержка протокола совместной работы над документами T. 120.

Шлюзы H.323

Технология передачи голоса по IP-сети вместо классической сети с коммутацией каналов предусматривает конфигурацию с установкой шлюзов. Шлюз обеспечивает сжатие информации (голоса), конвертирование ее в IP-пакеты и направление в IP-сеть. С противоположной стороны шлюз осуществляет обратные действия: расшифровку и расформирование пакетов вызовов. В результате обычные телефонные аппараты без проблем принимают эти вызовы.

Такое преобразование информации не должно значительно исказить исходный речевой сигнал, а режим передачи обязан сохранить обмен информацией между абонентами в реальном масштабе времени.

Более полно основные функции, выполняемые шлюзом, состоят в следующем.

- Реализация физического интерфейса с телефонной и IP-сетью.
- Детектирование и генерация сигналов абонентской сигнализации.
- Преобразование сигналов абонентской сигнализации в пакеты данных и обратно.
- Преобразование речевого сигнала в пакеты данных и обратно.
- Соединение абонентов.
- Передача по сети сигнализационных и речевых пакетов.
- Разъединение связи.

Большая часть функций шлюза в рамках архитектуры TCP/IP реализуются в процессах прикладного уровня.

Наличие разноплановых с вычислительной точки зрения функций, выполняемых системой, порождает проблему ее программной и аппаратной реализации. Рациональное решение этой проблемы основано на использовании распределенной системы, в которой управленческие задачи и связь с сетью осуществляется с помощью универсального процессора, а решения задач сигнальной обработки и телефонного интерфейса выполняются на цифровом процессоре обработки сигналов.

Схема обработки сигналов в шлюзе при подключении аналогового двухпроводного телефонного канала PSTN показана на рис. 5.6. Телефонный сигнал с двухпроводной абонентской линии поступает на дифференциальную систему, которая разделяет приемную и передающую части канала. Далее сигнал передачи вместе с "просочившейся" частью сигнала приема подается на аналого-цифровой преобразователь (ADC) и превращается либо в стандартный 12-разрядный сигнал, либо в 8-разрядный сигнал, закодированный по и- или А-закону. В последнем случае обработка должна также включать соответствующий экспандер. В устройстве эхо- компенсации

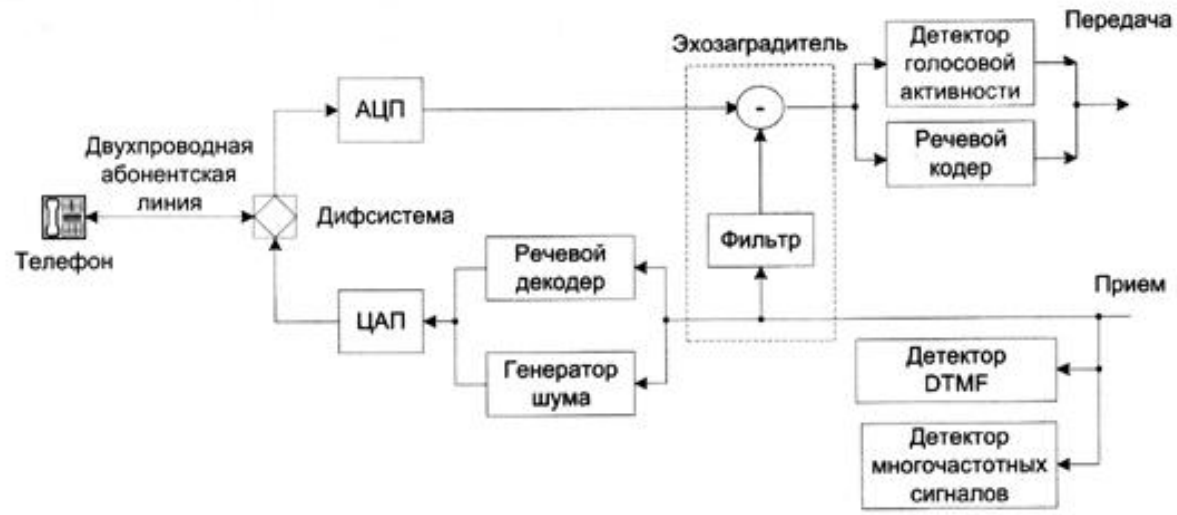


Рис. 5.6. Схема обработки сигналов в шлюзе

(Echo canceller) из сигнала передачи удаляются остатки принимаемого сигнала. Эхо-компенсатор представляет собой адаптивный нерекурсивный фильтр, длина памяти (порядок) которого и механизм адаптации выбираются такими, чтобы удовлетворить требованиям рекомендации МСЭ-Т G.165. Для обнаружения и определения сигналов внутриполосной многочастотной телефонной сигнализации (MF сигналов), сигналов частотного (DTMF) или импульсного наборов используются детекторы соответствующих типов. Дальнейшая обработка входного сигнала происходит в речевом кодере (Speech Coder). В анализаторе кодера сигнал сегментируется на отдельные фрагменты определенной длительности (в зависимости от метода кодирования) и каждому входному блоку сопоставляется информационный кадр соответствующей длины.

Часть параметров, вычисленная в анализаторе кодера, используется в блоке определения голосовой активности (VAD - voice activity detector), который решает, является ли текущий анализируемый фрагмент сигнала речью или паузой. При наличии паузы информационный кадр может не передаваться в службу виртуального канала. На сеансовый уровень передается лишь каждый пятый «паузный» информационный кадр. Кроме того, при отсутствии речи для кодировки текущих спектральных параметров используется более короткий информационный кадр. На приемной стороне из виртуального канала в логический поступает либо информационный кадр, либо флаг наличия паузы. На паузных кадрах вместо речевого синтезатора включается генератор комфортного шума (Noise Generator), который восстанавливает спектральный состав паузного сигнала. Параметры генератора обновляются при получении паузного информационного кадра. Наличие информационного кадра включает речевой декодер, на выходе которого формируется речевой сигнал. Для эхо-компенсатора этот сигнал является сигналом дальнего абонента, фильтрация которого дает составляющую электрического эха в передаваемом сигнале. В зависимости

от типа цифро-аналогового преобразования (DAC) сигнал может быть подвергнут дополнительной кодировке по А - или ц-закону.

Можно выделить следующие основные проблемы цифровой обработки сигналов в шлюзе. При использовании двухпроводных абонентских линий актуальной остаётся задача эхокомпенсации, особенность которой состоит в том, что компенсировать необходимо два различных класса сигналов - речи и телефонной сигнализации. Очень важной является задача обнаружения и детектирования телефонной сигнализации. Её сложность состоит в том, что служебные сигналы могут перемешиваться с сигналами речи.

С построением кодеков тесно связана задача синтеза VAD. Основная трудность состоит в правильном детектировании пауз речи на фоне достаточно интенсивного акустического шума (шум офиса, улицы, автомобиля и т.д.)

Gatekeeper H.323

Функцию управления вызовами выполняет gatekeeper (контроллер зоны). Gatekeeper выполняет следующие функции:

- преобразовывает адреса-псевдонимы в транспортные адреса;
- контролирует доступ в сеть на основании авторизации вызовов, наличия необходимой для связи полосы частот и других критериев, определяемых производителем;
- контролирует полосу пропускания;

управляет зонами.

Причем gatekeeper осуществляет вышеперечисленные функции в отношении терминалов, шлюзов и устройств управления, зарегистрированных в нем. Идентификация узла может осуществляться по его текущему IP-адресу, телефонному номеру E.164 или подстановочному имени - строке символов, наподобие адреса электронной почты. Gatekeeper упрощает процесс вызова, позволяя использовать легко запоминающееся подстановочное имя.

Функции gatekeeper могут быть встроены в шлюзы, элементы распределенных УПАТС, блоки управления многоточечными конференциями, а также в конечные узлы H.323 (терминалы). С помощью механизмов RAS (Registration/Admissions/Status) терминалы могут находить gatekeeper и регистрироваться в них.

Сервер управления конференциями (MCU)

Сервер управления конференциями (MCU - Multipoint Control Unit) обеспечивает связь трех и более H.323-терминалов. Все терминалы, участвующие в конференции, устанавливают соединение с MCU. Сервер управляет ресурсами конференции, согласовывает возможности терминалов по обработке звука и видео, определяет аудио- и видеопотоки, которые необходимо направлять по многим адресам.

В рамках архитектуры H.323 может быть использовано два подхода для

построения системы управления многоточечными конференциями:

- децентрализованное управление многоточечной конференцией;
- централизованное управление многоточечной конференцией.

Первый тип требует, чтобы все участники конференции пересылали многоадресные (групповые) сообщения всем остальным. Это позволяет избежать концентрации трафика в некоторых сегментах сети, но управлять такой конференцией не очень удобно. Но большинство производителей предлагают централизованные системы MCU. При их использовании конечные узлы передают сигнал системе MCU, которая и обеспечивает его рассылку. Чтобы связывать группы участников конференции, централизованные системы MCU могут каскадироваться.

По архитектуре MCU подразделяются на системы на базе стандартных серверов (Windows NT) и автономные программно-аппаратные комплексы, устанавливаемые в стойку. Примерами MCU первого типа являются - Encounter Netserver 1.2.1 фирмы VideoServer, MeetingPoint 4.0 фирмы -White Pine Software, PictureTel330 NetConference MultiPoint Video Server фирмы PictureTel. Продукты MultiMedia Communications Exchange (MMCX) компании Lucent Technologies и MCU-323 фирмы RADVision представляют собой устройства второго типа. Такие системы, будучи однажды сконфигурированными, могут круглосуточно работать в коммутационных шкафах и управляться дистанционно. MMCX компании Lucent представляет собой универсальную коммуникационную систему, поддерживающую любые H.323-совместимые устройства и IP-телефоны.

5.4.2. Сигнализация по стандарту H.323

Для выполнения действий сигнализации между шлюзами и gatekeeper в соответствии с Рекомендацией МСЭ-Т H.323 должны использоваться следующие протоколы:

- сигнализация RAS (Registration, Admission, Status);
- сигнализация 931 (согласно H.225.0);
- протокол управления H.245.

В общем случае алгоритм включает следующие фазы:

1. установление соединения
2. определение ведущего/ведомого оборудования и обмен данными об их функциональных возможностях
3. установление аудиовизуальной связи между вызывающим и вызываемым оборудованием
4. если необходимо создание конференций и обращение к дополнительным услугам завершение соединения

5.4.3. Сигнализация RAS

Протокол сигнализации RAS (регистрации, подтверждения и состояния) применяется для передачи служебных сообщений между терминалами и контроллером зоны H.323. RAS-сообщения служат для регистрации терминалов, допуска их к сеансу связи, изменения используемой полосы пропускания, информирования о состоянии сеанса и его прекращении. В отсутствии контроллера зоны (gatekeeper) протокол RAS не задействуется.

Функции сигнализации RAS используют сообщения протокола H.225.0. Канал сигнализации RAS не зависит от канала управления вызовом и канала управления H.245.

С помощью сигнализации RAS должно осуществляться:

- нахождение gatekeeper, на котором возможна регистрация оконечного оборудования;
- регистрация оконечного устройства;
- определение географического положения оконечного устройства;
- указание необходимой полосы пропускания;
- изменение полосы пропускания.
- передача сообщений RAS осуществляется в дейтаграммах UDP. Для адресации RAS должна использоваться адресная информации, в которую входят:
- сетевой адрес оборудования;
- идентификатор TSAP (Transport Layer Service Access Point);
- мнемонический адрес (Alias Adress).

Сетевой адрес является адресом в формате, используемом в сети с коммутацией пакетов, например, адрес в форматах IPv4, IPv6, IPX, NetBIOS.

Идентификатор TSAP используется для идентификации информационных потоков, отправленных с одного сетевого адреса. Для gatekeeper выделены постоянные значения идентификатора TSAP: 1718 (для поиска gatekeeper) и 1719 (для передачи сообщений сигнализации RAS).

Мнемонический адрес служит для адресации оконечного оборудования в удобной пользователю форме. Адресом может быть телефонный номер в формате E.164, телефонный номер в корпоративной сети, адрес электронной почты и т.д. Gatekeeper не имеет мнемонического адреса.

Нахождение gatekeeper должно осуществляться с помощью широковещательного запроса GRQ (Gatekeeper Request), передаваемого оконечным оборудованием с идентификатором TBAP, равным 1718. Если gatekeeper найден, и он готов обслужить запрос от оконечного оборудования, в ответ оно должно получить сообщение GCF (Gatekeeper Confirm). Если оконечное оборудование получило ответ от нескольких gatekeeper, выбор одного из них должен осуществляться оконечным оборудованием произвольным образом. Если gatekeeper не может обслужить запрос от

оконечного оборудования, то в ответ он должен передать сообщение GRJ (Gatekeeper Reject), в котором должна сообщаться причина отказа, и может содержаться адрес альтернативного gatekeeper. При нахождении gatekeeper между ним и оконечным оборудованием осуществляется установление логического канала сигнализации, по которому будут передаваться остальные сообщения RAS.

После нахождения gatekeeper оконечное оборудование в сообщении RRQ (Registration Request) должно сообщить gatekeeper свой сетевой и мнемонический адрес. В ответ gatekeeper должен передать сообщение RCF (Registration Confirm) для подтверждении регистрации оконечного оборудования, либо RRJ (Registration Reject) в случае отказа от регистрации.

Регистрация оконечного оборудования на gatekeeper может осуществляться один раз и не повторяться при включении оконечного оборудования. В этом случае gatekeeper должен определять состояние оконечного оборудования. Для этого gatekeeper должен периодически передавать сообщение IRQ (Information Request). Интервал определяется производителем оборудования и должен быть не менее 10 секунд.

После регистрации о конечного оборудования на gatekeeper оно может установить соединение с вызываемым оконечным оборудованием. Для этого оконечное оборудование- инициатор должно передать сообщение ARQ (Admissions Request) и установить логический канал для передачи сообщений 931. В сообщении ARQ указываются скорость передачи, кратная 100 бит/с, и количество каналов, необходимых для передачи речевой информации. Например, при использовании интерфейсов ISDN для выделения полосы 192 кбит/с необходимо указать значения соответственно 640 и 3. Скорость указывается без учета размеров заголовков пакетов и блоков данных транспортных протоколов. Если сеть может обеспечить требуемые параметры, то gatekeeper должен передать подтверждение ACF (Admissions Confirm), в противном случае передается сообщение ARJ (Admissions Reject) с указанием причины отказа.

После получения подтверждения оконечное оборудование устанавливает соединение с вызываемым оконечным оборудованием с использованием сигнализации Q.931 (в соответствии с H.225.0). Сообщения сигнализации Q.931 могут передаваться по логическому каналу через gatekeeper или непосредственно между двумя оконечными устройствами. Выбор способа осуществляет gatekeeper и сообщает об этом оконечному оборудованию в сообщении ACF.

Если сообщения передаются через gatekeeper, то он может либо закрыть логический канал после установления соединения для передачи речевой информации, либо оставить его до конца сеанса связи, если поддерживаются дополнительные услуги.

Для установления соединения используются сообщения Setup и Connect, после передачи которых устанавливается канал управления H.245. Канал для передачи информации управления H.245 может быть установлен

двумя способами: через gatekeeper или непосредственно между оконечными устройствами. В случае, если логический канал сигнализации 931 устанавливается через gatekeeper, то канал для передачи информации управления H.245 также должен устанавливаться через gatekeeper. Способ установления канала для передачи информации управления H.245 между оконечным оборудованием в настоящее время не специфицирован.

Если канал сигнализации RAS установлен, то он может использоваться для установления нескольких соединений. Идентификация сообщений сигнализации, принадлежащих одному и тому же соединению, осуществляется с помощью идентификатора Call ID.

5.4.4. Сигнализация H.225.0 (Q.931) и протокол управления H.245

Стандарт H.225 описывает протоколы сигнализации и формирования пакетов в системах пакетной передачи мультимедийного трафика. Канал управления вызовами H.225.0 используется для установления и разрыва соединений между двумя терминалами H.323, а также между терминалом и шлюзом. Служебные сообщения этого протокола передаются поверх TCP или UDP (рис.5.7).

<table>
<tr><td colspan="2">гарантированная доставка TCP</td><td colspan="3">негарантированная доставка UDP</td></tr>
<tr><td rowspan="2">H.245</td><td colspan="2">H.255</td><td colspan="2">речь и видеоинф</td></tr>
<tr><td>управление соединением</td><td>RAS</td><td>RTCP</td><td>RTP</td></tr>
<tr><td colspan="2">TCP</td><td colspan="3">UDP</td></tr>
<tr><td colspan="5">IP</td></tr>
<tr><td colspan="5">Канальный уровень</td></tr>
<tr><td colspan="5">Физический уровень</td></tr>
</table>

Рис.5.7. Положение H.255.0 в стеке протоколов H.323.

Протокол управления мультимедийной передачей H.245 обеспечивает:
- согласование возможностей компонентов;
- становление и разрыв логических каналов;
- передачу запросов на установление приоритета;
- управление потоком (загрузкой канала);
- передачу общих команд и индикаторов.

Сообщения протокола H.245 передаются по специальному каналу *управления.* Это логический канал «0», который, в отличие от каналов обмена

мультимедиа-потоками, постоянно открыт. Обмен параметрами между терминалами позволяет согласовывать режимы работы и форматы кодирования информации, что обеспечивает взаимодействие терминалов от разных производителей. В процессе обмена сообщениями о параметрах уточняются возможности терминалов принимать и передавать различные виды трафика.

С помощью сигнализации Q.931 согласно рекомендации МСЭ-Т H.225.0 и протоколу управления H.245 должно осуществляться:

• передача запроса на установление соединения;
• инициализация соединения и обмен информацией о возможностях;
• установление соединения для передачи речевой информации;
• разъединение соединения.

Для установления соединения инициатор вызова (оконечное оборудование 1) должно передать сообщение Setup оконечному оборудованию 2 по логическому каналу сигнализации.

В ответ получатель (оконечное оборудование 2) должен передать сообщение Connect, сообщающее инициатору о готовности установить соединение. Инициатор сообщения должен получить сообщения Call proceeding, Connect, Alerting в течении 4 секунд. После получения сообщения Connect должен быть установлен логический канал управления H.245, по которому передается информация о возможностях оконечного оборудования в сообщении terminal Capability Set.

После инициализации соединения создается логический канал для передачи речевой информации. Установление канала для передачи речевой информации осуществляется оконечным оборудованием после получения сообщения Open Logical Channel по каналу управления H.245. Передача речевой информации по логическому каналу должна осуществляться в пакетах RTP. Передача управляющей информации должна осуществляться в пакетах RTCP.

Базовое соединение с участием привратника показано на рис.5.8. На рисунке видно, что в обслуживании вызова в разные фазы принимают участие 3 вида сигнализации.

Соединение разъединяется следующим образом:

- инициатор разъединения должен закрыть канал сообщением close Logical Channel, передаваемым по каналу управления H.245;
- инициатор разъединения должен передать сообщение and Session Command, передаваемым по каналу управления H.245;
- удаленное оборудование дожидается сообщения and Session Command, передаваемое по каналу управления H.245;

если логический канал сигнализации 931 открыт, он закрывается сообщением Release Complete. Если в системе присутствует Gatekeeper, то он должен освободить ранее выделенную полосу пропускания. Освобождение полосы пропускания осуществляется сообщением DRQ (Disengage Request) сигнализации RAS, передаваемым оконечным оборудованием. В ответ

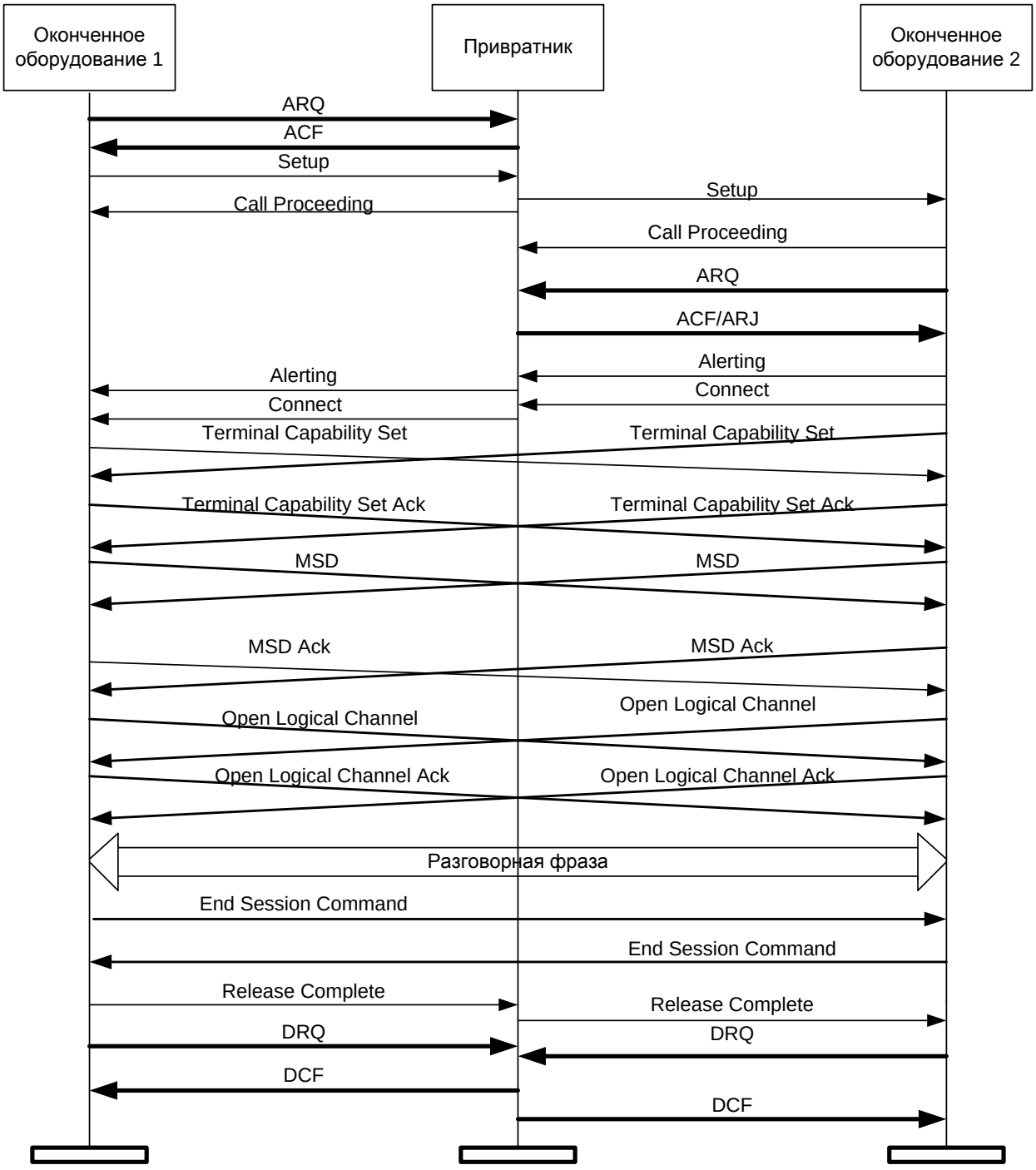


Рис.5.8. Базовое соединение с участием привратника.

должно быть получено сообщение подтверждения DCF (Disengage Confirm) или сообщение отказа DRJ (Disengage Reject).

5.5. Протокол SIP

5.5.1.Функциональные возможности протокола SIP

Вторым вариантом построения сетей стал протокол SIP, разработанный группой MMUSIC (Multiparty Multime-dia Session Control) комитета IETF (Internet Engineering Task Force), а спецификации протокола представлены в документе RFC 2543

Протокол инициирования сеансов - Session Initiation Protocol (SIP) - является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и распределения мультимедийной информации, в основу которого заложены следующие принципы.

- Персональная мобильность пользователей. Пользователи могут перемещаться без ограничений в пределах сети, поэтому услуги связи должны предоставляться им в любом месте этой сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится. Для этого пользователь с помощью специального сообщения - REGISTER - информирует о своих перемещениях сервер определения местоположения.
- Масштабируемость сети характеризуется, в первую очередь, возможностью увеличения количества элементов сети при ее расширении. Серверная структура сети, построенной на базе протокола SIP, в полной мере отвечает этому требованию.
- Расширяемость протокола характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.
- Интеграция в стек существующих протоколов Интернет. Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом Internet Engineering Task Force (IETF).
- Взаимодействие с другими протоколами сигнализации. Протокол SIP может быть использован совместно с протоколом H.323. Возможно также взаимодействие протокола SIP с системами сигнализации ТфОП - DSS1 и ОКС7. Для упрощения такого взаимодействия сигнальные сообщения протокола SIP могут переносить не только специфический SIP-адрес, но и телефонный номер формата E.164 или любого другого формата. Кроме того, протокол SIP, наравне с протоколами H.323 и ISUP/IP, может применяться для синхронизации работы устройств управления шлюзами, в этом случае он должен взаимодействовать с протоколом MGCP. Другой важной особенностью протокола SIP является то, что он приспособлен к организации доступа пользователей сетей IP-телефонии к услугам интеллектуальных сетей, и существует мнение, что именно этот протокол станет основным при организации связи между указанными сетями.

Для организации взаимодействия с существующими приложениями IP-

сетей и для обеспечения мобильности пользователей протокол SIP использует адрес, подобный адресу электронной почты. В качестве адресов рабочих станций используются специальные универсальные указатели ресурсов - URL (Universal Resource Locators), так называемые SIP URL

SIP-адреса бывают четырех типов:

• имя@домен;
• имя@хост,
• имя@IP-адрес;
• №телефона@шлюз.

Таким образом, адрес состоит из двух частей. Первая часть - это имя пользователя, зарегистрированного в домене или на рабочей станции. Если вторая часть адреса идентифицирует какой-либо шлюз, то в первой указывается телефонный номер абонента.

Во второй части адреса указывается имя домена, рабочей станции или шлюза. Для определения IP-адреса устройства необходимо обратиться к службе доменных имен - Domain Name Service (DNS). Если же во второй части SIP-адреса размещается IP-адрес, то с рабочей станцией можно связаться напрямую.

В начале SIP-адреса ставится слово «sip:», указывающее, что это именно SIP-адрес, т.к. бывают и другие (например, «mailto:»). Ниже приводятся примеры SIP-адресов:

sip: student@sk.niis.uz
sip: userTUIT@192.168.100.152
sip: 294-75-47@gateway.ru

5.5.2. Интеграция протокола SIP с IP-сетями

Интеграция в стек существующих протоколов Интернет, разработанных IETF. Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом Internet Engineering Task Force (IETF). Эта архитектура включает в себя также протокол резервирования ресурсов (Resource Reservation Protocol - RSVP), транспортный протокол реального времени (Real-Time Transport Protocol - RTP), протокол передачи потоковой информации в реальном времени (Real-Time Streaming Protocol - RTSP), протокол описания параметров связи (Session Description Protocol - SDP). Однако функции протокола SIP не зависят ни от одного из этих протоколов.

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. В качестве транспорта могут использоваться протоколы X.25, Frame Relay, AAL5, IPX и др. Структура сообщений SIP не зависит от выбранной транспортной технологии. Но в то же время предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDP.

Здесь же следует отметить, что сигнальные сообщения могут переноситься не только протоколом транспортного уровня UDP, но и протоколом TCP. По сети с маршрутизацией пакетов IP может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация, называемая мультимедийной информацией. При организации связи между терминалами пользователей необходимо известить встречную сторону, какого рода информация может приниматься (передаваться), алгоритм ее кодирования и адрес, на который ее следует передавать. Таким образом, одним из обязательных условий организации связи при помощи протокола SIP является обмен между

Протокол инициирования сеансов связи (SIP)	Прикладной уровень
Протоколы TCP и UDP	Транспортный уровень
Протоколы IPv4 и IPv6	Сетевой уровень
PPP, AAL5. ATM, Ethernet, V.34.	Уровень звена данных
UTP5, ВОЛС и др.	Физический уровень

Рис.5.9. Место протокола SIP в стеке протоколов TCP/IP

предполагаемыми участниками этой связи данными об их функциональных возможностях. Для этой цели чаще всего используется протокол описания сеансов связи SDP (Session Description Protocol). В течение сеанса связи может производиться его модификация, поэтому предусмотрена передача средствами SDP сообщений SIP с новыми описаниями сеанса.

В протоколе SIP не реализованы механизмы управления потоками информации и предоставления гарантированного качества обслуживания. Кроме того, протокол SIP не предназначен для передачи пользовательской информации, в его сообщениях может переноситься информация лишь ограниченного объема.

Для передачи речевой информации комитет IETF предлагает использовать протокол RTP, но сам протокол SIP не исключает возможность применения для этих целей других протоколов.

Протокол SIP предусматривает организацию конференций трех видов:

- в режиме многоадресной рассылки (multicasting), когда информация передается на один multicast-адрес, а затем доставляется сетью конечным адресатам;
- при помощи устройства управления конференции (MCU), к которому участники конференции передают информацию в режиме точка-точка, а оно, в свою очередь, обрабатывает ее (т.е. смешивает или коммутирует) и рассылает участникам конференции;
- путем соединения каждого пользователя с каждым в режиме точка-точка.

Протокол SIP дает возможность присоединения новых участников к уже существующему сеансу связи, т.е. двусторонний сеанс может перейти в конференцию.

5.5.3. Архитектура сети SIP

Протокол SIP работает по схеме клиент-сервер. Клиент выдает запросы, в которых указывает, что он желает получить от сервера. Сервер принимает запрос, обрабатывает его и выдает ответ, который может содержать уведомление об успешном выполнении запроса, уведомление об ошибке или информацию, затребованную клиентом.

Рис.5.10. Схема "клиент-сервер"

Протоколом SIP предусмотрены 3 основных сценария установления соединения: с участием прокси-сервера, с участием сервера переадресации, и непосредственно между пользователями. Различие между перечисленными сценариями заключается в том, что по-разному осуществляется поиск и приглашение вызываемого пользователя. В первом случае эти функции возлагает на себя прокси-сервер, а вызывающему пользователю необходимо знать только постоянный SIP-адрес вызываемого пользователя. Во втором случае вызывающая сторона самостоятельно устанавливает соединение, а сервер переадресации лишь реализует преобразование постоянного адреса вызываемого абонента в его текущий адрес. И, наконец, в третьем случае вызывающему пользователю для установления соединения необходимо знать текущий адрес вызываемого пользователя.

Таким образом сеть SIP содержит основные элементы трех видов: агенты пользователя, прокси-серверы и серверы переадресации.

Агенты пользователя (User Agent или SIP client) являются приложениями терминального оборудования и включают в себя две составляющие: агент пользователя - клиент (User Agent Client - UAC) и агент пользователя - сервер (User Agent Server - UAS), иначе известные как клиент и сервер соответственно. Клиент UAC инициирует SIP-запросы, т.е. выступает в качестве вызывающей стороны. Сервер UAS принимает запросы и возвращает ответы, т.е. выступает в качестве вызываемой стороны.

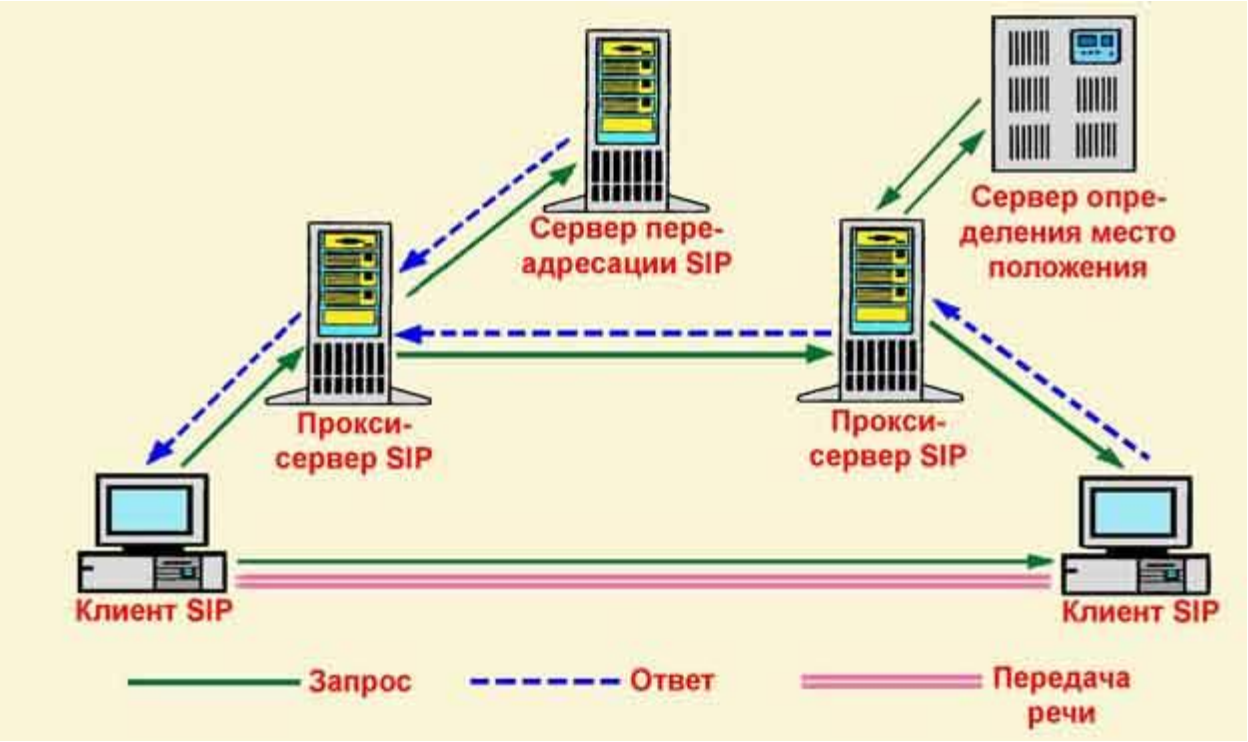


Рис.5.11. Архитектура SIP сети

Следует особо отметить, что сервер UAS и клиент UAC могут (но не обязаны) непосредственно взаимодействовать с пользователем, а другие клиенты и серверы SIP этого делать не могут. Если в устройстве присутствуют и сервер UAS, и клиент UAC, то оно называется агентом пользователя - User Agent (UA), а по своей сути представляет собой терминальное оборудование SIP.

Кроме терминалов определены два основных типа сетевых элементов SIP: прокси-сервер (proxy server) и сервер переадресации (redirect server).

Прокси-сервер (от английского proxy - представитель) представляет интересы пользователя в сети. Он принимает запросы, обрабатывает их и, в зависимости от типа запроса, выполняет определенные действия. Это может быть поиск и вызов пользователя, маршрутизация запроса, предоставление услуг и т.д. Прокси-сервер состоит из клиентской и серверной частей, поэтому может принимать вызовы, инициировать собственные запросы и возвращать ответы. Ответные сообщения следуют по тому же пути обратно к прокси-серверу, а не к клиенту.

Прокси - сервер может быть физически совмещен с сервером определения местоположения (в этом случае он называется registrar) или существовать отдельно от этого сервера, но иметь возможность взаимодействовать с ним.

Предусмотрено режима работы прокси-серверов - с сохранением состояний (stateful) и без сохранения состояний (stateless).

Сервер первого типа хранит в памяти входящий запрос, который явился причиной генерации одного или нескольких исходящих запросов. Эти исходящие запросы сервер также запоминает. Все запросы хранятся в памяти

сервера только до окончания транзакции, т.е. до получения ответов на запросы.

Сервер первого типа позволяет предоставить большее количество услуг, но работает медленнее, чем сервер второго типа.

Сервер без сохранения состояний просто ретранслирует запросы и ответы, которые получает. Он работает быстрее, чем сервер первого типа, так как ресурс процессора не тратится на запоминание состояний, вследствие чего сервер этого типа может обслужить большее количество пользователей. Недостатком такого сервера является то, что на его базе можно реализовать лишь наиболее простые услуги. Впрочем, прокси-сервер может функционировать как сервер с сохранением состояний для одних пользователей и как сервер без сохранения состояний - для других.

Сервер переадресации предназначен для определения текущего адреса вызываемого пользователя. Вызывающий пользователь передает к серверу сообщение с известным ему адресом вызываемого пользователя, а сервер обеспечивает переадресацию вызова на текущий адрес этого пользователя. Для реализации этой функции сервер переадресации должен взаимодействовать с сервером определения местоположения.

Сервер переадресации не терминирует вызовы как сервер RAS и не инициирует собственные запросы как прокси-сервер. Он только сообщает адрес либо вызываемого пользователя, либо прокси-сервера. По этому адресу инициатор запроса передает новый запрос. Сервер переадресации не содержит клиентскую часть программного обеспечения.

Но пользователю не обязательно связываться с каким-либо SIP-сервером. Он может сам вызвать другого пользователя при условии, что знает его текущий адрес.

Сервер определения местоположения пользователей. Пользователь может перемещаться в пределах сети, поэтому необходим механизм определения его местоположения в текущий момент времени. Например, сотрудник предприятия уезжает в командировку, и все вызовы, адресованные ему, должны быть направлены в другой город на его временное место работы. О том, где он находится, пользователь информирует специальный сервер с помощью сообщения REGISTER.

Для хранения текущего адреса пользователя служит сервер определения местоположения пользователей, представляющий собой базу данных адресной информации. Кроме постоянного адреса пользователя, в этой базе данных может храниться один или несколько текущих адресов.

5.5.4. Сравнительный анализ H.323 и SIP

Сравнивать возможности H.323 и SIP довольно трудно.

Оба протокола являются результатом решения одних и тех же задач специалистами ITU-T и комитета IETF. Естественно, что решение ITU-T

оказалось ближе к традиционным телефонным сетям, а решение комитета IETF базируется на принципах, составляющих основу сети Internet.

Перейдем непосредственно к сравнению протоколов, которое будем проводить по нескольким критериям.

1. Дополнительные услуги.

Набор услуг, поддерживаемых обоими протоколами, примерно одинаков. Дополнительные услуги, предоставляемые протоколом H.323, стандартизированы в серии рекомендаций ITU-T H.450.X. Протоколом SIP правила предоставления дополнительных услуг не определены, что является его серьезным недостатком, так как вызывает проблемы при организации взаимодействия оборудования разных фирм-производителей. Некоторые специалисты предлагают решения названных проблем, но эти решения пока не стандартизированы.

Примеры услуг, предоставляемых обоими протоколами:

• Перевод соединения в режим удержания (Call hold);

• Переключение связи (Call Transfer);

• Переадресация (Call Forwarding);

• Уведомление о новом вызове во время связи (Call Waiting);

• Конференция.

Протокол SIP предусматривает три способа организации конференции: с использованием устройства управления конференциями MCU, режима многоадресной рассылки и соединений участников друг с другом. В последних двух случаях функции управления конференциями могут быть распределены между терминалами, т.е. центральный контроллер конференций не нужен. Это позволяет организовывать конференции с практически неограниченным количеством участников. Рекомендация H.323 предусматривает те же три способа, но управление конференцией во всех случаях производится централизованно контроллером конференций MC.

В то же время, протокол H.323 предоставляет больше возможностей управления услугами, как в части аутентификации и учета, так и в части контроля использования сетевых ресурсов. Возможности протокола SIP в этой части беднее, и выбор оператором этого протокола может служить признаком того, что для оператора важнее техническая интеграция услуг, чем возможности управления услугами.

Технология H.323 предоставляет больше возможностей по управлению услугами, как в части аутентификации и учета, так и в части контроля использования сетевых ресурсов. Возможности протокола SIP в этой части беднее, и выбор оператором этого протокола может служить признаком того, что для оператора важнее техническая интеграция услуг, чем возможности управления услугами.

2. Персональная мобильность пользователей.

Протокол SIP имеет хороший набор средств поддержки персональной мобильности пользователей, в число которых входит переадресация вызова к новому местоположению пользователя, одновременный поиск по нескольким

направлениям (с обнаружением зацикливания маршрутов) и т.д. В протоколе SIP это организуется путем регистрации на сервере определения местоположения, взаимодействие с которым может поддерживаться любым протоколом. Персональная мобильность поддерживается и протоколом H.323, но менее гибко. Так, например, одновременный поиск пользователя по нескольким направлениям ограничен тем, что привратник, получив запрос определения местоположения пользователя, не транслирует его к другим привратникам.

3. Расширяемость протокола. Возможность введения новых версий протоколов и обеспечение совместимости различных версий одного протокола. Расширяемость (extensibility) протокола обеспечивается:

- согласованием параметров;
- стандартизацией кодеков;
- модульностью архитектуры.

Протокол SIP достаточно просто обеспечивает совместимость разных версий. Поля, которые не понятны оборудованию, просто игнорируются. Это уменьшает сложность протокола, а также облегчает обработку сообщений и внедрение новых услуг.

Новые функциональные возможности вводятся в протокол H.323 с помощью поля NonStandardParameter. Оно содержит код производителя и, следом за ним, код услуги, который действителен только для этого производителя. Это позволяет производителю расширять услуги, но сопряжено с некоторыми ограничениями. Во-первых, невозможно запросить у вызываемой стороны информацию о поддерживаемых ею услугах, во-вторых, невозможно добавить новое значение уже существующего параметра. Существуют также проблемы, связанные с обеспечением взаимодействия оборудования разных производителей.

4.Масштабируемость сети .

Многие специалисты считают протокол SIP более масштабируемым, чем H.323. Это связано с тем, что сервер SIP, по умолчанию, не хранит сведений о текущих сеансах связи и поэтому может обработать больше вызовов, чем привратник H.323, который хранит эти сведения . Вместе с тем, отсутствие таких сведений, по мнению некоторых специалистов, может вызвать трудности при организации взаимодействия сети IP-телефонии с ТФОП, работающей в режиме state-full.

5. Время установления соединения.

В запросе INVITE протокола SIP содержится вся необходимая для установления соединения информация, включая описание функциональных возможностей терминала. Таким образом, в протоколе SIP для установления соединения требуется одна транзакция, а в протоколе H.323 необходимо производить обмен сообщениями несколько раз. По этим причинам затраты времени на установление соединения в протоколе SIP значительно меньше затрат времени в протоколе H.323.

6. Адресация.

Использование URL является сильной стороной протокола SIP и позволяет легко интегрировать его в существующую систему DNS-серверов и внедрять в оборудование, работающее в IP-сетях. Пользователь получает возможность переправлять вызовы на Web-страницы или использовать электронную почту. Адресом в SIP может также служить телефонный номер с адресом используемого шлюза.

В протоколе H.323 используются транспортные адреса и alias-адреса. В качестве последнего может использоваться телефонный номер, имя пользователя или адрес электронной почты. Для преобразования alias-адреса в транспортный адрес обязательно участие привратника.

7. Сложность протокола.

Протокол H.323, несомненно, сложнее протокола SIP. Протокол H.323 использует большое количество информационных полей в сообщениях (до 100), при нескольких десятках таких же полей в протоколе SIP.

Протокол SIP использует текстовый формат сообщений, подобно протоколу HTTP. Это облегчает синтаксический анализ и генерацию кода, позволяет реализовать протокол на базе любого языка программирования, облегчает эксплуатационное управление, дает возможность ручного ввода некоторых полей, облегчает анализ сообщений. Название заголовков SIP-сообщений ясно указывает их назначение. Протокол H.323 использует двоичное представление своих сообщений на базе языка ASN.1, поэтому их непосредственное чтение затруднительно.

В целом можно сделать вывод, что протокол SIP ориентирован на Интернет-провайдеров, которые рассматривают услугу Интернет-телефонии лишь как небольшую часть своего сервисного пакета. Будучи самодостаточной, технология H.323 больше подходит для корпоративных сетей (интранет) и поставщиков услуг Ip-телефонии, для которых данные услуги не являются доминирующими. В целом H.323 и SIP не следует рассматривать каРеализация дополнительных услуг на базе протокола SIP

5.5.5. Запросы протокола SIP

В настоящей версии протокола SIP определено шесть типов запросов. Каждый из них предназначен для выполнения довольно широкого круга задач, что является явным достоинством протокола SIP, так как благодаря этому число сообщений, которыми обмениваются терминалы и серверы, сведено к минимуму. С помощью запросов клиент сообщает о текущем местоположении, приглашает пользователей принять участие в сеансах связи, модифицирует уже установленные сеансы, завершает их и т.д. Сервер определяет тип принятого запроса по названию, указанному в стартовой строке.

Запрос INVITE приглашает пользователя принять участие в сеансе связи. Он обычно содержит описание сеанса связи, в котором указывается

вид принимаемой информации и параметры (список возможных вариантов параметров), необходимые для приема информации, а также может указываться вид информации, которую вызываемый пользователь желает передавать. В ответе на запрос типа INVITE указывается вид информации, которая будет приниматься вызываемым пользователем, и, кроме того, может указываться вид информации, которую вызываемый пользователь собирается передавать (возможные параметры передачи информации). В этом сообщении могут содержаться также данные, необходимые для аутентификации абонента, и, следовательно, доступа клиентов к SIP-серверу. При необходимости изменить характеристики уже организованных каналов передается запрос INVITE с новым описанием сеанса связи. Для приглашения нового участника к уже установленному соединению также используется сообщение INVITE.

Запрос ACK подтверждает прием ответа на запрос INVITE. Следует отметить, что запрос ACK используется только совместно с запросом INVITE, т.е. этим сообщением оборудование вызывающего пользователя показывает, что оно получило окончательный ответ на свой запрос INVITE. В сообщении ACK может содержаться окончательное описание сеанса связи, передаваемое вызывающим пользователем.

Запрос CANCEL отменяет обработку ранее переданных запросов с теми же, что и в запросе CANCEL, значениями полей Call-ID, To, From и CSeq, но не влияет на те запросы, обработка которых уже завершена. Например, запрос CANCEL применяется тогда, когда прокси-сервер размножает запросы для поиска пользователя по нескольким направлениям и в одном из них его находит. Обработку запросов, разосланных во всех остальных направлениях, сервер отменяет при помощи сообщения CANCEL.

Запросом BYE оборудование вызываемого или вызывающего пользователя завершает соединение. Сторона, получившая запрос BYE, должна прекратить передачу речевой (мультимедийной) информации и подтвердить его выполнение ответом 200 OK.

При помощи запроса типа REGISTER пользователь сообщает своё текущее местоположение. В этом сообщении содержатся следующие поля:

• Поле To содержит адресную информацию, которую надо сохранить или модифицировать на сервере;

• Поле From содержит адрес инициатора регистрации. Зарегистрировать пользователя может либо он сам, либо другое лицо, например, секретарь может зарегистрировать своего начальника

• Поле Contact содержит новый адрес пользователя, по которому должны передаваться все дальнейшие запросы INVITE. Если в запросе REGISTER поле Contact отсутствует, то регистрация остаётся прежней. В случае отмены регистрации здесь помещается символ «*»;

• В поле Expires указывается время в секундах, в течение которой регистрация действительна. Если данное поле отсутствует, то по умолчанию назначается время — 1 час, после чего регистрации отменяется. Регистрацию

можно также отменить, передав сообщение REGISTER с полем Expires, которому присвоено значени(О), и с соответствующим полем Contact.

Запросом OPTIONS вызываемый пользователь запрашивает информацию о функциональных возможностях терминального оборудования вызываемого пользователя. В ответ на этот запрос оборудование вызываемого пользователя сообщает требуемые сведения. Применение запроса OPTIONS ограничено теми случаями, когда необходимо узнать о функциональных возможностях оборудования до установления соединения. Для установления соединения запрос этого типа не используется.

После испытаний протокола SIP в реальных сетях оказалось, что для решения ряда задач вышеуказанных шести типов запросов недостаточно. Поэтому возможно, что в протокол будут введены новые сообщения. Так, в текущей версии протокола SIP не предусмотрен способ передачи информации управления соединением или другой информации во время сеанса связи. Для решения этой задачи был предложен новый тип запроса — INFO. Он может использоваться:

- для переноса сигнальных сообщений ТфОП/ ISDN/ сотовых сетей между шлюзами в течение разговорной сессии;
- для переноса сигналов DTMF в течение разговорной сессии;
- для переноса биллинговой информации.

5.5.6. Ответы протокола SIP

Все ответы делятся на две группы: информационные и финальные.

Информационные ответы показывают, что запрос находится в стадии обработки. Они кодируются трехзначным числом, начинающимся с единицы, — 1xx. Некоторые информационные ответы, например, 100 Trying, предназначены для установки на нуль таймеров, которые запускаются в оборудовании, передавшем запрос. Если к моменту срабатывания таймера ответ на запрос не получен, то считается, что этот запрос потерян и может (по усмотрению производителя) быть передан повторно. Один из распространенных ответов— 180 Ringing; по назначению он идентичен сигналу «Контроль посылки вызова» в ТфОП и означает, что вызываемый пользователь получает сигнал о входящем вызове.

Финальные ответы кодируются трехзначными числами, начинающимися с цифр 2, 3, 4, 5 и 6. Они означают завершение обработки запроса и содержат, когда это нужно, результат обработки запроса. Назначение финальных ответов каждого типа рассматривается ниже.

Ответы 2xx означают, что запрос был успешно обработан. В настоящее время из всех ответов типа 2xx определен лишь один— 200 ОК. Его значение зависит от того, на какой запрос он отвечает:

• ответ 200 ОК на запрос INVITE означает, что вызываемое оборудование согласно на участие в сеансе связи; в теле ответа указываются

функциональные возможности этого оборудования;
• ответ 200 ОК на запрос BYE означает завершение сеанса связи, в теле ответа никакой информации не содержится;
• ответ 200 ОК на запрос CANCEL означает отмену поиска, в теле ответа никакой информации не содержится;
• ответ 200 ОК на запрос REGISTER означает, что регистрация прошла успешно;
• ответ 200 ОК на запрос OPTION служит для передачи сведений о функциональных возможностях оборудования, эти сведения содержатся в теле ответа.

Ответы 3xx информируют оборудование вызывающего пользователя о новом местоположении вызываемого пользователя или переносят другую информацию, которая может быть использована для нового вызова:
• в ответе 300 Multiple Choices указывается несколько SIP-адресов, по которым можно найти вызываемого пользователя, и вызывающему пользователю предлагается выбрать один из них;
• ответ 301 Moved Permanently означает, что вызываемый пользователь больше не находится по адресу, указанному в запросе, и направлять запросы нужно на адрес, указанный в поле Contact;
• ответ 302 Moved Temporary означает, что пользователь временно (промежуток времени может быть указан в поле Expires) находится по другому адресу, который указывается в поле Contact.

Ответы 4xx информируют о том, что в запросе обнаружена ошибка. После получения такого ответа пользователь не должен передавать тот же самый запрос без его модификации:
• ответ 400 Bad Request означает, что запрос не понят из-за наличия в нем синтаксических ошибок;
• ответ 401 Unauthorized означает, что запрос требует проведения процедуры аутентификации пользователя. Существуют разные варианты аутентификации, и в ответе может быть указано, какой из них использовать в данном случае;
• ответ 403 Forbidden означает, что сервер понял запрос, но отказался его обслуживать. Повторный запрос посылать не следует. Причины могут быть разными, например, запросы с этого адреса не обслуживаются и т.д.;
• ответ 485 Ambiguous означает, что адрес в запросе не определяет вызываемого пользователя однозначно;
• ответ 486 Busy Here означает, что вызываемый пользователь в на- стоящий момент не может принять входящий вызов по данному адресу. Ответ не исключает возможности связаться с пользователем по другому адресу или, к примеру, оставить сообщение в речевом почтовом ящике.

Ответы 5xx информируют о том, что запрос не может быть обработан из-за отказа сервера:
• ответ 500 Server Internal Error означает, что сервер не имеет возможности обслужить запрос из-за внутренней ошибки. Клиент может попытаться

повторно послать запрос через некоторое время;
• ответ 501 Not lmplemented означает, что в сервере не реализованы функции, необходимые для обслуживания этого запроса. Ответ передается, например, в том случае, когда сервер не может распознать тип запроса;
• ответ 502 Bad Gateway информирует о том, что сервер, функционирующий в качестве шлюза или прокси-сервера, принял некорректный ответ от сервера, к которому он направил запрос;
• ответ 503 Service Unavailable говорит от том, что сервер не может в данный момент обслужить вызов вследствие перегрузки или проведения технического обслуживания.

Ответы 6XX информируют о том, что соединение с вызываемым пользователем установить невозможно:
• ответ 600 Busy Everywhere сообщает, что вызываемый пользователь занят и не может принять вызов в данный момент ни по одному из имеющихся у него адресов. Ответ может указывать время, подходящее для вызова пользователя;
• ответ 600 Decline означает, что вызываемый пользователь не может или не желает принять входящий вызов. В ответе может быть указано подходящее для вызова время;
• ответ 600 Does Not Exist Anywhere означает, что вызываемого пользователя не существует.

5.5.7. Сценарий установления соединения через сервер переадресации

Вызывающему пользователю требуется вызвать другого пользователя. Он передает запрос INVITE (1) на известный ему адрес сервера переадресации и на порт 5060, используемый по умолчанию (см.рис.5.11).
В запросе вызывающий пользователь указывает адрес вызываемого пользователя. Сервер переадресации запрашивает текущий адрес нужного пользователя у сервера определения местоположения (2), который сообщает ему этот адрес (3). Сервер переадресации в своем ответе 302 Moved temporarily передает вызывающей стороне текущий адрес вызываемого пользователя (4), или сообщает список зарегистрированных адресов вызываемого пользователя, предлагая вызывающему самому выбрать один из них. Вызывающая сторона подтверждает прием ответа 302 передачей сообщения ACK (5).
Теперь вызывающая сторона может связаться с вызываемой стороной. Для этого она передает новый запрос INVITE (6). В теле сообщения INVITE указываются данные о функциональных возможностях вызывающей стороны в формате протокола SDP.

Вызываемая сторона принимает запрос INVITE и начинает его обработку, о чем сообщает ответом 100 Trying (7) встречному оборудованию для перезапуска его таймеров. После завершения обработки поступившего

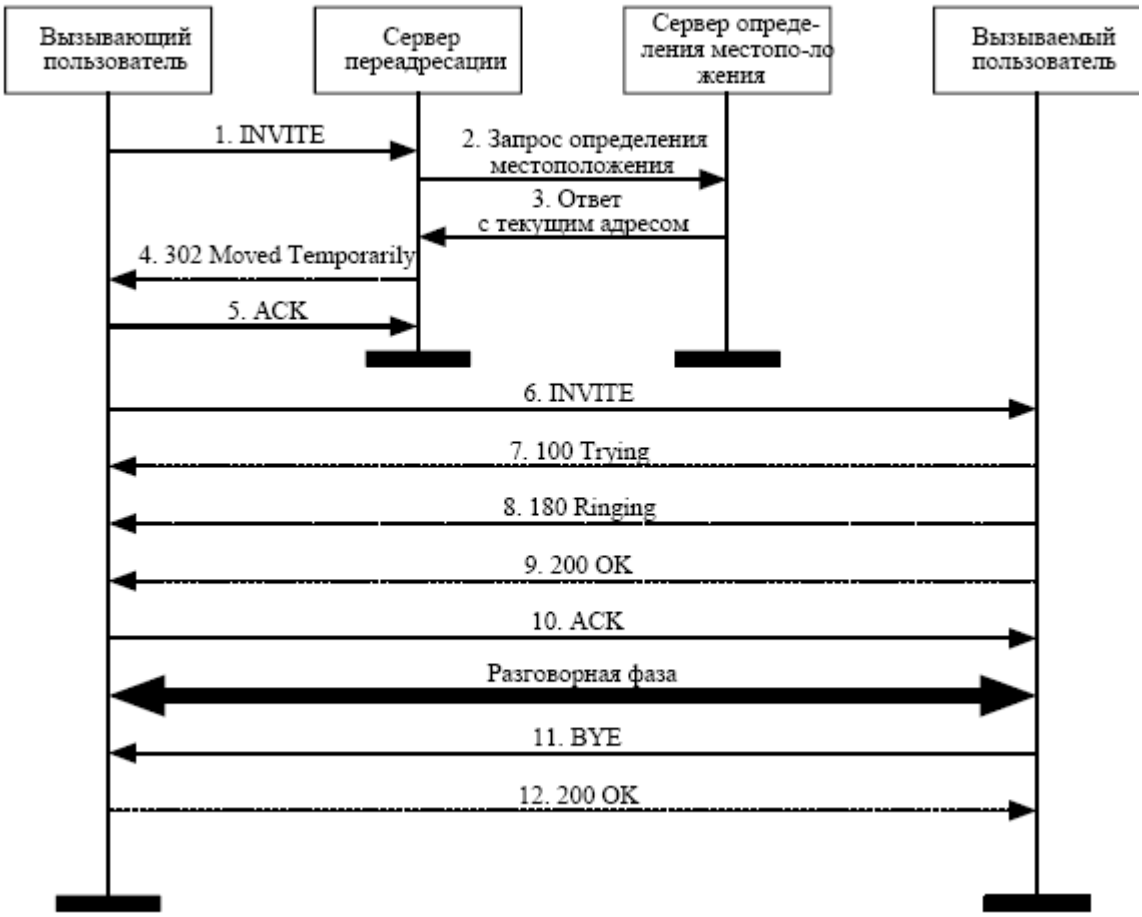


Рис. 5.11. Сценарий установления соединения через сервер переадресации

запроса оборудование вызываемой стороны сообщает своему пользователю о входящем вызове, а встречной стороне передает ответ 180 Ringing (8). После приема вызываемым пользователем входящего вызова встречной стороне передается сообщение 200 OK (9), в котором содержатся данные о функциональных возможностях вызываемого терминала в формате протокола SDP.

Терминал вызывающего пользователя подтверждает прием ответа запросом ACK (10). На этом фаза установления соединения заканчивается, и начинается разговорная фаза. По завершении разговорной фазы любая из сторон передает запрос BYE (11), который подтверждается ответом 200 OK (12).

5.5.8. Сценарий установления соединения через прокси-сервер

В этом случае действия 1–3 такие же, как и при использовании сервера переадресации. После выяснения адреса (на сервере определения местоположения) прокси-сервер передает по этому адресу запрос INVITE (4).

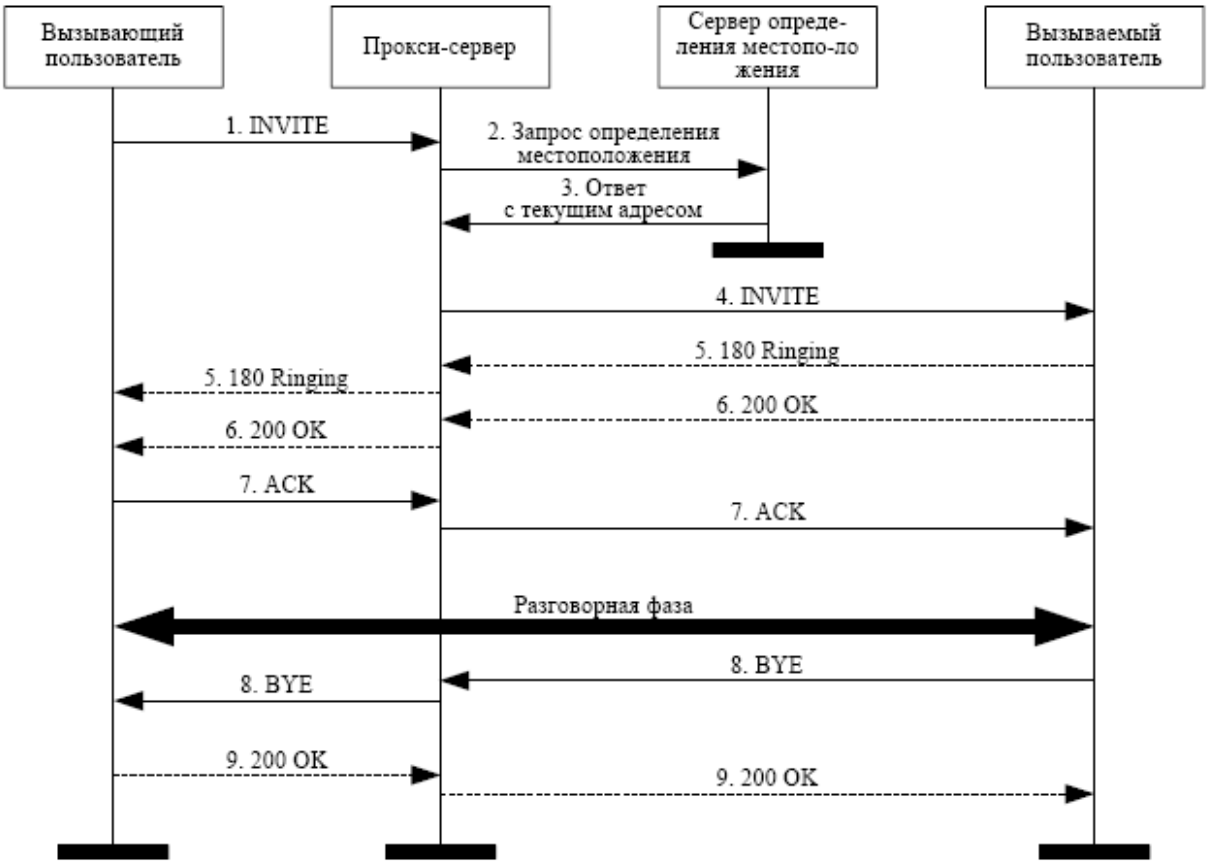


Рис. 5.12. Сценарий установления соединения через прокси сервер

Вызываемый пользователь B оповещается акустическим или визуальным сигналом о том, что его вызывают (5); он поднимает трубку, и ответ 200 OK отправляется к прокси-серверу (6). Прокси-сервер переправляет этот ответ вызвавшему пользователю A (7), последний подтверждает правильность приема, передавая запрос ACK (8), который переправляется к вызванному пользователю B (9). Соединение установлено, идет разговор. Вызванный пользователь B кладёт трубку, передается запрос BYE (10), прием которого подтверждается ответом 200 OK (11).

5.6. Архитектура сети на базе MGCP и MEGACO

Третий подход к построению сетей IP-телефонии, основанный на использовании протокола MGCP предложен комитетом IETF, рабочей группой MEGACO.

При разработке этого протокола рабочая группа MEGACO опиралась на сетевую архитектуру, содержащую основные функциональные блоки трех видов (рис.5.12):

- шлюз - Media Gateway (MG), который выполняет функции преобразования речевой информации, поступающей со стороны ТфОП

с постоянной скоростью передачи, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP (кодирование и упаковку речевой информации в пакеты RTP/UDP/IP, а также обратное преобразование);

- контроллер шлюзов - Call Agent, которой выполняет функции управления шлюзами;

шлюз сигнализации - Signaling Gateway (SG), который обеспечивает доставку сигнальной информации, поступающей со стороны ТфОП, к контроллеру шлюзов и перенос сигнальной информации в обратном направлении.

Таким образом, весь интеллект функционально распределенного шлюза сосредоточен в контроллере, функции которого могут быть распределены между несколькими компьютерными платформами.

Шлюз сигнализации выполняет функции STP - транзитного пункта сети сигнализации ОКС7. Сами шлюзы выполняют только функции преобразования речевой информации. Один контроллер управляет одновременно несколькими шлюзами. В сети могут присутствовать несколько контроллеров. Предполагается, что они синхронизованы между собой и согласованно управляют шлюзами, участвующими в соединении.

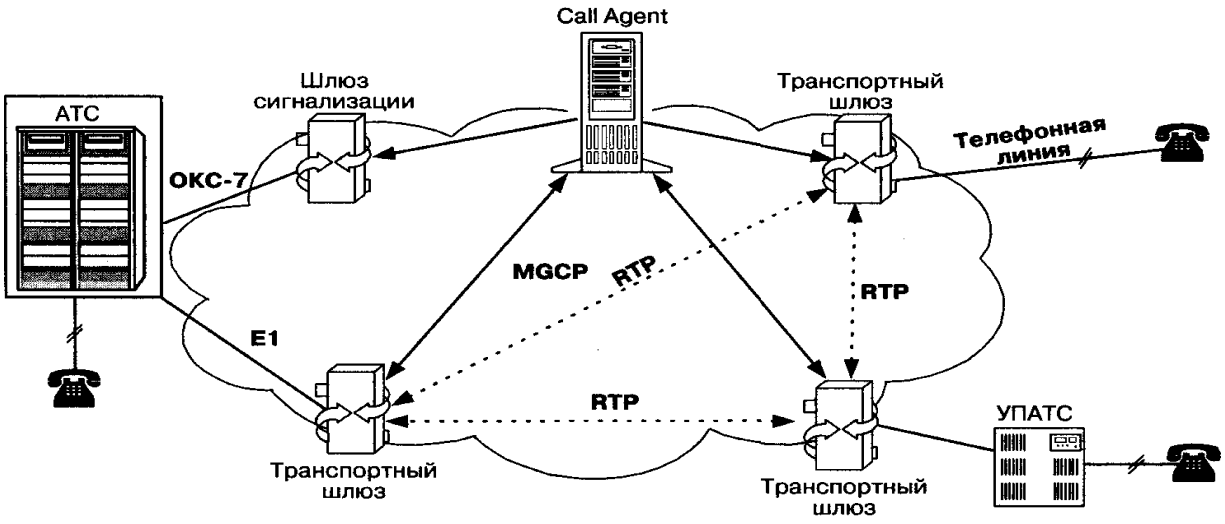


Рис.5.12. Архитектура сети на базе протокола MGCP

Вместе с тем, MEGACO не определяет протокола для синхронизации работы контроллеров. В ряде работ, посвященных исследованию возможностей протокола MGCP, для этой цели предлагается использовать протоколы H.323, SIP или ISUP/IP.

Сообщения протокола MGCP переносятся протоколом без гарантированной доставки сообщений UDP. Рабочая группа SIGTRAN комитета IETF в настоящее время разрабатывает механизм взаимодействия контроллера шлюзов и шлюза сигнализации.

Шлюз сигнализации должен принимать поступающие из ТфОП пакеты трех нижних уровней системы сигнализации ОКС7 (уровней подсистемы

переноса сообщений MTP) и передавать сигнальные сообщения верхнего, пользовательского, уровня к контроллеру шлюзов. Шлюз сигнализации также должен уметь передавать по IP-сети приходящие из ТфОП сигнальные сообщения Q.931 .

Если в ТфОП используется сигнализация по выделенным сигнальным каналам (ВСК), то сигналы сначала поступают вместе с пользовательской информацией в транспортный шлюз, а затем передаются в контроллер шлюзов без посредничества шлюза сигнализации.

Протокол MGCP является внутренним протоколом для обмена информацией между функциональными блоками распределенного шлюза, который извне представляется одним шлюзом. Протокол MGCP является master/slave протоколом. Это означает, что контроллер шлюзов является ведущим, а сам шлюз - ведомым устройством, которое должно выполнять все команды, поступающие от контроллера Call Agent.

Вышеописанное решение обеспечивает масштабируемость сети и простоту управления сетью через контроллер шлюзов. Шлюзы не должны быть интеллектуальными устройствами, требуют меньшей производительности процессоров и, следовательно, становятся менее дорогими. Кроме того, очень быстро вводятся новые протоколы сигнализации или дополнительные услуги, так как эти изменения затрагивают только контроллер шлюзов, а не сами шлюзы.

5.7. Алгоритмы установления и разрушения соединения с использованием протокола MGCP

Рассмотрим алгоритмы установления и разрушения соединения с использованием протокола MGCP. Первый пример охватывает взаимодействие протокола MGCP с протоколом ОКС7 (рис.8.2). Второй пример иллюстрирует взаимодействие протокола MGCP с протоколами ОКС7 и H.323 (рис.5.13).

От телефонной станции АТС-А к шлюзу сигнализации SG1 по общему каналу сигнализации поступает запрос соединения в виде сообщения IAM протокола ISUP [6]. На рис.5.13 шлюз сигнализации SG1 и SG2 совмещены с транспортными шлюзами TGW1 и TGW2 соответственно.

1. Шлюз SG1 передает сообщение IAM к контроллеру шлюзов, который обрабатывает запрос и определяет, что вызов должен быть направлен к АТС-Б посредством шлюза TGW2.
2. Контроллер резервирует порт шлюза TGW1 (разговорный канал). С этой целью он передает к шлюзу команду CreateConnection. Отметим, что порт шлюза TGW1 может только принимать информацию (режим «recvonly»), так как он еще не осведомлен о том, по какому адресу и каким образом ему следует передавать информацию.
3. В ответе на эту команду шлюз TGW1 возвращает описание параметров

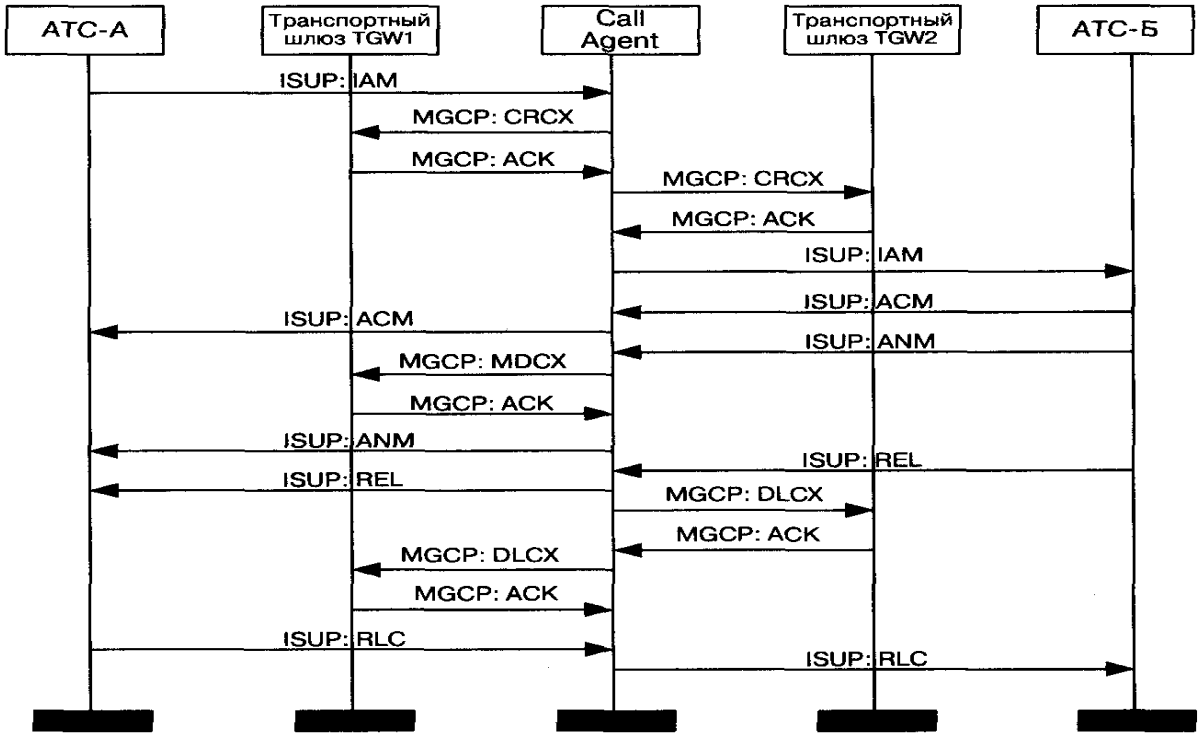


Рис.5.13. Установление и разрушение соединения с использованием протокола MGCP

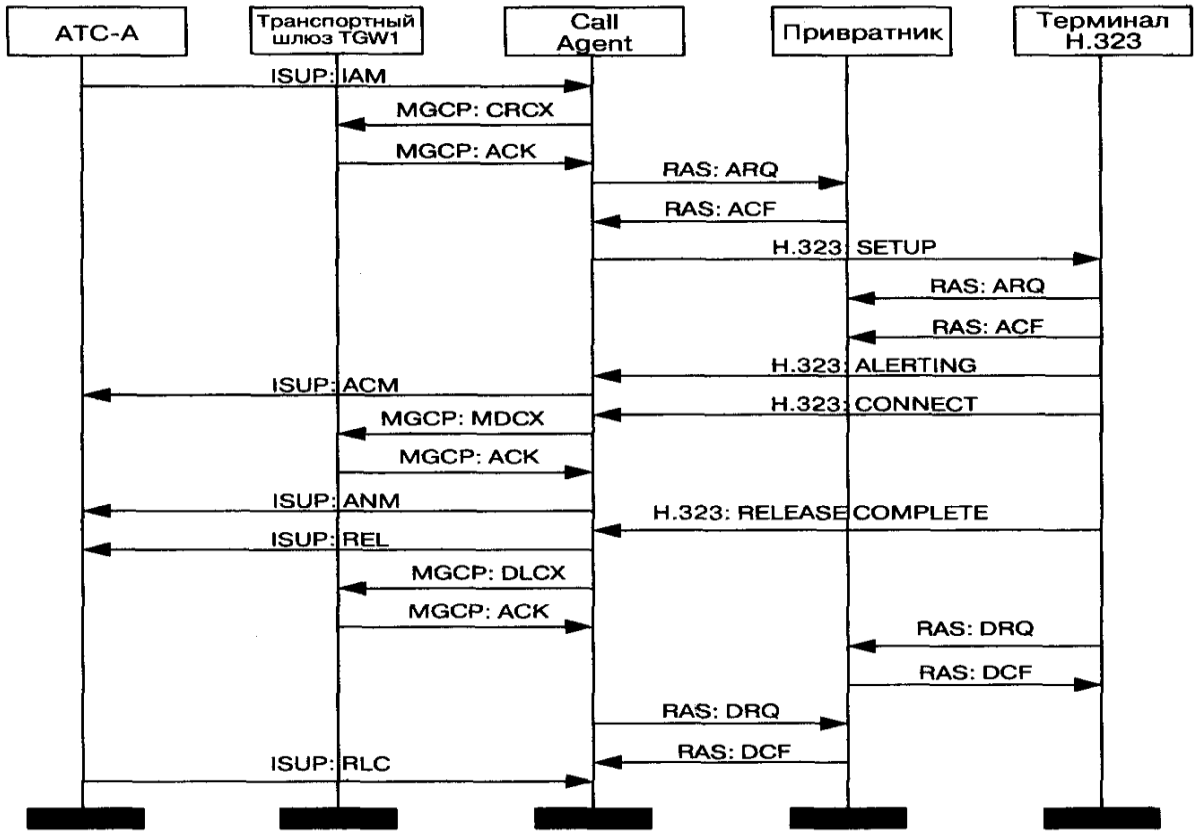


Рис.5.14. Установление и разрушение соединения с использованием протоколов MGCP, H.323, ОКС7

сеанса связи.

4. Приняв ответ шлюза TGW1, контроллер передает команду CRCX второму шлюзу TGW2 с целью зарезервировать порт в этом шлюзе.
5. Шлюз TGW2 выбирает порт, который будет участвовать в соединении, и подтверждает прием команды CRCX. При помощи двух команд CRCX создается однонаправленный разговорный канал для передачи вызывающему абоненту акустических сигналов или речевых подсказок и извещений. В то же время, порт шлюза TGW2 уже может не только принимать, но и передавать информацию, так как он получил описание параметров связи от встречного шлюза.
6. Далее контроллер шлюзов передает сообщение IAM к АТС-Б.
7. На сообщение IAM станция АТС-Б отвечает подтверждением ACM, которое немедленно пересылается к станции АТС-А.
8. После того как вызываемый абонент примет вызов, АТС-Б передает к контроллеру шлюзов сообщение ANM.
9. Далее контроллер заменяет в шлюзе TGW1 режим «recvonly» на полнодуплексный режим при помощи команды MDCX.
10. Шлюз TGW1 выполняет и подтверждает изменение режима.
11. Контроллер передает сообщение ANM к АТС-А, после чего начинается разговорная фаза соединения.
12. Завершение разговорной фазы происходит следующим образом. В нашем случае вызвавший абонент Б дает отбой первым. АТС-Б передает через шлюз сигнализации сообщение REL к контроллеру шлюзов.
13. Приняв сообщение REL, контроллер шлюзов завершает соединение с вызванным абонентом.
14. Шлюз подтверждает завершение соединения и передает к контроллеру собранные за время соединения статистические данные.
15. Контроллер шлюзов передает сообщение RLC к АТС-Б с целью подтвердить разъединение.
    Параллельно контроллер завершает соединение с вызвавшей стороной.
16. ШлюзTGW1 подтверждает завершение соединения и передает к контроллеру собранные за время соединения статистические данные.
17. АТС-А подтверждает завершение соединения передачей сообщения RLC, после чего соединение считается разрушенным.

5.8. Протокол MEGACO/H.248

5.8.1 История создания и особенности протокола MEGACO/H.248

На рис.5.15 представлено дерево эволюции протокола MEGACO/H.248. Основные особенности протокола MEGACO/ H.248.

- Для переноса сигнальных сообщений MEGACO/H.248 могут использоваться протоколы UDP, TCP, SCTP или транспортная технология

АТМ. Поддержка протокола UDP - одно из обязательных требований к контроллеру шлюзов. Протокол TCP должен поддерживаться и контроллером, и транспортным шлюзом, а поддержка SCTP, технологии АТМ, является необязательной.

- сообщения MEGACO/H.248 могут кодироваться двумя способами. Комитет IETF предложил текстовый способ кодирования сигнальной информации, а для описания сеанса связи предложил использовать протокол SDP. ITU-T предусматривает бинарный способ представления сигнальной информации - ASN. 1, а для описания сеансов связи

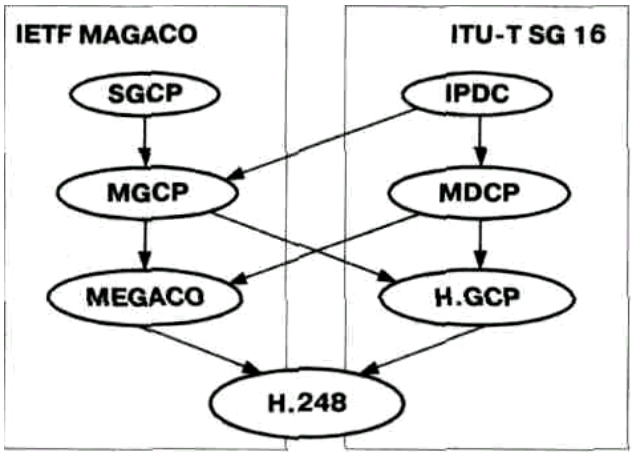


Рис.5.15. Дерево эволюции протокола MEGACO/H.248

рекомендует специальный инструмент - Tag-length-value (TLV). Контроллер шлюза должен поддерживать оба способа кодирования, в то время как шлюз - только один из этих способов

5.8.2. Модель процесса обслуживания вызова

Протокол MEGACO оперирует с двумя логическими объектами внутри транспортного шлюза: порт (termination) и контекст (context), которыми может управлять контроллер шлюза. Пример модели процесса обслуживания вызова приведен на рис.5.16.

Порты являются источниками и приемниками речевой информации. Определено два вида портов: физические и виртуальные. Физические порты, существующие постоянно с момента конфигурации шлюза, это аналоговые телефонные интерфейсы оборудования, поддерживающие одно телефонное соединение, или цифровые каналы, также поддерживающие одно телефонное соединение и сгруппированные по принципу временного разделения каналов в тракт E1. Виртуальные порты, существующие только в течение разговорной сессии, являются портами со стороны IP сети (RTP-порты), через которые ведутся передача и прием пакетов RTP.

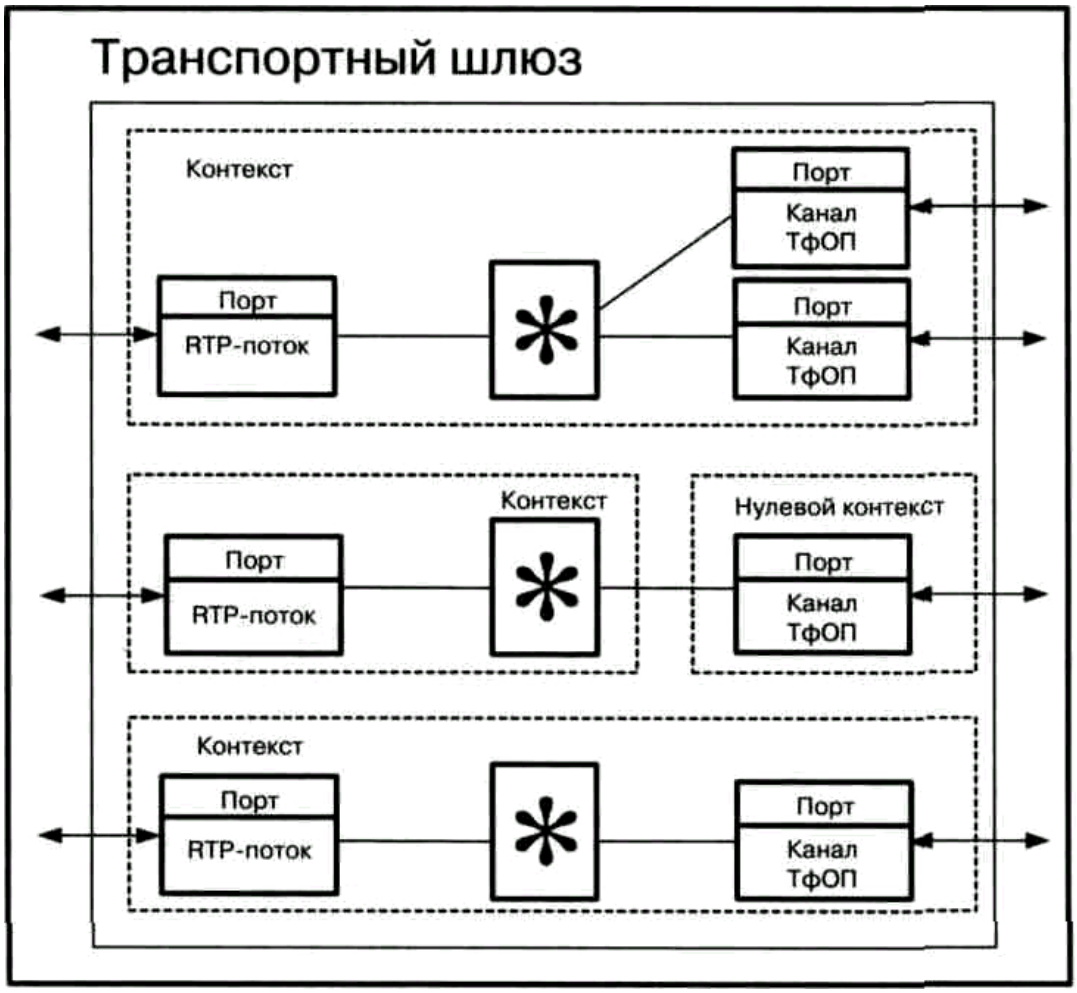


Рис.5.16. Примеры модели процесса обслуживания вызова

Виртуальные порты создаются шлюзом при получении от контроллера команды Add и ликвидируются при получении команды Subtract, тогда как физические порты при получении команды Add или Subtract, соответственно, выводятся из нулевого контекста или возвращаются обратно в нулевой контекст.

Порт имеет уникальный идентификатор (TerminationID), который назначается шлюзом при конфигурации порта. Например, идентификатором порта может служить номер тракта E1 и номер временного канала внутри тракта. Иногда команды могут относиться ко всему шлюзу, тогда используется специальный идентификатор порта (TerminationID) - «Root».

Порты обладают рядом свойств (properties), каждое из которых имеет уникальный идентификатор (propertylD). Например, порты могут обладать свойствами генерировать речевые подсказки, акустические и вызывные сигналы, а также детектировать сигналы DTMF.

При создании портов некоторые свойства присваиваются им по умолчанию. При помощи протокола MEGACO контроллер может изменять свойства портов шлюза. Свойства портов группируются в дескрипторы, которые включаются в команды управления портами (таблица 5.2).

Таблица 5.2

Дескрипторы протокола MEGACO

Название дескриптора	Описание
Modem	Идентифицирует тип и параметры модема
Mux	Описывает тип мультиплексирования информации, используемый мультимедийными терминалами, например, H.221, H.223, H.225.0
Media	Специфицирует параметры информационного потока
TerminationState	Специфицирует свойства порта шлюза. Дескриптор содержит два параметра. Параметр ServiceStates описывает статус порта (работает в тестовом режиме - test, находится в нерабочем состоянии - out of service, по умолчанию указывается, что порт работает в нормальном режиме - in service). Параметр BufferedEventProcessingMode описывает реакцию шлюза на событие, о котором не надо немедленно оповещать контроллер. Определены две реакции на событие: игнорировать или обработать
Stream	Включает в себя ряд дескрипторов (Remote, Local, LocalControl, Signals, Events), специфицирующих параметры отдельного двунаправленного информационного потока
Local	Содержит параметры, описывающие информационный поток, передаваемый или принимаемый данным шлюзом. Информация, содержащаяся в этом дескрипторе, переносится от одного шлюза к другому
Remote	Содержит параметры, описывающие информационный поток, передаваемый или принимаемый удаленным шлюзом. Информация, содержащаяся в этом дескрипторе, переносится от одного шлюза к другому
LocalControl	Содержит параметр Mode - режим работы и ряд свойств порта. Параметр Mode может принимать значения send-only, receive-only, send/receive, inactive, loop-back и delete. Дескриптор передается на участке между шлюзом и контроллером
Events	Определяет события, которые шлюз должен отслеживать, и реакцию на эти события. Определены следующие реакции: NotifyAction (известить контроллер), Accumulate (сохранить информацию о событии в буфере), AccumulateByDigitMap (накопить цифры номера в соответствии с планом нумерации), KeepActive (известить контроллер, и продолжить

	передачу сигнала)
Signals	Описывает сигналы конечному пользователю, передачу которых порт шлюза должен начать или прекратить
Audit	Содержит информацию (в виде ряда дескрипторов), которую контроллер запрашивает у шлюза. Посылается в командах AuditValue и AuditCapabilities
Packages	Описывает совокупность свойств порта, передается в команде AuditValue
DigitMap	При помощи этого дескриптора контроллер информирует шлюз об используемом плане нумерации
ServiceChange	Содержит информацию, относящуюся к изменению состояния порта шлюза, такую как причина, метод изменения и др.
Observed Events	Содержит информацию о произошедших событиях. Передается в командах Notify и AuditValue
Statistics	Содержит статистическую информацию, собранную портом за время соединения
Extension	Позволяет передавать информацию, не специфицированную в протоколе

Контекст - это отображение связи между несколькими портами, то есть абстрактное представление соединения двух или более портов одного шлюза. В любой момент времени порт может относиться только к одному контексту, который имеет свой уникальный идентификатор. Существует особый вид контекста - нулевой. Все порты, входящие в нулевой контекст, не связаны ни между собой, ни с другими портами. Например, абстрактным представлением свободного (не занятого) канала в модели процесса обслуживания вызова является порт в нулевом контексте.

В общем случае для присоединения порта к контексту служит команда Add. При этом, если контроллер не специфицирует существующий контекст, к которому должен быть добавлен порт, то шлюз создает новый контекст.
Если шлюз поддерживает конференцию, то контекст определяет топологию связей между портами, участвующими в конференции, то есть возможные направления потоков информации для каждой пары портов.

5.8.3. Сравнительный анализ протоколов MGCP и MEGACO

Общие черты протоколов MGCP и MEGACO.

- Оба протокола используются в сетях с одинаковой архитектурой, где

транспортными шлюзами управляют высокоинтеллектуальные контроллеры.

- Оба протокола умеют работать со шлюзами одних и тех же видов, классификация шлюзов была дана в предыдущей главе.
- Порты шлюзов поддерживают детектирование одних и тех же событий и генерацию одних и тех же сигналов.
- Используются одинаковые транспортные механизмы для доставки сообщений систем сигнализации ОКС7, DSS1, ВСК.
- Процедуры установления и разрушения соединений, реализуемые обоими протоколами, идентичны.
- используются одинаковые механизмы поддержания защиты сети.

Отличие протокола MEGACO/H.248 от протокола MGCP

- использование иной модели организации связи. Протокол MEGACO/H.248 работает не только с телефонными портами, но и UDP-портами. Connection в модели MGCP - это, в общем случае, подключение к соединению между портами разного оборудования, context в модели MEGACO/H.248 всегда отображает связь между портами одного шлюза (рис. 8.6).
- Меняя топологию связей портов, относящихся к одному контексту, при помощи протокола MEGACO контроллер может гибко управлять конференциями. Данной возможности в протоколе MGCP не предусмотрено.
- для протокола MEGACO/H.248 предусмотрено два способа кодирования, тогда как сообщения протокола MGCP представляются в текстовом формате, а бинарный способ кодирования не поддерживается. Кроме того, в протоколах используются разные параметры команд и коды ошибок.

Протокол MEGACO/H.248, так же, как и протокол MGCP, предусматривает корреляцию команд и ответов. Но если в протоколе MGCP транзакция образуется из команды и ответа на нее, то в протоколе MEGACO/H.248 транзакция состоит из запроса - совокупности акций и отклика на запрос.

Каждая акция, в свою очередь, состоит из одной или нескольких команд, относящихся к одному контексту, и ответов на них (рис.5.17). Использование такого инструмента позволяет значительно уменьшить объем передаваемой сигнальной информации и увеличить скорость установления соединений за счет того, что контроллер может параллельно вести обработку сигнальной информации, относящейся к разным соединениям.

Аналоги двух избыточных команд EndpointConfiguration и NotificationRequest протокола MGCP в протоколе MEGACO/H.248 отсутствуют, но, в тоже время, добавлена команда Move, позволяющая в одно действие перевести порт из одного контекста в другой. В качестве примера использования команды Move приведем сценарий дополнительных услуг «Уведомление о входящем вызове и перевод существующего соединения в режим удержания», англоязычное название услуг - Call Waiting и Call Hold.

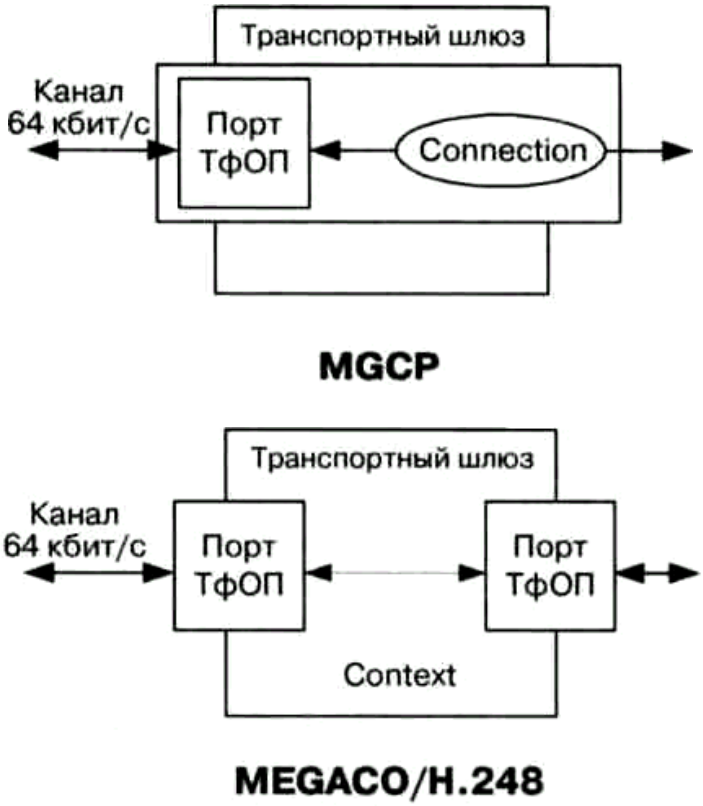


Рис.5.17. Модели MGCP и MEGACO/H.248

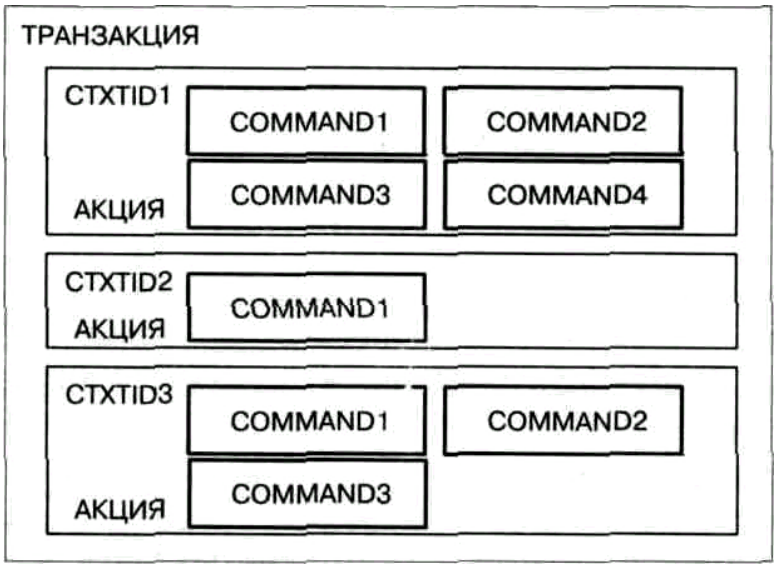


Рис.5.18. Транзакция протокола MEGACO/H.248

На базе протокола MGCP построен ряд сетей IP-телефонии. Все это означает, что оба протокола MGCP и MEGACO/H.248 вполне могут совместно использоваться в одной сети.

5.8.4. Структура команд и ответов H.248/MEGACO

Команды используются для манипулирования двумя основными объектами протокола MEGACO/H.248 - портами и контекстами. В большинстве случаев команды передает контроллер, но существуют два исключения: команда Notify, передается шлюзом, а команда ServiceChange может передаваться и шлюзом, и контроллером.

Таблица 5.3.

Команды протокола MEGACO/H.248

Команда	Направление передачи	Назначение
Add (Добавить)	MGC -> MG	Контроллер дает указание шлюзу добавить порт к контексту
Modify (Изменить)	MGC → MG	Контроллер дает указание шлюзу изменить свойства порта
Subtract (Отключить)	MGC → MG	Контроллер изымает порт из контекста
Move (Перевести)	MGC → MG	Контроллер переводит порт из одного контекста в другой в одно действие
AuditValue (Проверить порт)	MGC → MG	Контроллер запрашивает свойства порта, произошедшие события или сигналы, передаваемые в канал, а также статистику, собранную на текущий момент времени
AuditCapabilities (Проверить возможности порта)	MGC → MG	Контроллер запрашивает возможные значения свойств порта, список событий, которые могут быть выявлены портом, список сигналов, которые порт может посылать в канал, статические данные
Notify (Уведомить)	MG → MGC	Шлюз информирует контроллер о произошедших событиях
ServiceChange (Рестарт)	MG→MGC, MGC → MG	Шлюз информирует контроллер о том, что один или несколько портов выходят из рабочего состояния или возвращаются в рабочее состояние. Контроллер может предписать порту или группе портов выйти из обслуживания или вернуться в обслуживание

Команда Add добавляет порт к контексту. Если команда относится к первому порту, который должен быть добавлен к контексту, то создается новый контекст. В ответе на команду должен передаваться TerminationID, назначенный шлюзом.

Команда Modify изменяет свойства, события или сигналы для

существующего порта. Если команда относится к конкретному порту шлюза, участвующего в контексте, то должен быть указан идентификатор порта.

Команда Subtract отключает порт от существующего контекста. В ответ на команду Subtract в дескрипторе StatisticsDescriptor шлюз посылает статистику, собранную за время соединения.

Команда Move переводит порт из текущего контекста в другой контекст в одно действие.

При помощи команды AuditValue контроллер запрашивает сведения о свойствах порта, произошедших событиях или сигналах, передаваемых в канал, а также статистику, собранную на текущий момент. В ответ на команду передаются запрашиваемые параметры порта или портов шлюза.

При помощи команды AuditCapabilities контроллер запрашивает возможные значения свойств порта, список событий, которые могут быть обнаружены портом, список сигналов, которые порт может передавать в канал, статические данные. В ответ на команду передаются запрашиваемые параметры порта.

Команда Notify служит для того, чтобы известить контроллер о событиях, которые произошли в шлюзе.

Команда ServiceChange позволяет шлюзу известить контроллер о том, что порт или группа портов вышли из обслуживания или вернулись в обслуживание. Media Gateway Controller может предписать порту выйти из обслуживания или вернуться в обслуживание. При помощи данной команды контроллер может передать управление шлюзом другому контроллеру. В таблице 5.4 приведены коды ошибок, используемые в протоколе MEGACO/H.248.

Таблица 5.4.

Коды ошибок

Код ошибок	Описание
400	Некорректный запрос
401	Ошибка в протоколе
402	Авторизация не подтверждена
403	Синтаксическая ошибка в транзакции
410	Некорректный идентификатор
411	В транзакции указан идентификатор несуществующего контекста
412	Отсутствуют свободные идентификаторы контекста
420	Нет такого события или сигнала в пакете (package)
421	Неизвестная акция или некорректная комбинация акций
422	Синтаксическая ошибка в акции
430	Неизвестный идентификатор порта
431	Несуществующий идентификатор порта
432	Отсутствуют свободные идентификаторы портов

433	Порт, с указанным идентификатором, уже добавлен к контексту
440	Не поддерживаемый или неизвестный пакет
441	Отсутствует дескриптор Remote
442	Синтаксическая ошибка в команде
443	Не поддерживаемая или неизвестная команда
444	Не поддерживаемый или неизвестный дескриптор
445	Не поддерживаемое или неизвестное свойство
446	Не поддерживаемый или неизвестный параметр
447	Дескриптор не совместим с командой
448	Два одинаковых дескриптора в команде
450	Отсутствующее в пакете свойство
451	Отсутствующее в пакете событие
452	Отсутствующий в пакете сигнал
453	Отсутствующая в пакете статистическая информация
454	Отсутствующее значение параметра в пакете
455	Параметр не совместим с дескриптором
456	Два одинаковых параметра или свойства в дескрипторе
500	Внутренняя ошибка в шлюзе
501	Не поддерживается
502	Оборудование не готово
503	Услуга не реализована
510	Недостаточно ресурсов
512	Шлюз не оборудован для детектирования требуемого события
513	Шлюз не оборудован для генерирования требуемого сигнала
514	Шлюз не может воспроизвести уведомление или подсказку
515	Не поддерживаемый вид информации
517	Не поддерживаемый или некорректный режим
518	Переполнение буфера, в котором хранится информация о произошедших событиях
519	Не хватает памяти для хранения плана нумерации
520	Шлюз не имеет информации об используемом плане нумерации
521	Порт рестартовал
526	Недостаточная полоса пропускания
529	Внутренняя неисправность в аппаратном обеспечении
530	Временная неисправность сети
531	Постоянная неисправность сети
581	Не существует

5.8.5. Пример установления и разрушения соединения

На рис.5.19 приведен пример установления соединения с использованием протокола MEGACO между двумя шлюзами (Residential Gateway), управляемыми одним контроллером. В данном примере вызывающий шлюз MG1 - имеет IP-адрес 124.124.124.222, адрес вызываемого шлюза MG2 - 125.125.125.111, адрес контроллера шлюзов MGC - 123.123.123.4. Порт для связи по протоколу MEGACO для всех трех устройств по умолчанию имеет значение 55555

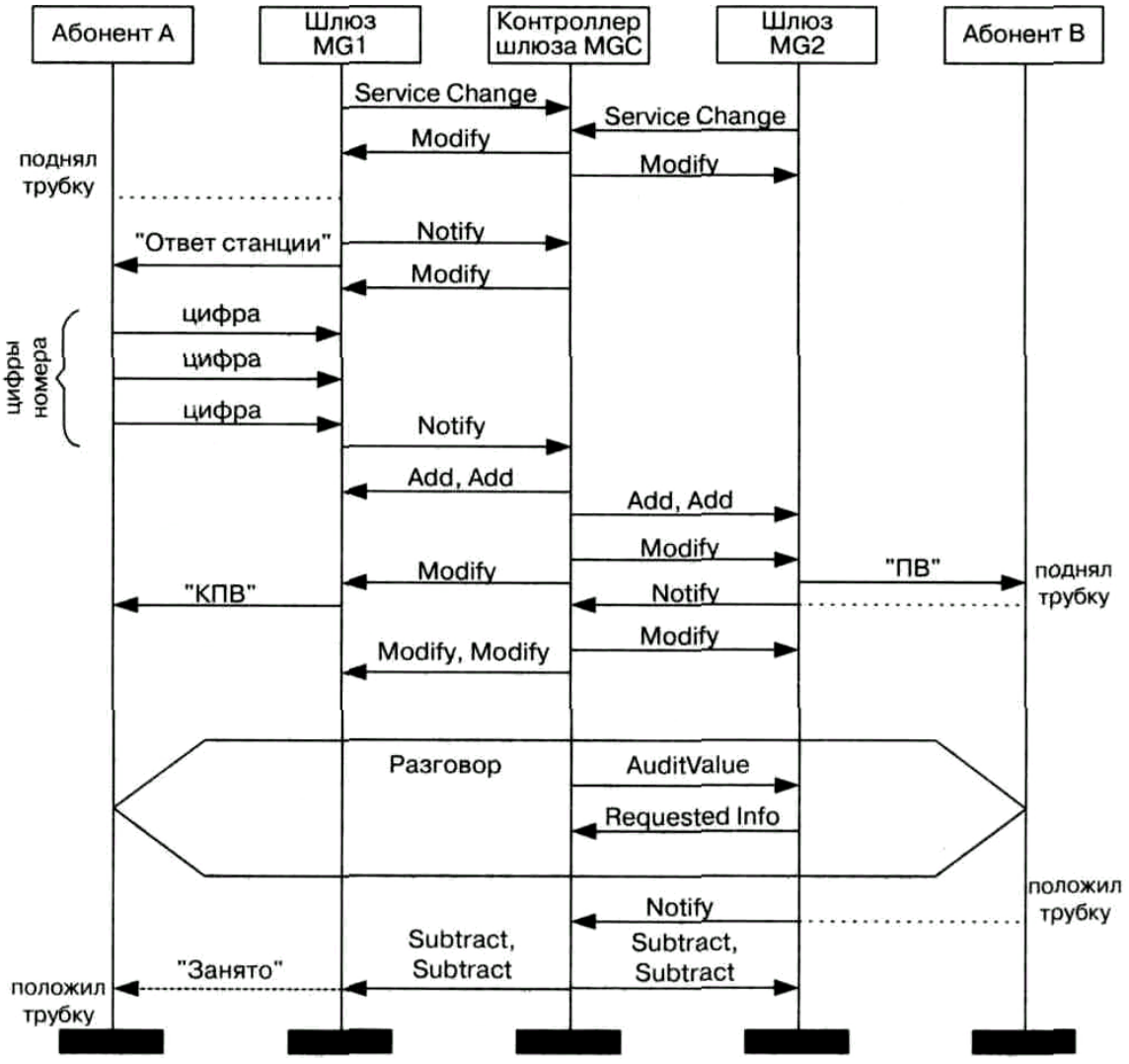


Рис.5.19. Алгоритм установления и разрушения соединения с помощью протокола MEGACO

1. Шлюз MG1 регистрируется у контроллера MGC при помощи команды ServiceChange. Использование нулевого контекста означает, что порт в настоящий момент не участвует ни в каком соединении, а использование идентификатора порта ROOT означает, что команда относится ко всему шлюзу, а не к какому-нибудь определенному порту.

2. Контроллер подтверждает регистрацию шлюза
3. Шлюз имеет свободные аналоговые порты, которые должны быть запрограммированы для отслеживания изменения сопротивления абонентского шлейфа, означающего поднятие абонентом трубки, после чего шлюз должен передать абоненту акустический сигнал «Ответ станции». Программирование производится при помощи команды Modify с соответствующими параметрами, причем программируется порт, находящийся в нулевом контексте. В команде указывается идентификатор порта (terminationid) -A4444, идентификатор информационного потока (streamid) -1, транспортный адрес оборудования, передавшего команду - [123.123.123.4] :55555, специфицируется режим функционирования - дуплексный (SendReceive).
На этом же этапе в шлюз может быть загружен план нумерации (в дескрипторе digit map). В этом случае, после того как абонент поднимет трубку, шлюз должен передать ему акустический сигнал «Ответ станции» и начинать прием сигналов DTMF в соответствии с планом нумерации. Однако в нашем примере план
нумерации будет загружен только после того, как абонент поднимет трубку, на 8 шаге.
Кроме того, следует отметить, что шаги 3 и 4 данного алгоритма могут быть совмещены с шагами 8 и 9, соответственно, при помощи дескриптора EventsDescriptor. При этом шаги 6 и 7 опускаются.
4. Шлюз MG1 подтверждает выполнение команды Modify:
5. Подобным же образом (шаги 1-4) программируется аналоговый порт шлюза MG2, в нашем примере имеющий идентификатор A5555.
6. Далее шлюз MG1 обнаруживает, что абонент А поднял трубку, и извещает об этом событии Media Gateway Controller при помощи команды Notify. mgi
7. Контроллер подтверждает получение команды Notify:
8. На следующем шаге MGC дает шлюзу инструкцию накапливать цифры номера вызываемого абонента в соответствии с выбранным планом нумерации. Кроме того, после получения первой цифры номера необходимо остановить передачу акустического сигнала «Ответ станции».
14. Контроллер MGC создает в шлюзе MG2 контекст для установления дуплексного соединения (режим SendReceive) с вызывающим пользователем.
15. Создание контекста подтверждается, физический порт шлюза MG2 A5555 соединяется с UDP/RTP портом, имеющим идентификатор A5556. Отметим, что RTP-порт имеет номер 1111, т.е. отличный от номера порта Megaco/H.248 - 55555.
16. Контроллер MGC предписывает порту A5555 шлюза MG2 начать передачу вызывного сигнала.
17. Шлюз MG2 подтверждает передачу сигнала «Посылка вызова» вызываемому абоненту.
18. Контроллер предписывает шлюзу MG1 начать передачу вызывающему абоненту акустического сигнала «Контроль посылки вызова (КПВ)».

19. Шлюз MG1 подтверждает передачу указанного акустического сигнала в порт A4444.
На этом этапе обоим абонентам, участвующим в соединении, посылаются соответствующие сигналы, и шлюз MG2 ждет, пока вызываемый абонент примет входящий вызов, после чего между двумя шлюзами будут организованы двунаправленные разговорные каналы.
20. Шлюз MG2 обнаружил, что вызываемый абонент поднял трубку, и извещает об этом контроллер MGC.
21. Контроллер подтверждает получение команды Notify.
22. Далее контроллер MGC предписывает шлюзу MG2 прекратить передачу вызывного сигнала.
23. Шлюз MG2 подтверждает выполнение команды.
24. Далее, контроллер разрешает шлюзу MG1 не только принимать, но и передавать информацию (режим SendReceive), и останавливает передачу вызывающему абоненту акустического сигнала «КПВ».
25. Шлюз MG1 подтверждает выполнение команды.
MG1 to MGC:
26. После этого начинается разговорная фаза соединения, в течение которой участники обмениваются речевой информацией. Следующим шагом контроллер MGC принимает решение проверить RTP-порт в шлюзе MG2.
27. Шлюз MG2 выполняет команду. В ответе на команду AuditValue передается вся запрашиваемая информация, в том числе статистика, собранная за время соединения. Кроме того, из ответа видно, что не произошло никаких событий и не передавалось никаких сигналов.
28. Вызываемый абонент первым завершает соединение, и шлюз MG2 извещает об этом контроллер MGC.
29. Контроллер MGC подтверждает получение сообщения Notify.
MGC to MG2:
30. Получив информацию от любого из шлюзов о том, что один из абонентов положил трубку, контроллер MGC завершает соединение. К обоим шлюзам передается команда Subtract. Алгоритм завершения соединения предусматривает одинаковый обмен сигнальными сообщениями между контроллером и обоими шлюзами, поэтому здесь этот алгоритм рассматривается на примере шлюза MG2.
31. Каждый из портов шлюза MG2, участвующих в соединении (физический порт - A5555 и RTP-порт - A5556), возвращает статистику, собранную за время соединения. В общем случае, контроллер может запрашивать статистическую информацию только у одного из портов.
32. После завершения соединения контроллер MGC предписывает шлюзам MG1 и MG2 быть готовыми к тому, что кто-то из обслуживаемых ими абонентов поднимет трубку. Портам шлюза, отображаемым окончаниями в нулевом контексте, по умолчанию может быть предписано обнаруживать, что абонент поднял трубку, при этом контроллер не передает шлюзам специальные команды, как это было показано ранее (шаг 3).

Контрольные вопросы

1. Какие из протоколов являются сигнальными протоколами сети NGN?
2. Какие из протоколов являются протоколами услуг сети NGN?
3. Что должен осуществлять программный коммутатор (Softswitch)?
4. Какой протокол является основным транспортным протоколом для мультимедийных приложений?
5. Какие типы каналов входят в пользовательский интерфейс ISDN?
6. Что такое интерфейс BRI, PRI?
7. Из каких компонентов состоит сеть доступа интерфейса V.5?
8. Что обеспечивают протоколы сигнализации?
9. На какие фазы делится процедура установления соединения?
10. Какие основные компоненты описываются рекомендации H.323?
11. Что такое зона H.323?
12. Какие функции выполняют терминал H.323, контроллер зоны, шлюз, устройство управления многоточечной конференцией?
13. Чем отличаются устройства привратник, gatekeeper, контроллер зоны?
14. Какие типы адресов используются в сети IP-телефонии стандарта H.323?
15. Каким образом стыкуется нумерация в ТфОП с адресацией в IP-сетях?
16. Какие протоколы обеспечивают кодирование/декодирование речи в сети H.323?
17. Что такое клиент SIP?
18. В каком режиме работает протокол SIP?
19. Какую функцию выполняет прокси-сервер?
20. Для чего предназначен сервер переадресации?
21. К какому уровню модели OSI можно отнести протокол SIP?
22. Какая технология используется протоколом SIP в качестве транспортной?
23. Какой тип адресации используется в протоколе SIP?
24. Какой формат сообщений и структуру имеют сообщения протокола SIP?
25. Какие существуют виды сообщений?
26. Каково назначение запросов протокола SIP?
27. Каково назначение ответов протокола SIP?
28. В чем разница двух сценариев установления соединения (с участием сервера переадресации и с участием прокси-сервера)?
29. В какие моменты времени терминалы пользователей посылают информацию о своих функциональных возможностях? В каких сообщениях эта информация располагается?
30. Какое минимальное число сообщений необходимо для установления соединения?
31. Что означает принцип декомпозиции шлюза?
32. Сколько шлюзов должно быть при протоколе MGCP?
33. Какой протокол обеспечивает перенос сообщений протокола MGCP?
34. Какие существуют виды команд MEGACO/H.248?
35. Каково назначение ответов протокола MEGACO/H.248?

6. ОБОРУДОВАНИЕ ССП

6.1. Softswitch, шлюзы, терминальное оборудование – основные характеристики и требования к ним

Основными типами оборудования, используемыми в сетях следующего поколения являются Softswitch, шлюзы, терминальное оборудование, рассмотрим основные характеристики и требования к ним.

6.1.1. Softswitch

Softswitch реализует функции по логике обработки вызова, доступу к серверам приложения, сбору статистической информации, сигнальному взаимодействию с сетью ТфОП и внутри пакетной сети, управлению установлением соединения и др.

Softswitch является основным устройством, реализующим функции уровня управления коммутацией и передачей информации. В оборудовании Softswitch должны быть реализованы следующие основные функции:

− функция управления базовым вызовом, обеспечивающая прием и

обработку сигнальной информации и реализацию действий по установлению соединения в пакетной сети;
- функция аутентификации и авторизации абонентов, подключаемых в пакетную сеть как непосредственно, так и с использованием оборудования доступа ТфОП;
- функция маршрутизации вызовов в пакетной сети;
- функция тарификации, сбора статистической информации;
- функция управления оборудованием транспортных шлюзов;
- функция предоставления ДВО (дополнительных видов обслуживания). Реализуется в оборудовании Softswitch или совместно с сервером приложений;
- функция OAM&P: эксплуатация, управление (администрирование), техническое обслуживание и предоставление той информации, которая не нужна непосредственно для управления вызовом и может передаваться к системе управления элементами через логически отдельный интерфейс;
- функция менеджмента: обеспечивает взаимодействие с системой менеджмента сети.

Дополнительно в оборудовании Softswitch могут быть реализованы следующие функции:
- функция SP STP сети ОКС7;
- функция предоставления расширенного списка ДВО. Реализуется самостоятельно или с использованием серверов приложений;
- функция взаимодействия с серверами приложений;
- функция SSP;

Основные характеристики Softswitch.

Производительность – максимальное количество обслуживаемых базовых вызовов за единицу времени (как правило, за час). Производительность Softswitch — это одна из главных характеристик, на основе которой должен проводиться выбор оборудования и проектирование сети. Следует понимать, что *Softswitch* обслуживает вызовы от различных источников нагрузки, каковыми являются:
- вызовы от терминалов, предназначенных для работы в сетях *ССП* (терминалы SIP и H.323, а также IP-УПАТС);
- вызовы от терминалов, не предназначенных для работы в сетях *ССП* (аналоговые и ISDN-терминалы) и подключаемых через оборудование *резидентных шлюзов* доступа;
- вызовы от оборудования сети доступа, не предназначенного для работы в сетях *ССП* (концентраторы с интерфейсом V5) и подключаемого через оборудование *шлюзов* доступа;
- вызовы от оборудования, использующего первичный доступ (УПАТС) и подключаемого через оборудование *шлюзов* доступа;

- вызовы от сети ТфОП, обслуживаемые с использованием сигнализации ОКС7, с включением сигнальных каналов ОКС7 либо непосредственно в *Softswitch*, либо через оборудование *сигнальных шлюзов*;
- вызовы от других *Softswitch*, обслуживаемые с использованием сигнализации SIP-T.

Производительность оборудования *Softswitch* различна при обслуживании вызовов от различных источников, что объясняется как различным объемом и характером поступления сигнальной информации от разных источников, так и заложенными алгоритмами обработки сигнальной информации. При проектировании сети *ССП*, в части возможностей *Softswitch*, важно иметь наиболее полную информацию о производительности для различных видов нагрузки, а также для смешанных типов нагрузки при различных долях каждого из видов.

Надежность – свойство объекта сохранять во времени и в установленных пределах значения всех параметров и способность выполнять требуемые функции в заданных режимах и условиях применения. Требования по надежности к оборудованию *Softswitch* характеризуются средней наработкой на отказ, средним временем восстановления, коэффициентом готовности, сроком службы. При проектировании сети следует понимать, что выход из строя *Softswitch* приведет к пропаже всех видов связи в обслуживаемом сетевом фрагменте (домене); поэтому должны быть предусмотрены меры по обеспечению дублирования и защиты оборудования.

Поддерживаемые протоколы

Оборудование *Softswitch* может поддерживать следующие виды протоколов.

1. При взаимодействии с существующими фрагментами сети ТфОП:
    - непосредственное взаимодействие: ОКС7 в части протоколов MTP, ISUP и SCCP;
    - взаимодействие через *сигнальные шлюзы*,: M2UA, M3UA, M2PA для передачи сигнализации ОКС7 через пакетную сеть;
    - V5UA для передачи сигнальной информации V5 через пакетную сеть;
    - IUA для передачи сигнальной информации первичного доступа ISDN через пакетную сеть;
    - MEGACO (H.248) для передачи информации, поступающей по системам сигнализации по выделенным сигнальным каналам (2ВСК). В настоящее время известны подобные реализации в части системы сигнализации R1; требований и примеров реализации MEGACO для поддержки российской системы сигнализации R1.5 не существует.
2. При взаимодействии с терминальным оборудованием:
    - непосредственное взаимодействие с терминальным оборудованием пакетных сетей: SIP и H.323;

- взаимодействие с оборудованием *шлюзов*, обеспечивающим подключение терминального оборудования ТфОП: MEGACO (H.248) для передачи сигнализации по аналоговым абонентским линиям; IUA для передачи сигнальной информации базового доступа ISDN.

3. При взаимодействии с другими *Softswitch*: SIP-T.
4. При взаимодействии с оборудованием интеллектуальных платформ (SCP): INAP.
5. При взаимодействии с серверами приложений: в настоящее время такое взаимодействие, как правило, базируется на внутрифирменных протоколах, в основе которых лежат технологии JAVA, XML, SIP и др.
6. При взаимодействии с оборудованием *транспортных шлюзов*:
   - для *шлюзов*, поддерживающих транспорт IP или IP/ATM: H.248, MGCP, IPDC и др.;
   - для *шлюзов*, поддерживающих транспорт ATM: BICC.

Поддерживаемые интерфейсы

Как правило, оборудование *Softswitch* поддерживает следующие виды интерфейсов:

- интерфейс E1 (2048 Кбит/с) для подключения сигнальных каналов ОКС7, включаемых непосредственно в *Softswitch*;
- интерфейсы семейства Ethernet для подключения к IP-сети. Через Ethernet-интерфейсы передается сигнальная информация в направлении пакетной сети.

6.1.2. Шлюзы (Gateways)

Шлюзы (Gateways) – устройства доступа к сети и сопряжения с существующими сетями. Оборудование *шлюзов* реализует функции по преобразованию сигнальной информации сетей с коммутацией пакетов в сигнальную информацию пакетных сетей, а также функции по преобразованию информации транспортных каналов в пакеты IP / ячейки ATM и маршрутизации пакетов IP / ячеек ATM. ***Шлюзы*** функционируют на транспортном уровне / уровне доступа.

Для реализации возможности подключения к мультисервисной сети различных видов оборудования ТфОП используются различные программные и аппаратные конфигурации *шлюзового* оборудования:

- ***транспортный шлюз (Media Gateway (MG))*** – реализация функций преобразования речевой информации в пакеты IP / ячейки ATM и маршрутизации пакетов IP / ячеек ATM;
- ***сигнальные шлюзы (Signalling Gateway (SG))*** – реализация функции преобразования систем межстанционной сигнализации сети ОКС7 (квазисвязный режим) в системы сигнализации пакетной сети (SIGTRAN (MxUA));

- ***транкинговый шлюз (Trunking Gateway (TGW))*** – совместная реализация функций MG и SG;
- ***шлюз доступа (Access Gateway (AGW))*** – реализация функции MG и SG для оборудования доступа, подключаемого через интерфейс V5;
- ***резидентный шлюз доступа (Residential Access Gateway (RAGW))*** – реализация функции подключения пользователей, использующих *терминальное оборудование* ТфОП/ЦСИС к мультисервисной сети.

Оборудование *транспортного шлюза* должно выполнять функции устройства, производящего обработку информационных потоков среды передачи.

Оборудование *транспортного шлюза* должно реализовывать следующий перечень обязательных функций:

- функцию адресации: обеспечивает присвоение адресов транспортировки IP для средства приема и передачи;
- функцию транспортировки: обеспечивает согласованную транспортировку потоков среды передачи между доменом IP и доменом сети с коммутацией каналов, включая, например, выполнение процедур преобразования кодировок и эхокомпенсации;
- функцию трансляции кодека: маршрутизирует информационные транспортные потоки между доменом IP и доменом сети с коммутацией каналов;
- функцию обеспечения секретности канала среды передачи: гарантирует секретность транспортировки информации в направлении к *шлюзу* и от *шлюза*;
- функцию транспортного окончания сети с коммутацией каналов: включает реализацию процедур всех низкоуровневых аппаратных средств и протоколов сети;
- функцию транспортного окончания сети пакетной коммутации: включает реализацию процедур всех протоколов, задействованных в распределении транспортных ресурсов, на сети пакетной коммутации, в том числе процедуры использования кодеков;
- функцию обработки транспортного потока с пакетной коммутацией / коммутацией каналов: обеспечивает преобразование между каналом передачи аудиоинформации, каналом передачи факсимильной информации или каналом передачи данных на стороне сети с коммутацией каналов и пакетами данных (например RTP/UDP/IP или ATM) на стороне сети пакетной коммутации;
- функцию предоставления канала для услуги: обеспечивает такие услуги, как передача уведомлений и тональных сигналов в направлении к сети с коммутацией каналов или к сети пакетной коммутации;
- функцию регистрации использования: определяет и/или регистрирует информацию о сигнализации и/или информацию о приеме или передаче сообщений, передаваемых в транспортных потоках;

- функцию информирования об использовании: сообщает внешнему объекту о текущем и/или зарегистрированном использовании (ресурсов);
- функцию OAM&P: эксплуатация, управление (администрирование), техническое обслуживание и предоставление той информации, которая не нужна непосредственно для управления вызовом и может передаваться к системе управления элементами через логически отдельный интерфейс;
- функцию менеджмента: обеспечивает взаимодействие с системой менеджмента сети.

Оборудование *сигнального шлюза* должно выполнять функции посредника при сигнализации между пакетной сетью и сетью с коммутацией каналов.

Оборудование *сигнального шлюза* сигнализации должно реализовывать следующий перечень обязательных функций:

- функцию окончания протоколов уровня, располагающегося ниже уровня протокола управления вызовом сети с коммутацией каналов;
- функцию секретности сигнальных сообщений: обеспечивает секретность сигнальных сообщений в направлении к *шлюзу* и от *шлюза*;
- функцию OAM&P: эксплуатация, управление (администрирование), техническое обслуживание и предоставление той информации, которая не нужна непосредственно для управления вызовом и может передаваться к системе управления элементами через логически отдельный интерфейс;
- функцию менеджмента: обеспечивает взаимодействие с системой менеджмента сети.

Основными характеристиками шлюзов являются следующие.

Емкость

Определяется как в направлении ТфОП, так и в направлении к пакетной сети. В первом случае емкость определяется количеством подключаемых потоков E1 в направлении сети ТфОП для *транспортных шлюзов*, а также количеством аналоговых абонентских линий и количеством (S,T)-интерфейсов для подключения абонентов базового доступа ISDN для резидентных *шлюзов* доступа.

В направлении к пакетной сети емкость определяется количеством и типом интерфейсов. Например, емкость в направлении пакетной сети может составлять один интерфейс Ethernet 100BaseT.

Производительность

Как правило, производительность является достаточной для обслуживания потоков вызовов, определяемых емкостными показателями оборудования.

Протоколы

Оборудование *шлюзов* может поддерживать следующие протоколы.

1. Для *транспортных шлюзов*:
    - в направлении к *Softswitch*: H.248, MGCP, IPDC для управления

вызовами при использовании транспортной технологии IP; BICC для управления вызовами при использовании транспортной технологии ATM;
- в направлении к другим *шлюзам* или терминальному оборудованию пакетной сети: RTP/RTCP при использовании транспортной технологии IP; PNNI или UNI при использовании ATM.

2. Для *сигнальных шлюзов*:
   - в направлении к сети ТфОП: в зависимости от реализации возможна поддержка уровня MTP2 или MTP3 системы сигнализации ОКС7. В первом случае *сигнальный шлюз* должен терминировать уровень MTP3 и передавать всю "вышестоящую " информацию в направлении *Softswitch* с использованием протокола M2UA. Во втором случае *сигнальный шлюз* должен терминировать уровень MTP3 и передавать "вышестоящую " информацию в направлении *Softswitch* с использованием протокола M3UA;
   - в направлении к *Softswitch*: в зависимости от используемых механизмов обработки ОКС7 могут поддерживаться M2UA или M3UA.
3. Для *шлюзов доступа*:
   - в направлении к *Softswitch* для передачи сигнальной информации, связанной с обслуживанием вызова: V5UA при подключении оборудования сети доступа: MEGACO (H.248) при подключении абонентов, использующих сигнализацию по аналоговой абонентской линии; IUA при подключении абонентов, использующих базовый доступа ISDN. Для передачи сигнальной информации управления *шлюзами*: H.248, MGCP, IPDC;
   - в направлении к другим *шлюзам* и терминальному оборудованию пакетной сети: RTP, RTCP;
   - в направлении к ТфОП: сигнализацию по аналоговым абонентским линиям, сигнализацию базового доступа ISDN в части протоколов уровня 2 (LAP-D), сигнализацию по интерфейсу V5 в части протоколов уровня 2 (LAP-V5).

Поддерживаемые интерфейсы

Как правило, оборудование *шлюзов* поддерживает следующие интерфейсы:

1. *Транспортные шлюзы*:
   - в направлении к ТфОП поддерживают интерфейсы PDH (E1) и/или SDH (STM1/4). В направлении пакетной сети на основе IP-технологий: интерфейсы Ethernet.
2. *Сигнальные шлюзы*:
   - в направлении ТфОП в основном поддерживают интерфейс PDH (E1), а в направлении пакетной сети – интерфейс 10Base Ethernet:
3. *Шлюзы доступа*:

- в направлении ТфОП поддерживают интерфейс по аналоговым абонентским линиям, интерфейсы базового доступа ISDN (U-, S-, S-T) для *резидентных шлюзов* и интерфейс PDH (E1) и *шлюзов доступа*, осуществляющих подключения оборудования интерфейса V5. В направлении пакетной сети на основе IP технологий: интерфейсы 10-100Base Ethernet. В направлении пакетной сети на основе ATM технологий: UNI.

С точки зрения технических характеристик (в пакетной части), для такого оборудования определяются требования по емкости, производительности, надежности, поддерживаемым протоколам и реализованным интерфейсам к пакетной сети.

6.1.3. Терминальное оборудование

Терминальное оборудование – терминальные устройства, используемые для предоставления голосовых и мультимедийных услуг связи и предназначенные для работы в пакетных сетях.

Существует два основных типа терминальных устройств, предназначенных для работы в пакетных сетях: SIP-терминалы и H.323-терминалы. Данное оборудование может иметь как специализированное аппаратное (standalone), так и программное исполнение (softphone).

Также иногда используется *терминальное оборудование* на основе протокола MEGACO. Такое *терминальное оборудование* совмещает в себе функции аналогового телефонного аппарата и *шлюза доступа* в части преобразования сигнализации по аналоговым абонентским линиям. Его функциональные возможности ограничиваются возможностями аналогового аппарата, но оно может непосредственно подключаться к пакетной сети.

Еще одним видом терминального оборудования являются интегрированные устройства доступа (IAD). Как правило, IAD обеспечивает подключение *терминального оборудования* сетей ТфОП (аналоговые ТА и терминалы ISDN) и терминального оборудования сетей передачи данных. В IAD реализуются функции по преобразованию протоколов сигнализации ТфОП в протоколы пакетных сетей (SIP/H.323) и преобразованию потоков пользовательской информации между сетями с коммутацией каналов и пакетными сетями. Ближайшая аналогия с IAD в сетях ТфОП — оборудование малых УПАТС.

Терминальное оборудование поддерживает протоколы SIP или H.323 в направлении *Softswitch* для передачи информации сигнализации и управления коммутацией и протоколы RTP/RTCP для передачи пользовательской информации. Для подключения к сети, как правило, применяется Ethernet-интерфейс.

6.1.4.Сервер приложений.

Сервер приложений используется для предоставления расширенного списка дополнительных услуг абонентам пакетных сетей или абонентам, получающим доступ в пакетные сети. Серверы приложений предназначены для выполнения функций уровня услуг и управления услугами.

Спецификация выполняемых функций зависит от реализуемой с помощью сервера услуги группы услуг и не может быть сформулирована на абстрактном уровне. Серверы приложений, как правило, взаимодействуют с оборудованием *Softswitch*, где задействованы технологии Java, XML, SOAP. Подключение производится в основном с использованием интерфейсов, базирующихся на Ethernet.

Рассмотрим реализацию мультипротокольной сети на базе решения U-SYS NGN компании Huawei Technologies. В соответствии с концепцией U-SYS в сети NGN используется четыре уровня, а именно уровни доступа, коммутации, управления сетью и управления услугами. Структура мультипротокольной сети представлена на рис.6.1. На уровне управления услугами в основном осуществляется предоставление дополнительных услуг, а также поддержка функционирования при установленных соединениях. Могут быть использованы следующие сервера услуг:

Интегральная Система Поддержки Эксплуатации iOSS, состоящая из двух систем: системы управления сетью (NMS) для централизованного управления сетевыми элементами МПС и интегрированной системы тарификации услуг.

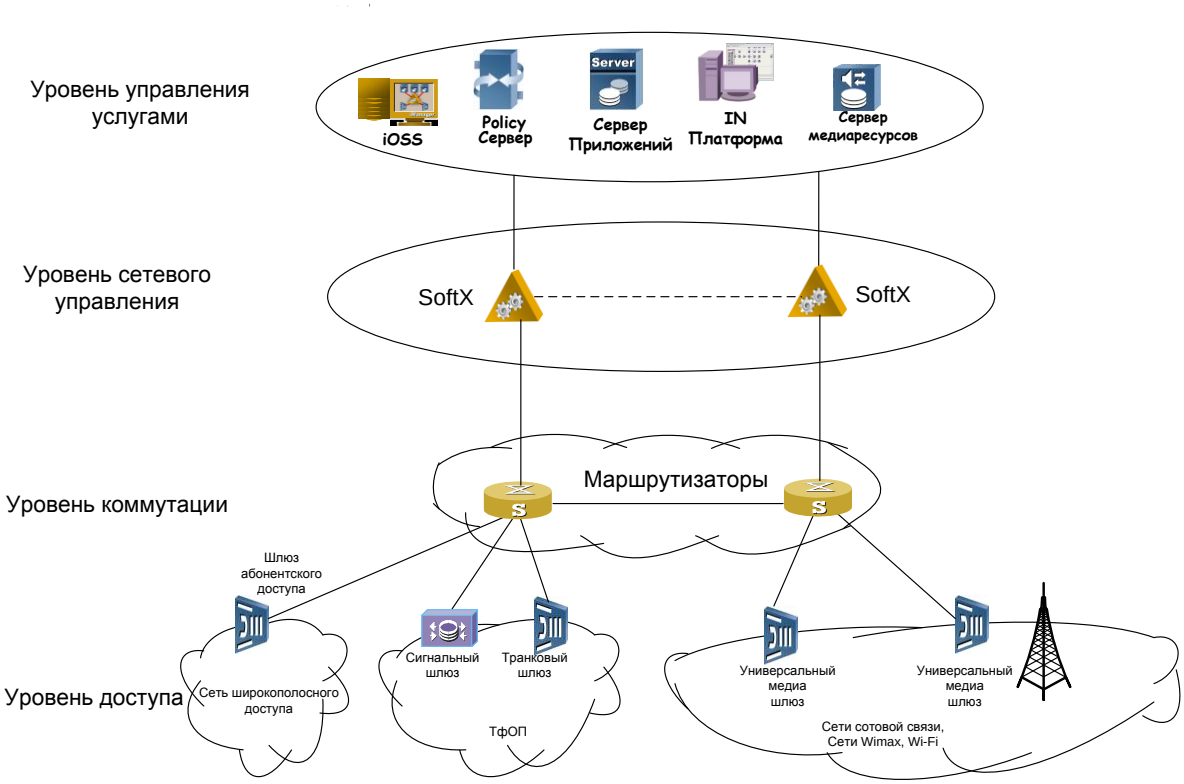


Рис.6.1. Структура мультипротокольной сети

Policy Сервер – Сервер управления – предоставлением абоненту средств связи, используется для управления предоставленными пользователю средствами связи, такими как список контроля доступа (ACL), полоса пропускания, трафик, качество обслуживания и т.д.

Сервер приложений – Application Server – используется для создания и управления логикой различных услуг с добавленной стоимостью и услуг интеллектуальной сети, а также для предоставления инновационной платформы по разработке услуг и предоставления услуг сторонних провайдеров с помощью открытых интерфейсов программируемых приложений (API). Поскольку сервер приложений является физически выделенным устройством, он независим от оборудования SoftSwitch, находящегося на уровне сетевого управления. Это обеспечивает разделение функции предоставления услуг от функции управления вызовом и содействует вводу новых услуг.

Сервер местоположения – Location Server – используется для динамического распределения маршрутов между оборудованием гибких коммутаторов SoftSwitch в сети NGN, определяет возможность установления соединений с пунктом назначения, обеспечивает лучшую эффективность использования таблицы направлений обмена за счет ее упрощения и повышения возможностей ее использования, и уменьшает усложненность маршрутов.

Сервер RADIUS (Remote Authentication Dial-In User Service) – Сервер службы аутентификации удаленных вызывающих пользователей – используется для централизованной аутентификации пользователей, шифровки пароля, выбора услуг и фильтрации, а также централизованной тарификации услуг.

Сервер медиаресурсов – MRS Server – используется для реализации функций обработки среды передачи при организации основных и усовершенствованных услуг. К данным функциям относятся следующие: обеспечение тональных сигналов услуг, услуг конференц-связи, интерактивный голосовой ответ IVR (Interactive Voice Response), услуга записанных сообщений и речевого меню.

Узел управления услугами – SCP – является основным узлом интеллектуальной сети (IN) и используется для хранения абонентских данных и логики услуг. В соответствии с поступающими вызовами, о которых сообщается узлом коммутации услуг (SSP), узел управления услугами SCP задействует соответствующую логику услуги, осуществляет поиск базы данных услуги и базы данных пользователя на основе задействованной логики услуги, и затем осуществляет посылку надлежащих команд управления вызовом в соответствующий узел коммутации услуг SSP для указания выполнения узлом SSP последующих действий, таким образом, осуществляя установление различных интеллектуальных вызовов. Это основная функция узла управления услугой SCCP.

В сети NGN весь интеллект сосредоточен на периферии, и основным требованием к сети остается обеспечение достаточной пропускной способности или широкополосность транспорта.

6.2. Мультисервисные сети Ethernet масштаба города (Metro Ethernet)

Появление и развитие гибридных сетей широкополосного доступа представляет собой типичный пример эволюционного развития технологий построения сетей доступа от узкоспециальных услуг к полнофункциональным услугам. Основной особенностью широполосных сетей кабельного телевидения (СКТ) их изначальное ориентирование на предоставление вещательных услуг. Первоначально сети широкополосного доступа применялись для трансляции программ кабельного телевидения. В качестве среды передачи данных в этих сетях использовался медный коаксиальный кабель, а телевизионный сигнал передавался по нему в аналоговом виде и в стандартном эфирном формате.

Трансляция сигнала одного телевизионного канала занимает полосу частот 8МГц, поэтому оператор кабельного телевидения может организовать одновременную трансляцию от 20 до 80 телевизионных программ. В дальнейшем, с увеличением количества абонентов, для построения магистральных сегментов своих сетей операторы кабельного телевидения стали использовать волоконно-оптический кабель (ВОК). При этом оптическая магистраль, как правило, использовалась для подключения к общей сети одной или нескольких связанных между собой коаксиальных ветвей.

Такие гибридные волоконно-оптические/коаксиальные сети, или иначе сети HFC, оказались способны передавать телевизионный сигнал на расстояние до нескольких десятков и даже сотен километров. В дальнейшем, по мере развития рынка и появления новых услуг со стороны провайдеров спутникового телевидения, операторы кабельного телевидения были вынуждены искать пути повышения качества предоставляемых услуг, а так же возможности для организации новых сервисов для своих клиентов: были предоставлены высокоскоростная передача данных и доступ в сети Интернет, используя сети HCF. Основными компонентами сети HCF являются кабельные модемы (CM) и транслирующая станция кабельных модемов (CMTS).

Растущая конкуренция на рынке телекоммуникаций заставляет операторов искать новые решения, которые позволят расширить спектр предлагаемых услуг, снизить расходы на сопровождение сети, повысить прибыльность и привлечь новых клиентов. Такие решения также должны обеспечивать хорошую масштабируемость и быть рассчитаны на быстрый рост клиентской базы и внедрение новых приложений, требующих поддержки функций качества обслуживания и значительной полосы

пропускания.

Всем этим требованиям наилучшим образом отвечает решение Metro Ethernet. Появление Metro Ethernet как серьезной альтернативы другим вариантам сетей городского масштаба обусловлено следующими факторами:

- ростом требований к полосе пропускания в связи с появлением новых типов приложений;
- высокой концентрацией абонентов в офисных и жилых зданиях;
- ростом интереса к массовому рынку домашних абонентов вследствие высокой насыщенности рынка корпоративных клиентов и падения доходности услуг на этом рынке;
- низкой стоимостью первоначальных затрат (CAPEX) и затрат на поддержку (OPEX);
- большим количеством специалистов, имеющих опыт работы с Ethernet.

Решение Metro Ethernet обеспечивает:

- мультисервисность и высокую надежность инфраструктуры, обеспечивающие поддержку соглашений об уровне обслуживания, необходимых для критичных приложений;
- низкую стоимость развертывания сети;
- исключительно низкую цену за Гбит/с;
- стандартный интерфейс с возможностью предоставления пакета услуг на одном клиентском порту (мультиплексирование сервисов);
- модульность и высокую плотность агрегации- решение рассчитано на быстрое внедрение в районах с высокой плотностью клиентов;
- отличную масштабируемость по количеству портов, производительности узлов и скорости каналов (до 80 Гбит/с);
- единую технологию, механизмы сигнализации и управления для всей сети;
- максимальную автоматизацию управления сетью и активации услуг, поддержку средств самообслуживания клиентов.

Рост требований к емкости городских сетей и успех существующих операторов Metro Ethernet ясно показывают, что данная модель предоставления телекоммуникационных услуг на базе Ethernet в городских сетях конкурентоспособна, востребована и прибыльна для операторов связи. И так же позволяет обеспечить основу для value-added сервисов, таких как IDS, хранение информации, VoIP и IPTV. Архитектура сети Metro Ethernet разработана с учетом следующих требований:

- масштабируемость;
- высокая надежность и доступность;
- поддержка качества услуг и соглашений об уровне обслуживания, необходимых для критичных бизнес-приложений, голосового трафика и широкополосного видео;
- высокая производительность;
- модульность и возможность быстрого развертывания;

- управляемость;
- поддержка наиболее полного набора услуг, как для бизнес клиентов, так и для домашних абонентов, возможность быстрого внедрения новых услуг;
- безопасность

Типовая сеть Metro Ethernet строится по трехуровневой иерархической схеме и включает ядро, уровень агрегации и уровень доступа (рис.6.2)

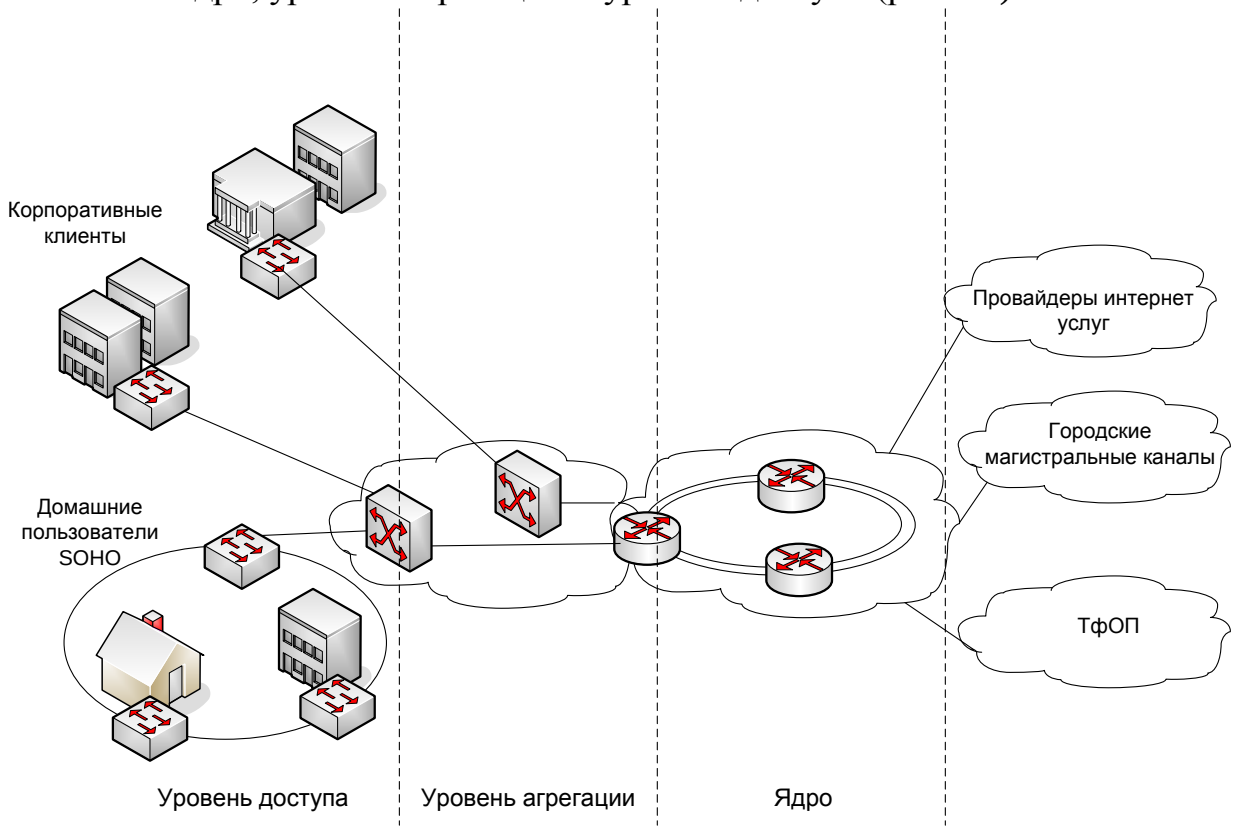


Рис.6.2. Типовая структура сети Metro Ethernet

В ядре и на уровне агрегации обеспечивается резервирование компонентов устройств, а также топологическое резервирование, что позволяет повысить доступность сети и сделать предоставление услуг непрерывным при сбоях каналов и узлов. Поддерживаемые современные механизмы резервирования (Statefull Switchover, Non-stop forwarding, Route Processor Redundancy) и защитной коммутации (Fast Reroute) обеспечивают время восстановления, сравнимое с сетями SDH и позволяют минимизировать потери трафика при сбоях на сети.

На уровне доступа реализуется полный комплекс мер безопасности, обеспечивающих идентификацию и изоляцию клиентов, а также защиту инфраструктуры оператора. В сети реализуются сквозные механизмы качества обслуживания (QoS) и поддерживаются различные типы прозрачного туннелирования клиентской QoS-маркировки трафика. На всех уровнях сети поддерживается эффективная многоадресная передача (multicast), что важно при реализации таких услуг, как телевидение поверх IP.

На начальном этапе для обеспечения передачи данных по сетям кабельного телевидения многие операторы использовали фирменные технологии, что существенно сдерживало развитие этого спектра услуг. Появление универсальной спецификации DOCSIS не только обеспечили требуемый уровень конкурентоспособности телевидения, но и заложили основу для построения будущих интерактивных мультисервисных сетей. Основные технические характеристики, регламентирующие передачу данных в системах DOCSIS, изложены в спецификациях, подготовленных некоммерческими организациями CableLabs и CableNET. В соответствии с требованиями спецификации DOCSIS сразу после включения кабельного модема он автоматически выполняет процедуру согласования параметров прямого и обратного канала с CMTS. Таким образом, использование DOCSIS при построении СКТ обеспечивает возможность создания гибридной мультисервисной сети. При этом перевод абонентов КТВ на новую схему предоставления услуг может быть выполнен постепенно, по мере приобретения ими соответствующего оборудования.

Сети беспроводного доступа долгое время использовались преимущественно для подключения мобильных абонентов к ресурсам локальной вычислительной сети или сетей общего пользования. Первые технологии беспроводной передачи данных Wi-Fi обеспечивали передачу данных на скорости несколько десятков мегабит в секунду на расстояния до 100м. Новый этап в развитии беспроводных технологий передачи данных совпал с периодом резкого повышения спроса на мультисервисные услуги. Мобильность и быстрая окупаемость увеличивают конкурентоспособность беспроводных решений при построении МСС и делают их, несомненно, очень привлекательными для операторов связи.

Мультисервисные ЛВС на основе Ethernet-технологий долгое время не рассматривались в качестве технологии передачи мультисервисного трафика. Это объяснялось тем, что технология Ethernet изначально не имела ни одного из обязательных признаков мультисервисных технологий, поскольку была разработана для обеспечения конкурентного доступа абонентов к разделяемой среде передачи данных. Однако, по мере развития и роста популярности, Ethernet постепенно приобрел все недостающие признаки мультисервисной технологии. Вследствие перехода от разделяемой к выделенной среде передачи данных - (сначала витая пара, а потом волоконно-оптический кабель) в сетях Ethernet появился полнодуплексный режим, скорость передачи данных при этом увеличилась в 1000 раз.

Постоянно растущие темпы производства компонентов сетей Ethernet вызвали резкое снижение их стоимости, что повысило привлекательность этих компонентов для потребителя. Все это в совокупности делает Ethernet одной из наиболее перспективных технологий доставки мультисервисного трафика, которая имеет большое будущее.

Для дальнейшего развития технологии, специалисты разработали спецификацию Ethernet, основанную на передачи данных по пассивной

оптической сети - EPON. Основными задачами, которые решали разработчики спецификации EPON, были:

- обеспечение симметричного полнодуплексного обмена по одному волокну оптического кабеля;
- разрешение коллизий при обращении к обратному каналу;
- интеграция трафика TDM в поток кадров Ethernet.

Специфика пассивной среды EPON заключается в том, что только один абонентский блок ONU может передавать данные, поскольку все ONU могут использовать только один обратный канал до оптического терминала ONT. Разделение ресурсов обратного канала между ONU выполняется ONT по запросам от оконечных устройств по принципу ВРК (TDM). Для реализации этого разделения между ONT и каждым ONU устанавливается взаимная синхронизация, которая обеспечивает динамическое измерение задержки распространения сигнала с точностью 16нс.

Таким образом, применение спецификации EPON позволяет создавать относительно недорогие МСС на основе технологии Ethernet. Применение пассивной оптической среды в данном случае позволяет получить дополнительные преимущества, поскольку схема передачи трафика P2MP идеально согласуется с концепцией группового (Multicast) обмена в сетях Ethernet/Интернет. Все это позволяет технологии EPON сочетать в себе главные достоинства как сети, основанной на разделяемой среде передачи данных, так и сети, построенной на выделенной среде передачи данных.

Применение технологий коммутации пакетов способно обеспечить максимальную эффективность использования пропускной способности канала передачи данных. Именно по этой причине такие технологии коммутации пакетов, как Ethernet и Интернет, которые широко используются для построения сетей передачи данных, являются привлекательными для создателей перспективных телефонных систем.

Развитие современных технологий, в частности построение МСС, приводит к тому, что видеоприложения все более глубоко проникают в различные бытовые сферы и разнообразные области человеческой деятельности. Цифровое преобразование видеосигнала обеспечивает возможность передачи видеосигнала по цифровому каналу передачи данных и повышает эффективность использования пропускной способности этого канала. Основным критерием эффективности сжатия видеоизображения является соотношение объемов данных, которые передаются оцифрованным и исходным видеосигналами. Это соотношение называется степенью сжатия (Compression Ratio). В среднем современные алгоритмы кодирования обеспечивают значения от 20 до 80 степеней сжатия видеоизображений.

Вследствие высокой популярности, разнообразные телевизионные системы, безусловно, были и остаются основной формой коммерческих видеоприложений. Самыми распространенными являются: системы, предназначенные для предоставления услуги "Видео по запросу" - VoD, которые обеспечивают абоненту возможность заказать доставку или

трансляцию выбранного видеофильма или видеопрограммы, а также системы IPTV - комплекс интернет-телевидения, в которых протоколы сети Интернет используются для трансляции телевизионных программ.

Следует отметить, что применение технологий сети Internet и Ethernet для построения МСС является далеко не бесспорным и отнюдь не безальтернативным, однако, присущая технологиям сети Интернет и Ethernet возможность масштабирования, а также постоянно растущий объем инвестиций в соответствующие области телекоммуникационной индустрии, обеспечивают возможность постоянной модернизации этих технологий и внедрения новых технических решений, расширяющих область их применения.

Построение магистральных соединений мультисервисных ЛВС на основе Ethernet. Магистральные соединения предназначены для обеспечения высокоскоростной передачи данных между узлами мультисервисных сетей. Некоторыми из наиболее существенных требований, которые предъявляются к характеристикам магистральных соединений современных МСС являются:

- скорость информационного обмена - 1-10 Гбит/сек;
- достоверность и надежность: вероятность возникновения отказа в процес¬се передачи данных по магистральному соединению - 10-9-10-12;
- автоматическая диагностика возникающих неисправностей.

В комплекс спецификаций IEEE 802.3 входят описания двух групп технологий, характеристики которых удовлетворяют большинству из перечисленных выше требований:

- группа технологий 1000 Base (Gigabit Ethernet);
- группа технологий 10G Base (lOGigabit Ethernet).

Магистрали Gigabit Ethernet обеспечивают передачу данных со скоростью 10Гбит/сек и могут быть построены на основе различных типов кабеля. В описании магистральных технологий Gigabit Ethernet можно выделить две частично независимые группы спецификаций – l000BaseX и l000BaseT.

При создании группы спецификаций l000BaseX дальнейшее развитие получили общие принципы, в соответствии с которыми построено подавляюще большинство спецификаций Ethernet. Спецификация l000BaseT представляет собой комплекс технических решений, обеспечивающих передачу данных на скорости 1Гбит/с по UTP категории 5 и является наиболее революционной среди спецификаций построения гигабитных магистралей Ethernet.

Комплекс технологий l0Gigabit Ethernet предназначен для построения сверхвысокоскоростных магистральных соединений в сетях IEEE 802.3/Ethernet, обеспечивая возможность передачи данных по магистральным соединениям ЛВС Ethernet на скорости 10Гбит/с.

Таким образом, Metro Ethernet, как среда реализации коммуникационных сервисов представляет собой технологическую базу для доставки услуг. Это понятие охватывает оптические и другие сети Ethernet в рамках масштаба города. Решения Metro Ethernet все больше становятся

основной сервисной архитектурой в городах. Операторы TV вещания все чаще и чаще при построении новой МСС комбинируют HFC и Metro Ethernet за счет наличия большого количества оптических жил в ВОК. При этом для построения СКТ используется архитектура FTTH (оптика в дом).

6.3. Технологии абонентского доступа

6.3.1. Сеть доступа и применение технологии ADSL

До недавнего времени основным способом взаимодействия оконечных пользователей с частными сетями и сетями общего пользования являлся доступ с использованием телефонной линии и модемов, устройств, обеспечивающих передачу цифровой информации по абонентским аналоговым телефонным линиям. Скорость такой связи была невелика, максимальная скорость может достигать 56кбит/с. Этого достаточно для доступа в Интернет, однако насыщение страниц графикой и видео, большие объемы электронной почты и документов в ближайшее время снова поставит вопрос о путях дальнейшего увеличения пропускной способности.

Наиболее перспективной в настоящее время является технология ADSL (Asymmetric Digital Subscriber Line) – модемная технология, превращающая стандартные абонентские телефонные аналоговые линии в линии высокоскоростного доступа. Технология ADSL позволяет передавать информацию к абоненту со скоростью до 6Мбит/с. В обратном направлении используется скорость до 640кбит/с. Это связанно с тем, что все современный спектр сетевых услуг предполагает весьма незначительную скорость передачи от абонента. Например, для получения видеофоильмов в формате MPEG-1 необходима полоса пропускания 1,5 Мбит/с. Для служебной информации передаваемой от абонента, вполне достаточно 64-128кбит/с (см. рис.6.3).

Услуга ADSL (см. рис.6.4) организуется с помощью модема ADSL, и стойки модемов ADSL, называемой DSL Access Module. Практически все DSLAM оснащаются портом Ethernet 10Base-T. Это позволяет использовать на узлах доступа обычные концентраторы, коммутаторы и маршрутизаторы.
Ряд производителей начали снабжать DSLAM интерфейсами ATM, что позволяет напрямую подключать их к ATM-коммутаторам территориально-распределенных сетей. Также ряд производителей создают пользовательские модемы, которые представляют собой ADSL модем, но для программного обеспечения являются адаптерами ATM.

На участке между ADSL модемом и DSLAM функционируют три потока: высокоскоростной поток к абоненту, двунаправленный служебный и речевой канал в стандартном диапазоне частот канала ТЧ (0,3-3,4 Кгц). Частотные разделители (*POTS Splitter*) выделяют телефонный поток, и

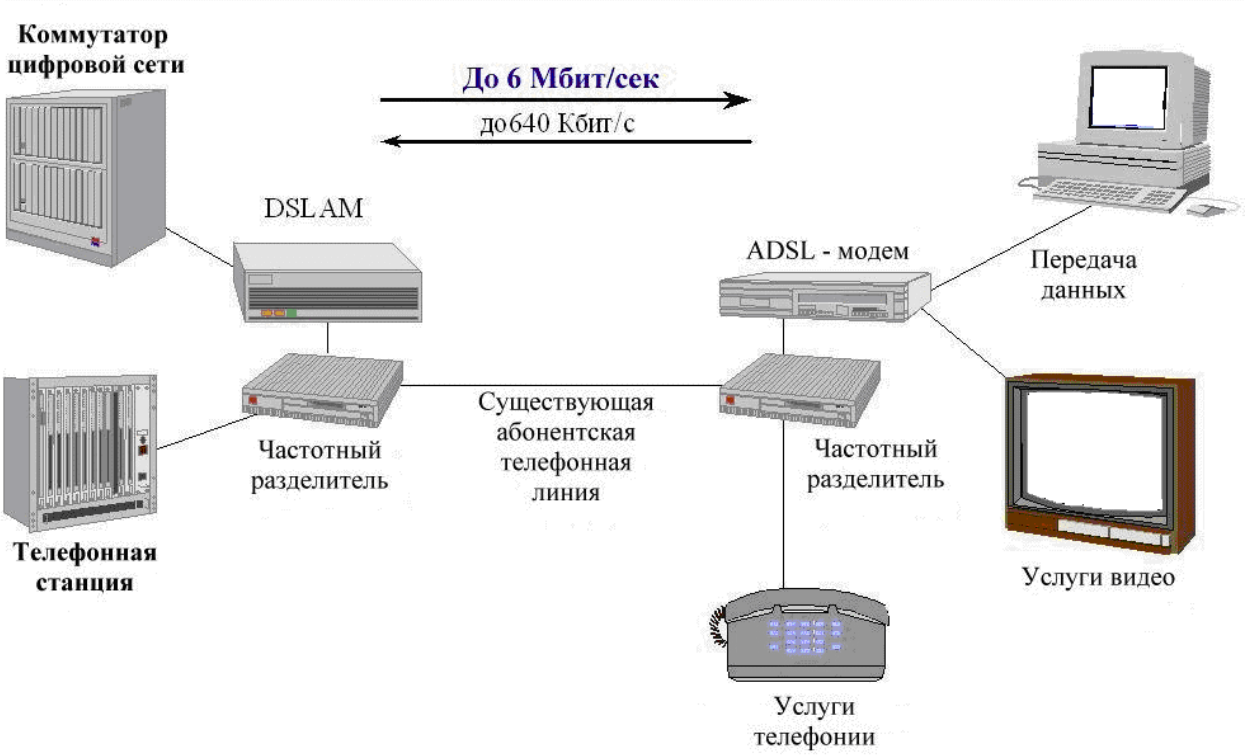


Рис.6.3. Структурная схема технологии ADSL.

направляют его к обычному телефонному аппарату. Такая схема позволяет разговаривать по телефону одновременно с передачей информации и пользоваться телефонной связью в случае неисправности оборудования ADSL. Конструктивно телефонный разделитель представляет собой частотный фильтр, который может быть как интегрирован в модем ADSL, так и быть самостоятельным устройством. В Приложении 1 приведена схема ADSL сплиттера фирмы Siemens и его частотная характеристика на его выходных портах (LINE-POTS, LINE-NT).

Согласно теореме Шеннона, невозможно с помощью модемов достичь скоростей выше 33,6кбит/с. В ADSL технологии цифровая информация передается вне диапазона частот стандартного канала ТЧ. Это приведет к тому, что фильтры, установленные на телефонной станции отсекут частоту выше 4 кГц, поэтому необходимо на каждой телефонной станции установить оборудование доступа к территориально-распределенным сетям (коммутатор или маршрутизатор).

Передача к абоненту осуществляется на скоростях от 1,5 до 6,1 Мбит/с, скорость служебного канала составляет от 15 до 640 Кбит/с. Каждый канал может быть разделен на несколько логических низкоскоростных каналов.

Скорости, предоставляемые модемами ADSL кратны скоростям цифровых каналов T1, E1. В минимальной конфигурации передача ведется на скорости 1,5 или 2,0 Мбит/с. В принципе, сегодня существуют устройства, передающие данные со скоростью до 8 Мбит/с, однако в стандартах такая

скорость не определена. Скорость модемов ADSL в зависимости от числа каналов приведена в таблице 6.1.

Таблица 6.1.

Зависимость скорости модемов ADSL от числа каналов

Базовая скорость	Количество каналов	Скорость
1,536 Мбит/с	1	1,536 Мбит/с
1,536 Мбит/с	2	3,072 Мбит/с
1,536 Мбит/с	3	4,608 Мбит/с
1,536 Мбит/с	4	6,144 Мбит/с
2,048 Мбит/с	1	2,048 Мбит/с
2,048 Мбит/с	2	4,096 Мбит/с
2,048 Мбит/с	3	6,144 Мбит/с

Максимально возможная скорость линии зависит от ряда факторов, включающих длину линии и толщину телефонного кабеля. Характеристики линии ухудшаются с увеличением его длины и уменьшении сечения провода. В таблице 6.2 показаны несколько вариантов зависимости скорости от параметров линии.

Таблица 6.2.

Зависимость скорости передачи ADSL модема от параметров линии

Длина линии (км)	Сечение провода (мм2)	Максимальная скорость (Мбит/с)
2,7	0,4	6,1
3,7	0,5	6,1
4,6	0,4	1,5 или 2
5,5	0,5	1,5 или 2

ADSL-модем представляет собой устройство, построенное на базе цифрового сигнального процессора (ЦСП или DSP), аналогичное применяемому в обычных модемах (см. рис.6.4). В общем случае, вся пропускная способность линии делится на два участка. Первый участок предназначен для передачи голоса, и находится в диапазоне 0,3-3,4 КГц. Диапазон сигнала для передачи данных лежит в пределах от 4 Кгц до 1 Мгц. Физические параметры большинства линий не позволяют передавать данные с частотой свыше 1МГц. К сожалению не все существующие телефонные линии (особенно большой протяженности), имеют даже такие характеристики, поэтому приходится уменьшать полосу пропускания, что влечет за собой уменьшение скорости передачи.

Для создания этих потоков используются два метода: метод с частотным разделением каналов и метод эхо компенсации.

Метод с частотным разделением состоит в том, что каждому из потоков

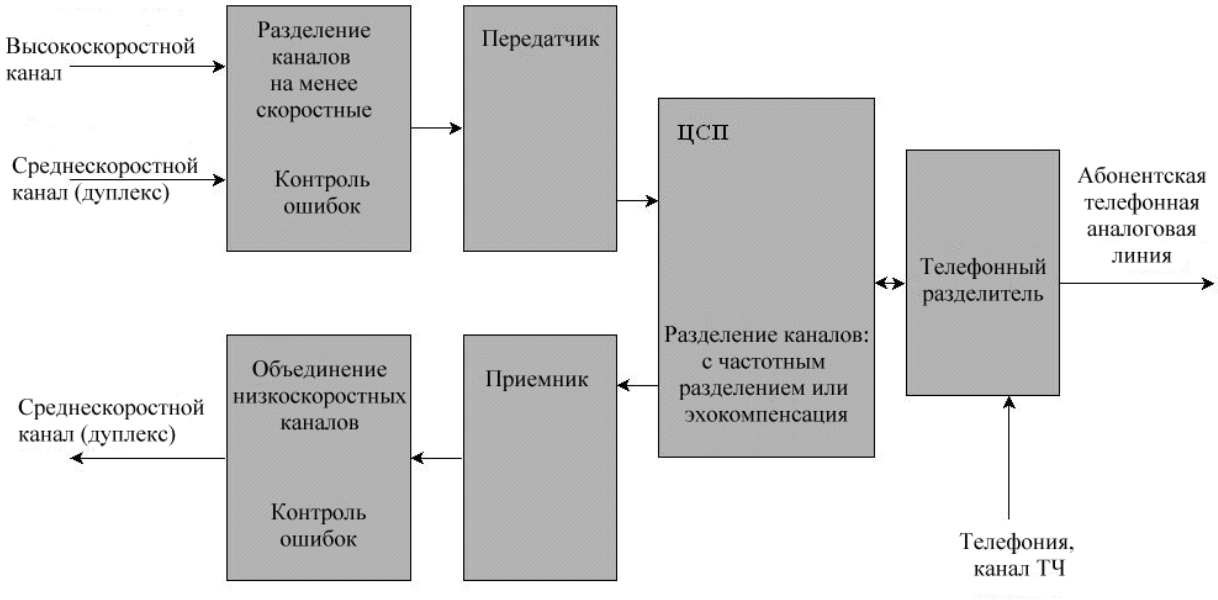


Рис.6.4. Структурная схема передающего узла ADSL модема

выделяется своя полоса пропускания частот. Высокоскоростной поток может разделяться на один или более низкоскоростных потоков. Передача этих потоков осуществляется методом "дискретной многотональной модуляции" (DMT).

Метод эхо компенсации состоит в том, что диапазоны высокоскоростного и служебного потоков накладываются друг на друга. Разделение потоков осуществляется с помощью дифференциальной системы, встроенной в модем. Этот способ используется в работе современных модемов V.32 и V.34. Высокоскоростной поток может разделяться на один или более низкоскоростных потоков Передача этих потоков осуществляется методом "дискретной многотональной модуляции" (DMT).

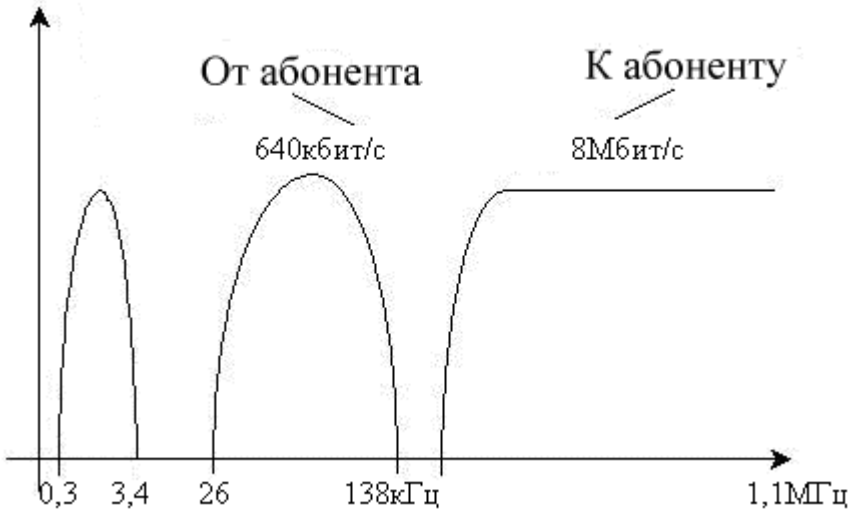


Рис.6.5. Мультиплексирование с частотным разделением

При передаче множества потоков происходит разделение каждого из них на блоки. Каждый блок снабжается кодом исправления ошибок (ECC). Схема организации выделенного канала по технологии ADSL приведена на рис.6.6.

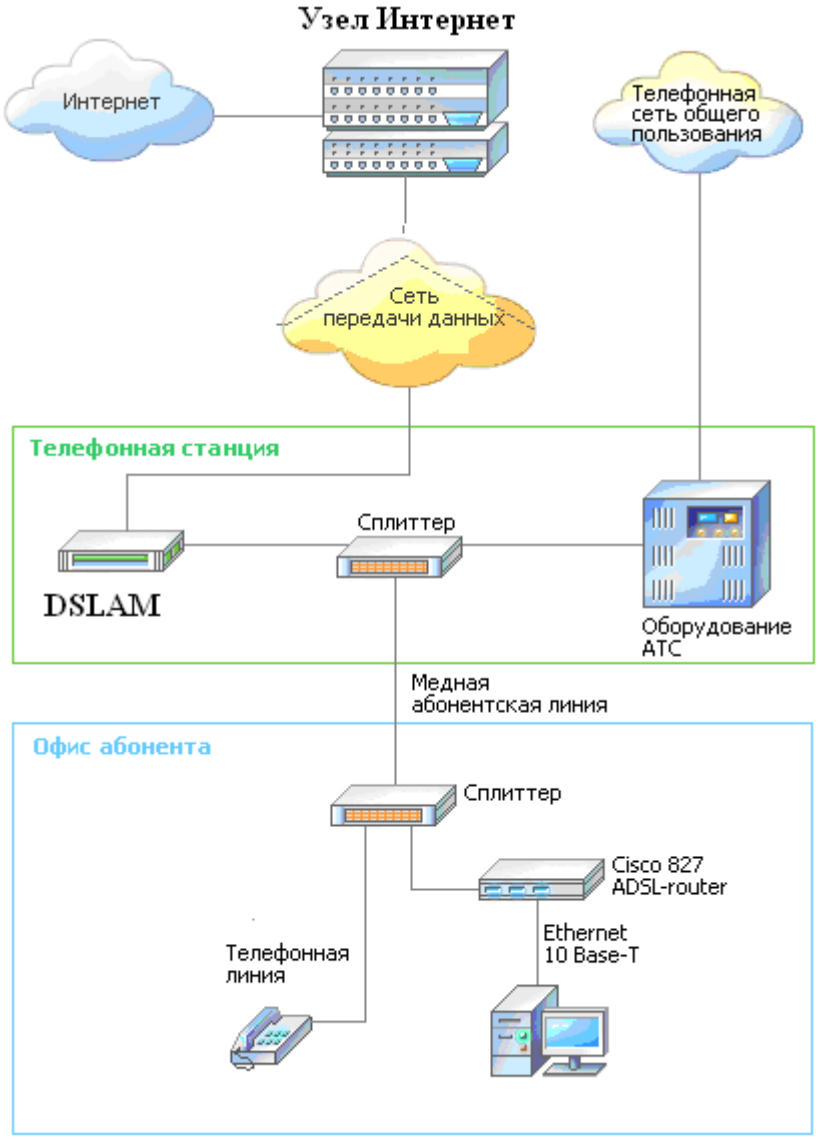


Рис.6.6. Схема организации выделенного канала по технологии ADSL

6.3.2. Семейство технологий xDSL

xDSL (ADSL, RDSL, SDSL, HDSL) x DSL представляет собой семейство технологий, позволяющих организовывать для абонентов высокоскоростные каналы доступа.

В аббревиатуре xDSL символ "x" используется для обозначения первого символа в названии конкретной технологии, а DSL обозначает цифровую абонентскую линию DSL (Digital Subscriber Line). Технологии x DSL позволяет передавать данные на скоростях от 64кбит/с до 8Мбит/с.

Многие технологии x DSL дают возможность совмещать высокоскоростную передачу данных и передачу голоса по одной и той же медной паре

Существующие типы технологий x DSL, различаются в основном по используемой форме модуляции и скорости передачи данных.

Технологии xDSL являются наиболее практичным решением, направленным на максимальное увеличение объема данных, передаваемых по существующим телефонным линиям. Использование технологий xDSL для высокоскоростного доступа особенно примечательно тем, что эти технологии используют в качестве среды передачи существующую кабельную инфрастуктуру местных телефонных сетей. Это позволяет провайдерам услуг экономить значительные средства и более быстро (и по разумной цене) создавать для своих абонентов большое количество новых услуг.

В семейство технологий xDSL входят следующие технологии: HDSL, SDSL, ADSL, RDSL и т.д., так же к технологиям xDSL можно отнести организации цифрового канала по технологии LRE (Long Reach Ethernet).
В таблице 6.2 приведены основные характеристики (скорость и дальность) современных технологий передачи данных по медной паре.

Таблица 6.2.

Скорость и дальность передачи данных по медной паре в зависимости от вида технологии

Технология	Скорость «вниз»	Расстояние	Режим
DS1 (T1)	1,544 Мбит/с	5,5 км (1)	Симметричный
E1	2,048 Мбит/с	5 км	Симметричный
DSL	160 кбит/с	5,5 км	Симметричный
HDSL	2,048 Мбит/с (2)	4 км	Симметричный
SDSL	2,048 Мбит/с	3,6 км	Симметричный
ADSL	8 Мбит/с	1,8 км (3)	Асимметричный
	128 кбит/с	8 км (3)	
VDSL (1/4 STS-1)	12,96 Мбит/с	1,5 км (3)	Асимметричный (4)
VDSL (1/2 STS-1)	25,82 Мбит/с	1 км (3)	Асимметричный (4)
VDSL (STS-1)	51, 84 Мбит/с	300 м (3)	Асимметричный (4)

Примечания:
(1) при использовании репитеров
(2) 1,544Мбит/с по двум парам, 2,048Мбит/с по трём парам
(3) скорость выбирается автоматически в зависимости от длины линии
(4) в будущем возможен симметричный VDSL, но на меньшей скорости

6.3.3. Сравнение характеристик оптических структур доступа

Сценарии развертывания FTTx можно перечислить, комбинируя три

параметра архитектуры FTTx: положение точки "x", технология доставки данных в оптической сети агрегации/распределения до точки "x" и технология доступа после точки "x".

Соответственно до точки "x" используется активный Ethernet или какая-либо из разновидностей PON; после точки "x", как правило, xDSL, Ethernet или DOCSIS по медному кабелю, иногда беспроводной доступ (Wi-Fi). На оптическом участке также возможно применение технологий спектрального уплотнения (в частности, CWDM) для увеличения пропускной способности и/или уменьшения количества волокон.

Сама точка "x" расположена либо у абонента, либо между абонентом и помещением узла связи оператора (подъезд дома, уличный шкаф и др.) (см.рис.6.7).

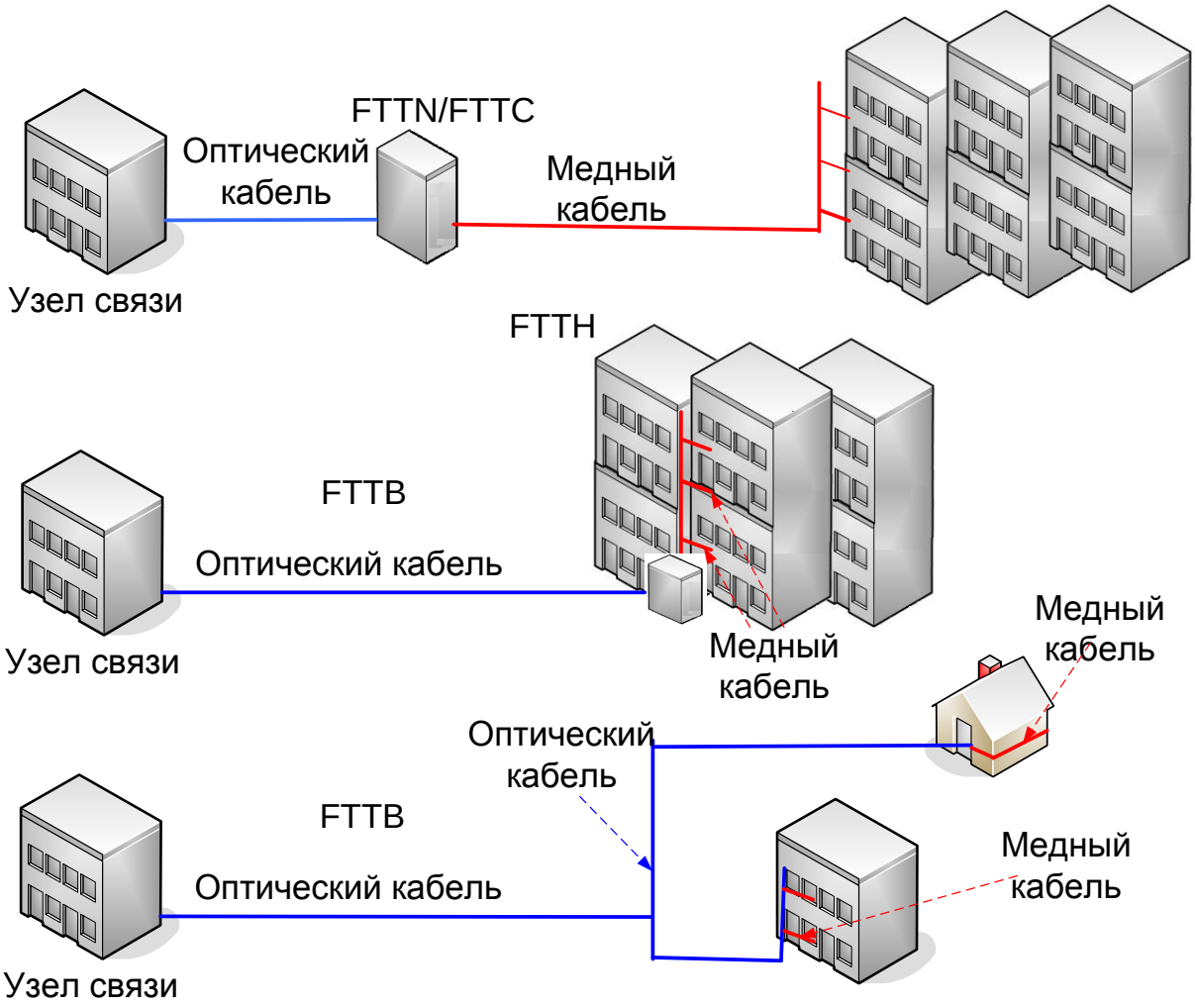


Рис.6.7. Варианты построения сетей FTTx

Использование этой архитектуры операторами фиксированного доступа обеспечивает им расширенные возможности по предоставлению услуг и повышению конкурентоспособности.

Использование оптического волокна - наиболее перспективная технология из ныне существующих, она позволяет модернизировать сеть так, чтобы можно было менять лишь оконечное передающее оборудование. Запас внутренних возможностей оптического волокна по пропускной способности еще не скоро достигнет своего предела, в отличие от эфирной передачи, передачи по медной паре и других технологий.

На сегодняшний день тенденции развития существующих сетей свидетельствует о наличии у операторов связи трех основных задач:

- предложение широкополосного доступа в новых зонах обслуживания;
- модернизация существующих сетей широкополосного доступа с целью повышения скорости передачи и предложения новых услуг, таких как IP-ТВ, VoD, HD и других аудиовизуальных приложений;
- защита от ухудшения качества услуг широкополосного доступа по мере роста плотности проникновения DSL вследствие взаимного электромагнитного влияния цепей в медном кабеле.

В течение нескольких лет услуги, в которых нуждаются пользователи, приблизили предложение операторов вплотную к границе в 100Мбит/с. Использовавшиеся до сих пор технологии DSL-доступа больше не в состоянии удовлетворить такие запросы.

Риски развертывания определяются двумя параметрами: процентом пользователей ШПД и рыночной долей конкретного оператора. Например, если в здании из 60 домохозяйств широкополосным доступом пользуются 50%, а рыночная доля оператора 40%, то он может рассчитывать на 12 домохозяйств [2]. Риски развертывания понижаются по мере отдаления вновь создаваемого узла инфраструктуры от конечного пользователя.

Наиболее низкий их уровень присущ архитектуре FTTC (Fiber to the Curb; оптоволокно до распределительного шкафа), в которой большая группа абонентов может обслуживаться одним вновь создаваемым узлом.

Если оператор стоит перед дилеммой: строить новую сеть доступа FTTH или модернизировать существующую инфраструктуру, то ему стоит обратить пристальное внимание на архитектуру FTTC (табл.6.4).

Главными преимуществами FTTC являются:

- снижение требуемого объема инвестиций (CAPEX);
- отсутствие работ по внутридомовой и внутриквартирной проводке;
- быстрое развертывание услуг с широкой полосой пропускания;
- поддержка дистанционного питания ТА.
- архитектура FTTC позволяет быстро модернизировать существующую инфраструктуру и обеспечивать удовлетворение запросов самых требовательных пользователей, не “вторгаясь” в жилище.
- общеизвестен факт, что последние 100м кабеля требуют наибольших усилий и времени на прокладку. В большинстве случаев затраты на этот отрезок линии связи составляют до 50% общей стоимости распределительной сети.

Таблица 6.4.

Сравнение характеристик оптических архитектур доступа

	FTTC /VDSL2	FTTB /VDSL2	FTTB /ETTH	FTTH /P2P	FTTH /GPON
Инвестиции (CAPEX)	~ 200 евро	~ 300 евро	150 евро	500 - 2000 евро	500 -2000 евро
Эксплуатационные расходы (OPEX)	Средние	Средние	Высокие	Низкие	Низкие
Время реализации	Быстро	Среднее	Среднее	Медленно	Медленно
Скорость передачи	↓30— 60 Мбит/с ↑4—30 Мбит/с	↓50—100 Мбит/с ↑30—100 Мбит/с	↓100 Мбит/с ↑100 Мбит/с	↓↑100Мбит/с или 1Гбит/с	↓↑ ~ 50 — 150 Мбит/с
Предпочтительная зона обслуживания	город/пригород/ село	город	город (много-этажная застройка)	город/ пригород	город (много-этажная застройка)
Дистанционное питание ТА	да	нет	да/нет	нет	нет
Риски развертывания (применительно к CAPEX)	Низкие	Средние/ высокие	Высокие	Средние/ высокие	Средние/ высокие

Архитектура FTTC в первую очередь предназначена для операторов, уже использующих технологии xDSL или PON: реализация этой архитектуры позволит им с меньшими затратами увеличить и число обслуживаемых пользователей, и выделяемую каждому из них полосу пропускания.

Комбинирование технологий доступа по оптоволоконным и медным линиям применяется совместно, когда необходимо обеспечить высокую пропускную способность и оптимальный по стоимости доступ для домашних или корпоративных пользователей. Гибридный комбинированный доступ – «оптоволокно до распределительного шкафа» и технология xDSL – является превосходным вариантом для предоставления услуг с использованием существующих медных линий от ближнего уличного шкафа.

6.3.5. Пример реализации FTTC

Различные компании-производители телекоммуникационного оборудования, представленные ны рынке телекоммуникационных узлуг Республики Узбекистан (Huawei, ZTE, Iskratel, Teledata) предлагают сходные типовые решения по гибридному доступу «оптоволокно-медь».

Рассмотрим решение компании Iskratel для сценариев «оптоволокно до распределительного шкафа» и «оптоволокно до здания» [3]:

- FTTC с использованием технологии VDSL2 для модернизации существующих подключений домашних и бизнес-абонентов с высокими требованиями к пропускной способности сети.
- FTTC с ADSL2+ для модернизации существующих подключений домашних абонентов.
- FTTC с POTS для перехода прежних аналоговых (POTS) абонентов в сети на основе VoIP.
- FTTC с комбинированным доступом (POTS и ADSL2+) для нацеленных на будущее развитие и пригодных к модернизации подключений для голосовой связи или DSL-подключений.
- FTTB с VDSL2 для абонентских подключений со сверхвысокой пропускной способностью в многоквартирных домах старой постройки.
- FTTB с ADSL2+ для модернизации существующих подключений домашних абонентов внутри зданий.
- FTTB с POTS для перехода прежних аналоговых (POTS) абонентов в сети на основе IP.
- FTTB с комбинированным доступом для нацеленных на будущее развитие и пригодных к модернизации подключений для голосовой связи.
- FTTB с Ethernet (ETTH) – доступ, объединенный с Ethernet, для зданий новой постройки с UTP-проводкой.

Вариант "FTTC с VDSL2" (см.рис.6.9), обеспечивает скорость передачи данных до 100Мбит/с (на расстоянии до 1км) для отдельного подключения конечного пользователя. Такая пропускная способность позволяет

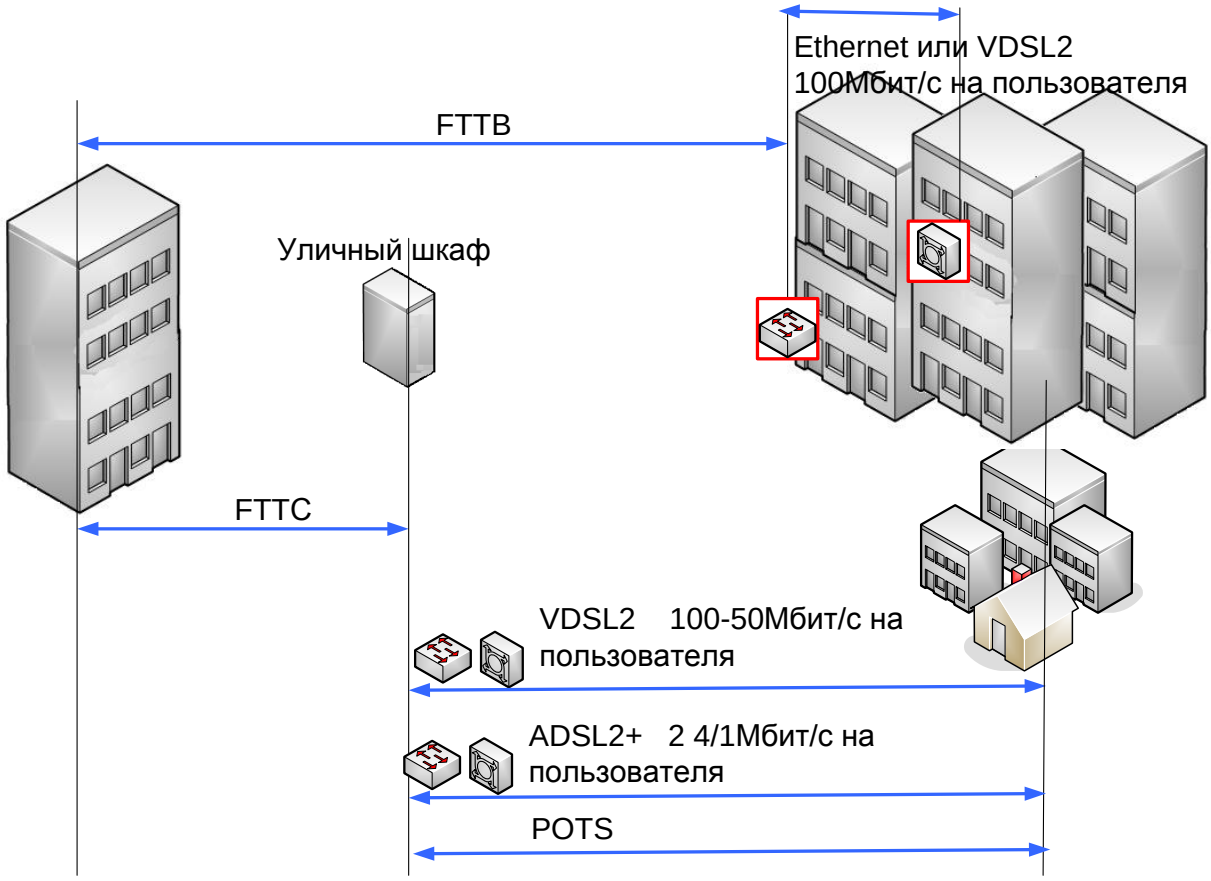


Рис.6.8. Решения Iskratel FTTC/B по гибридному доступу "оптоволокно-медь"

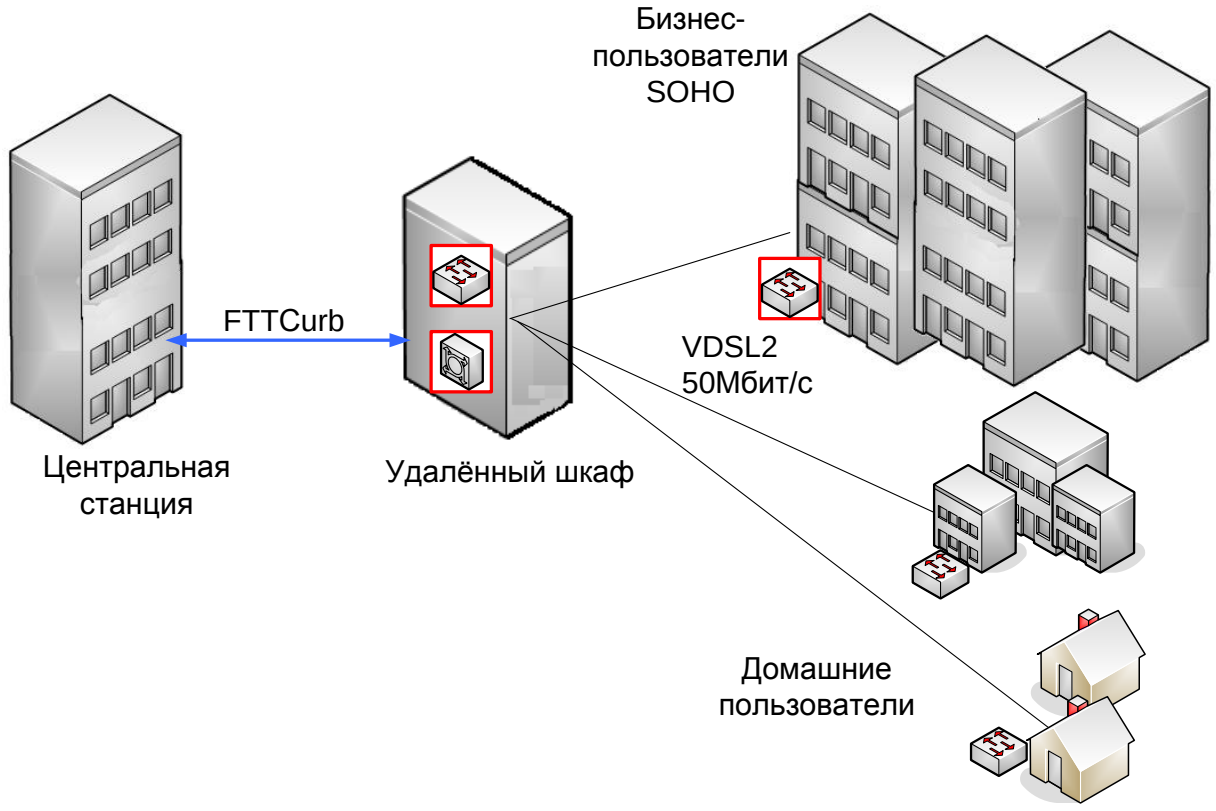


Рис.6.9. Вариант FTTC с VDSL2

предложить полную услугу Triple Play в этом варианте доступа с использованием существующей проводки на последней миле.

Вариант "FTTC+VDSL2" является оптимальным техническим решением по доступу для домашних и бизнес-пользователей SOHO, нуждающихся в высокой пропускной способности и уже подключенных к узкополосной сети (аналоговой телефонной сети или ISDN) по существующим медным линиям. Техническое решение по гибридному доступу позволяет модернизировать существующую узкополосную сеть для создания линий передачи данных с высокой пропускной способностью.

Абоненты подключаются к узлу доступа SI3000 Lumia или SI3000 MSAN, который размещается в находящемся неподалеку уличном шкафу (расстояние обычно не превышает 1км). Узел доступа, размещенный в защитном контейнере внешнего исполнения и оборудованный платами абонентских линий Iskratel VDSL2, соединяется с центральной станцией сетевого оператора по оптоволоконной линии восходящего направления.

Для обслуживания абонентов на небольших территориях Iskratel предлагает шкафы ODU-S меньшего размера. Длина абонентского шлейфа в этом случае не превышает 1км. На таком небольшом расстоянии максимальная скорость передачи достигает 100Мбит/с в нисходящем направлении и 50Мбит/с в восходящем направлении. Уменьшение расстояния между защитным контейнером и абонентом приводит к уменьшению требуемой пропускной способности для связи с защитным контейнером.

Для реализации варианта "FTTC+VDSL2" требуемыми сетевыми элементами являются:

- центральная станция -SI3000 Lumia или SI3000 MSAN с платами Giga Fiber;
- удаленный шкаф- SI3000 Lumia или SI3000 MSAN с платами VDSL2;
- защитный контейнер ODU-M (SI3000 Lumia или SI3000 MSAN в корпусе MEA 20);
- защитный контейнер ODU-S (SI3000 Lumia или SI3000 MSAN в корпусе MEA 10);
- домашний шлюз Innbox V35 для подключения пользователей.

Емкость одного защитного контейнера ODU-M составляет макс. 576 линий ADSL2+/VDSL2 со сплиттерами или 1056 аналоговых абонентских линий. Полностью укомплектованный защитный контейнер ODU-S позволяет подключить до 128 линий VDSL2, 192 линий ADSL2+ или 576 аналоговых абонентских линий. Электропитание - MPS 1000.50 для защитного контейнера ODU-M, MPS 1000.25 для защитного контейнера ODU-S. RPS- система дистанционного электропитания.

Домашний шлюз VDSL2 Home Gateway Proteus932N поддерживает доставку всех услуг Triple Play, а именно: передачу данных через Интернет, передачу голоса поверх IP (Voice over IP; VoIP) и передачу IP-видео, включая ресурсоемкую передачу HDTV. Для оконечных устройств с поддержкой

передачи пакетов этот шлюз предоставляет шесть портов Ethernet, включая гигабитный, а также точку беспроводного доступа 802.11N последнего поколения. Также имеется два порта для телефонных услуг, использующие технологию «Voice-over-IP», которые совместимы со средой серверов, работающих по протоколу SIP. Со встроенным брандмауэром и технологией «IP sharing» этот домашний шлюз обеспечивает надежный широкополосный доступ в Интернет, совместно используемый всеми подключенными клиентами. Доступны два хост-порта USB2.0, позволяющие предоставлять функции с добавленной стоимостью, такин как файловый сервер, FTP сервер, принтерный сервер или хаб.

Вариант "FTTC с ADSL2+" (см.рис.6.10) обеспечивает широкополосную связность на больших расстояниях [3]. При использовании технологии

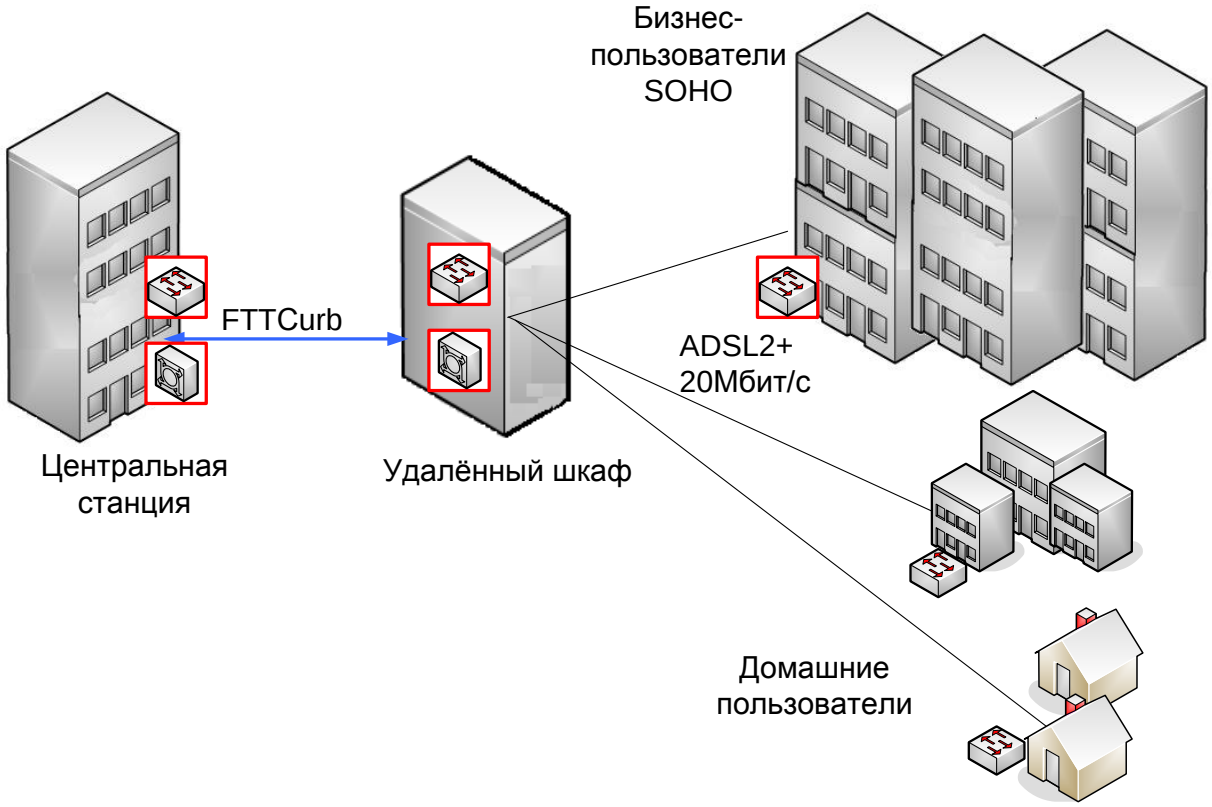


Рис.6.10. Вариант FTTC с ADSL2+

доступа ADSL2+ оператор может подключать абонентов на расстоянии до 5км и обеспечивать скорость передачи данных до 20Мбит/с в нисходящем направлении на меньшем расстоянии. Достоинствами "FTTC с ADSL2+" являются:

- эволюция широкополосного доступа – "естественный вариант" модернизации коммутируемого доступа;
- надежное решение в случае сомнительного качества медной проводки;
- отработанная, стандартизированная, полностью функционально совместимая и малозатратная технология.

Вариант "FTTC с ADSL2+" особенно подходит для районов с рассредоточенной абонентской базой для быстрого внедрения широкополосного доступа в городских, пригородных и сельских районах.

Узел доступа Iskratel SI3000 MSAN, оборудованный платами ADSL2+, обеспечивает потоковую передачу нескольких телевизионных каналов высокой четкости в абонентский порт, т.е. плата ADSL2+ позволяет передавать минимум 2 телеканала высокой четкости в один порт DSL для каждого абонента, подключенного к данной плате, гарантируя все необходимые параметры качества (QoS) и безопасности. Требуемыми сетевыми элементами являются:

- центральная станция-SI3000 Lumia или SI3000 MSAN с платами Giga Fiber;
- удаленный шкаф -SI3000 MSAN с платами ADSL2+.
- защитный контейнер ODU-M (SI3000 MSAN в корпусе MEA 20).
- защитный контейнер ODU-S (SI3000 MSAN в корпусе MEA 10 или в меньшем корпусе). Электропитание -MPS 1000.50 для защитного контейнера ODU-M. MPS 1000.25 для защитного контейнера ODU-S. RPS.
- домашний шлюз Innbox E40 для подключения пользователей.

В едином устройстве домашнего шлюза Home Gateway Innbox E40 с поддержкой Triple-Play объединены IP-маршрутизатор и механизм организации домашней сети. При использовании домашнего шлюза поставщики услуг могут предлагать подключения WAN со скоростью передачи до 24Мбит/с в нисходящем направлении и до 3Мбит/с в восходящем направлении с применением различных профилей частотного спектра ADSL2+. Устройство Innbox E40 может использоваться в технических решениях для домашних абонентов и SOHO для предоставления необходимой пропускной способности на более протяженных абонентских шлейфах. Устройство Innbox E40, также как домашний шлюз VDSL2 Home Gateway Proteus932N поддерживает доставку всех услуг Triple Play.

Вариант FTTC+POTS используется для поддержки голосовой телефонии. Существуют три типичные ситуации, при которых сетевые операторы должны сделать выбор в пользу внедрения FTTC+POTS, а именно:

1. Внедрение технического решения "FTTC+POTS" используется как средство миграции для абонентов ТфОП. Это решение позволяет очень экономично модернизировать инфраструктурные сетевые элементы и перейти к IP-связности по завершении жизненного цикла технологии TDM.
2. У многих сетевых операторов по-прежнему существует значительная доля абонентов, не желающих переходить на технологии широкополосного доступа. В таком сценарии техническое решение "FTTC+POTS", реализуемое на основе программного коммутатора Iskratel SI3000 CS, действует в качестве подмены сети TDM.
3. Использование аналоговой абонентской линии по-прежнему является

наиболее экономичным способом создания абонентского подключения с функциональностью линии бесперебойной связи (lifeline), имеющей 24-часовое резервное батарейное питание в защитном контейнере (при этом отсутствуют сложности, связанные с заменой батареи, как в случае VoIP в широкополосном доступе).

Вариант "FTTC+POTS" является самым оптимальным решением по доступу на основе IP в случае, когда, по крайней мере, один домашний абонент голосовой связи хочет сохранить существующее аналоговое подключение и аналоговые телефонные аппараты. Путем реализации технического решения по доступу "FTTC+POTS", сетевой оператор устраняет проблему необходимости поддержания старой TDM-станции.

Абоненты подключаются к узлу доступа SI3000 MSAN, который размещается в находящемся неподалеку уличном шкафу. Узел доступа, размещенный в защитном контейнере внешнего исполнения и оборудованный платами аналоговых абонентских линий Iskratel, соединяется с центральной станцией сетевого оператора по оптоволоконной линии связи Ethernet восходящего направления (рис.6.11).

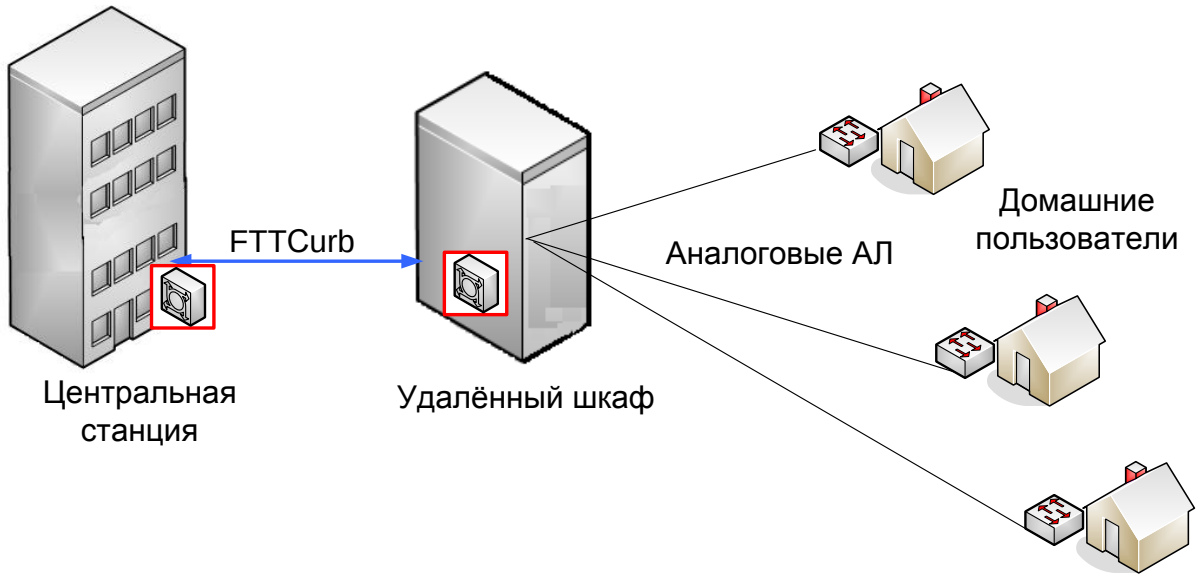


Рис.6.11. Вариант FTTC+POTS

Требуемыми сетевыми элементами являются:

- центральная станция-SI3000 Lumia или SI3000 MSAN с платами Giga Fiber;
- удаленный шкаф SI3000 MSAN с платами аналоговых АЛ;
- защитный контейнер ODU-M (SI3000 MSAN в корпусе MEA 20);
- защитный контейнер ODU-S (SI3000 MSAN в корпусе MEA 10 или в меньшем корпусе). Электропитание-MPS 1000.50 для защитного контейнера ODU-M. MPS 1000.25 для защитного контейнера ODU-S. RPS.

FTTC с комбинированным доступом (Combo Access) представляет собой совместное одной плате абонентских линий аналоговое подключение и

подключение ADSL2+. Комбинированный доступ оптимален в тех случаях, когда оператор стремится сохранить максимальную гибкость типа абонентского доступа. Основное подключение аналоговой АЛ можно быстро преобразовать в широкополосное подключение ADSL2+ с высокой пропускной способностью.

Наличие комбинированного доступа является большим преимуществом в случае, когда предполагается быстрое увеличение числа широкополосных абонентов в определенном районе (см.рис.6.12). При использовании плат

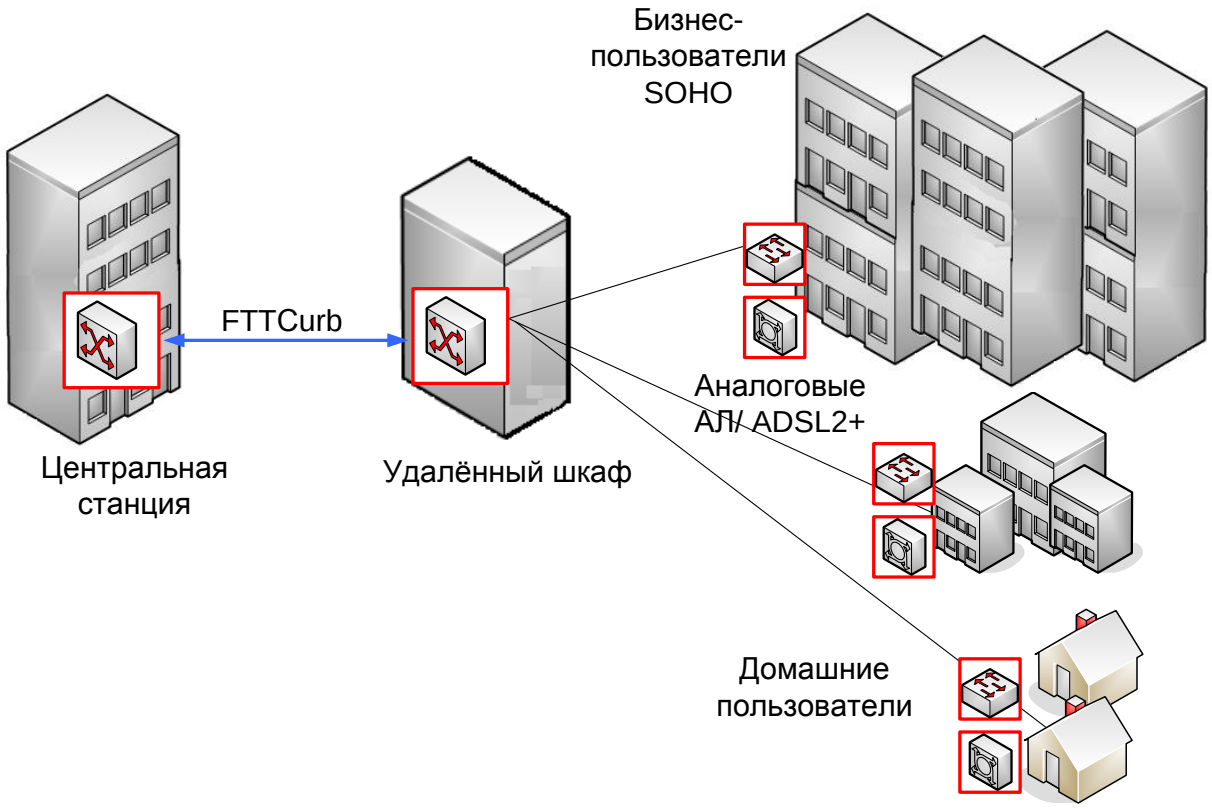


Рис.6.12. Вариант FTTC с комбинированным доступом

комбинированных АЛ, пользователь голосовой телефонии изначально получает аналоговое подключение/ADSL2+. Таким образом, будущий переход на исключительно широкополосное подключение осуществляется незамедлительно и этот переход не влечет никаких дополнительных затрат, поскольку для всех абонентов заранее смонтированы оба типа доступа.

При разработке схемы подключения оборудования доступа необходимо учитывать место размещения оборудования- среди многоквартирных домов или групп жилых построек.

В случае многоэтажных построек выгодно подключать узлы доступа по кольцевой схеме с резервированием оптического волокна (см.рис.6.13). Узлы доступа MSAN расположены в центре жилого массива в уличных шкафах.

Емкость MSAN выбирается равной емкости демонтируемого магистрального медного кабеля на данном участке. Комбинированный доступ «оптоволокно-медь» позволит абонентам поддерживать как

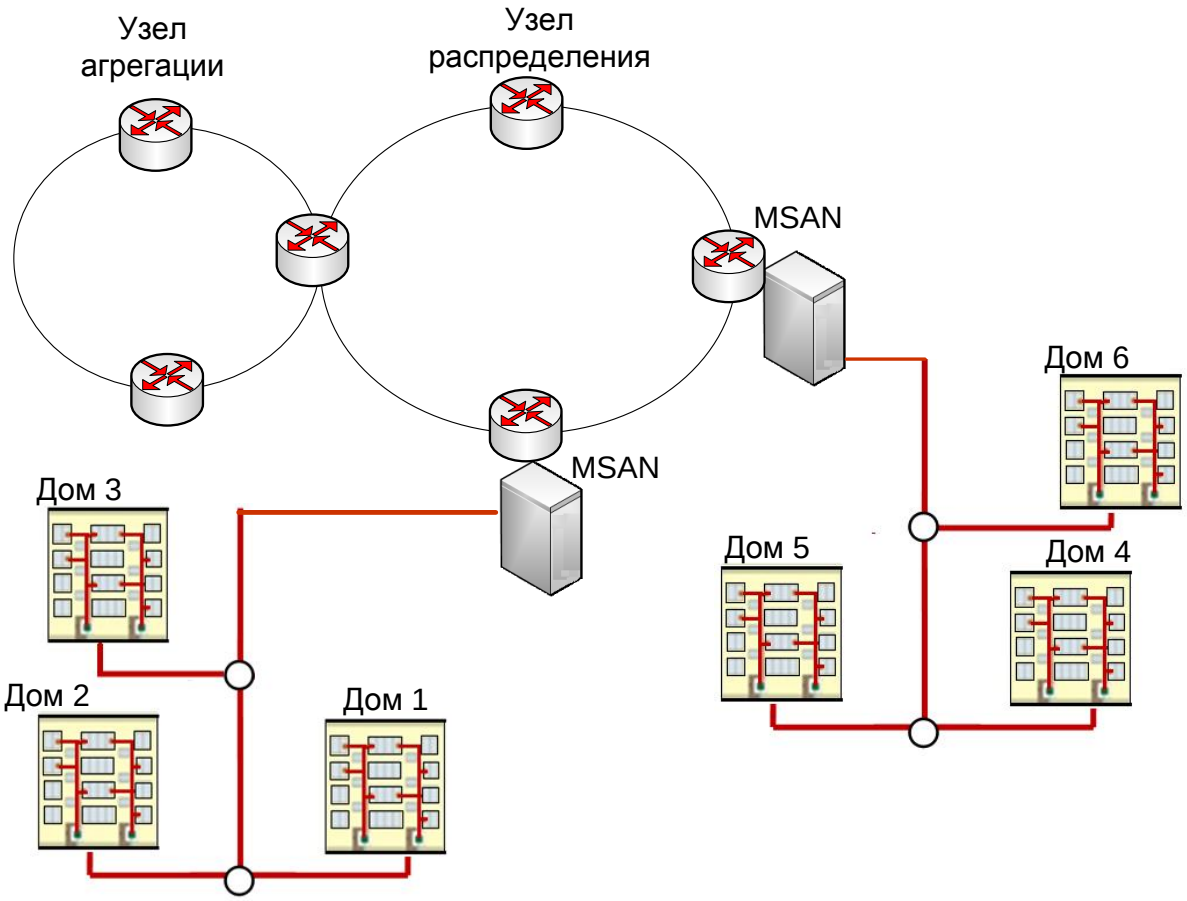


Рис.6.13. Кольцевая схема организации FTTC

традиционные услуги телефонии, так и высокоскоростной интернет по xDSL, число абонентов ШПД вырастет за счет сокращения длины медного участка.

6.4. Медиа шлюзы AMG, TMG, UMG

На уровне пограничного доступа может быть использовано различное оборудование, рассмотрим его на примере фирмы HUAWEI.

Устройство интегрального доступа (IAD): представляет собой устройство абонентского доступа, используемое в архитектуре NGN. С помощью этого устройства осуществляется организация услуг передачи данных, речевой связи, видеоинформации и других услуг по пакетной сети. В каждом устройстве (IAD) предусмотрено максимум 48 абонентских портов.

Медиашлюз доступа (AMG): С его помощью абоненту предоставляется разнообразный доступ к услугам, таким как аналоговый абонентский доступ, доступ к цифровой сети с интеграцией услуг ISDN, доступ V5 и доступ к цифровой абонентской линии (xDSL).

Медиашлюз сигнализации (SG): находится на уровне интерфейса сети системы сигнализации ОКС7 и сети Интернет-протокола (IP); обеспечивая

преобразование сигнализации между коммутируемой телефонной сетью общего пользования ТфОП и сетью IP.

Медиашлюз соединительных линий (TMG): находится между сетью с коммутацией каналов и IP сетью с коммутацией пакетов, обеспечивая преобразование формата между ИКМ-потоками и информационными потоками среды передачи IP.

Универсальный медиашлюз (UMG): выполняет преобразование формата потоков среды передачи и преобразование сигнализации в режимах TMG, встроенного SG или AMG. Обеспечивается подключение разнообразных устройств, таких как телефонная станция ТфОП, учрежденческая телефонная станция УАТС (PBX), сеть доступа, сервер сети доступа (NAS) и контроллер базовой станции.

Рассмотрим несколько примеров оборудования доступа.

Транспортный медиашлюз TMG8010 выполняет функцию перекодирования речи между канальным трафиком ТфОП и пакетным трафиком IP-сети, функцию упаковки/распаковки IP-пакетов и устранения эффекта переменной задержки доставки пакетов (джиттера). Он имеет встроенный шлюз сигнализации, который может использоваться при отсутствии выделенного шлюза сигнализации SG (Signaling Gateway) в сети или STP (Signaling Transfer Point). Встроенный шлюз сигнализации в TMG8010 взамодействует с гибким коммутатором SoftSwitch через M2UA (MTP2 User Adaptation Protocol) и IUA (ISDN Q.921 User Adaptation Protocol). На рис.12.4 показано положение шлюза TMG8010 в сети.

TMG8010 может выполнять функцию кодека сообщений сигнализации ОКС7 и речевого трафика одновременно. Емкость системы - до 3840 портов. Транспортный шлюз конструктивно выполнен в 3 типах:

плата - обеспечивает 4 потока E1

полка - обеспечивает 48 потоков E1

фрейм - обеспечивает 128 потоков E1.

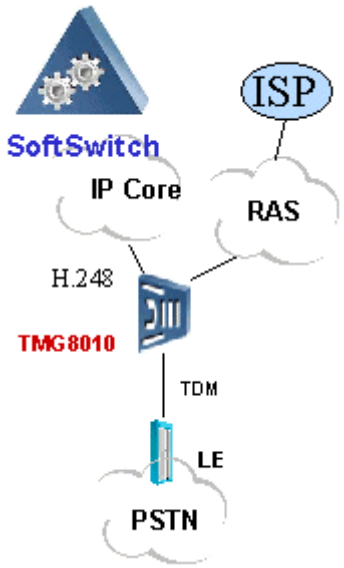


Рис.6.14. Положение шлюза TMG8010 в сети

Технические возможности:

1. Поддержка оптического интерфейса и универсальных портов
2. Обеспечивает оптический интерфейс TDM SDH155M, что экономит ресурсы 2M потоков и пространство автозала, упрощает кабельную разводку.
3. Поддерживает VoIP и RAS на одном порте. При однократных инвестициях оператор может обеспечить как услуги междугородной связи, так и услуги коммутируемого доступа к Интернет, полностью используя возможности оборудования и увеличивая доход от услуг.
4. Полный набор стандартных протоколов
   H.248 и MGCP.
   SS7 через M2UA.
   ISUP, TUP, PRI и R2.
5. TMG8010 и SoftX3000 могут выполнять функцию межсетевого шлюза.
   TMG8010 обеспечивает полную функцию аутентификации и перехвата. Аутентификация может быть выполнена по вызывающему номеру или префиксу, категории вызывающего, идентификатору группы входящих или исходящих соединительных линий, атрибуту вызова, по вызываемому номеру или префиксу, времени вызова и пр.

Универсальный медиашлюз UMG8900 представлен на рис.6.15 представлен универсальный медиашлюз UMG8900, который представляет собой устройство опорной сети в мобильных системах стандарта GSM, разработанное компанией Huawei Technologies. Сети мобильной связи стандарта GSM, ориентированные на будущее, обеспечивают экономию инвестиций и высокий доход операторов связи.

UMG8900 может работать в качестве различных сетевых устройств в зависимости от сетевых требований.

Аппаратная платформа UMG8900 разработана с целью комбинирования пакетного и узкополосного коммутаторов, что должно обеспечить эффективную поддержку узкополосных услуг на базе TDM и пакетных услуг поверх IP. Для потоков услуг и потока управляющих команд шлюз UMG8900 использует различные коммутационные поля.

Оборудование UMG8900 поддерживает режимы передачи данных IP/TDM и различные типы интерфейсов, обеспечивающих возможности взаимодействия с другими типами сетей:

- TDM: STM-1 SDH (электрооптический интерфейс), E1, T1
- IP: FE, GE (оптоволоконный интерфейс), STM-1/4 POS (оптоволоконный интерфейс)
- IPoA: STM-1 IPoA (Оптоволоконный интерфейс)

Система поддерживает следующие услуги и функции:

- встроенного шлюза сигнализации
- эхоподавления, проигрывание тональных сигналов и объявлений, соединение с оборудованием IN, предоставляющим дополнительные

услуги.

– детектор голосовой активности (VAD) и функции буфера джиттера позволяют экономить полосу пропускания и повышает качество голоса.

В системе подвижной связи UMG8900 выполняет изменение различных характеристик несущего канала, в том числе и хэндовера .

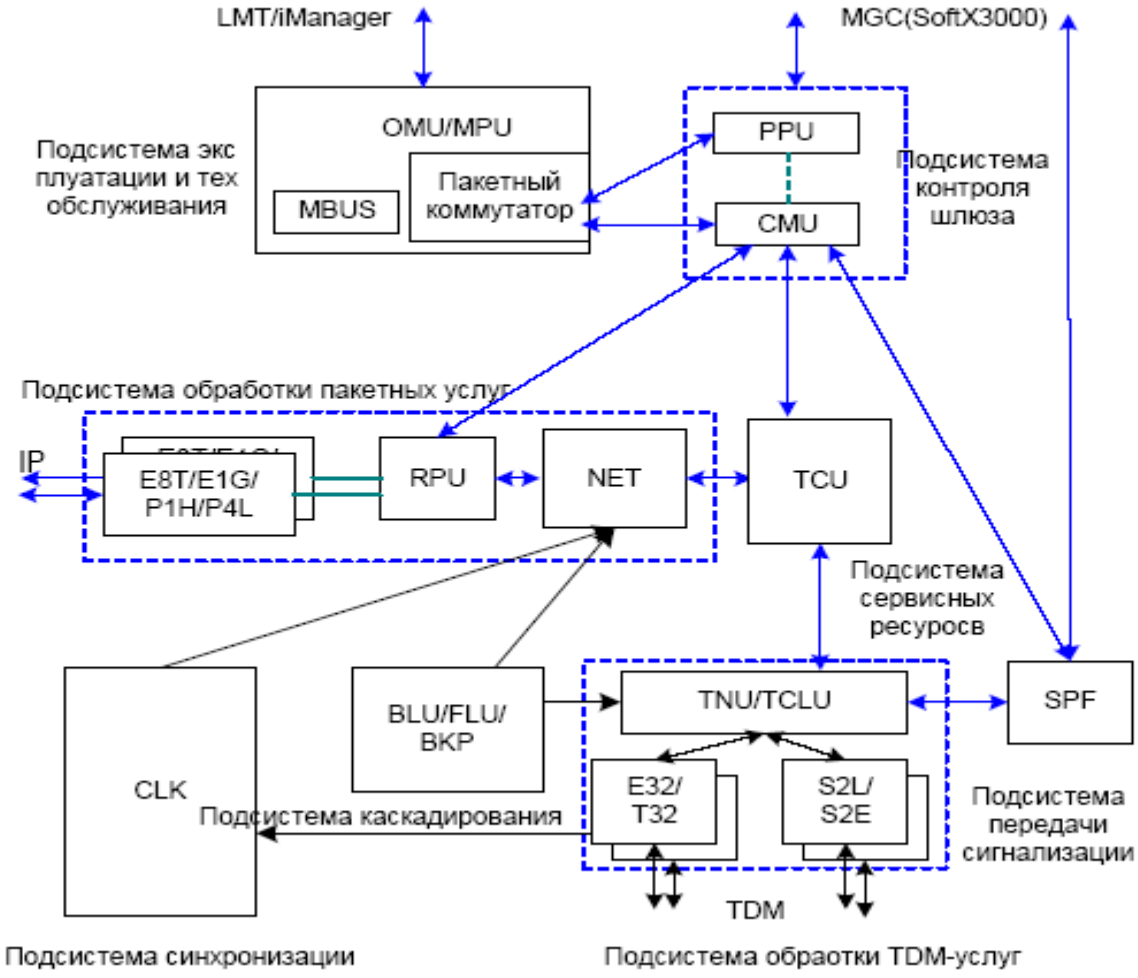


Рис.6.15. Архитектура медиашлюза UMG8900

6.5. DSLAM оборудование широкополосного доступа

Система мультисервисного доступа MA5100 [15] применяется на уровне доступа широкополосной сети. Она подключается к оборудованию ATM через оптический интерфейс высокоскоростной магистрали по восходящей линии (ATM STM-1) для организации широкополосной сети и обеспечения доступа к широкополосным услугам. Оборудование MA5100 собирает от абонентов широкополосные услуги через различные типы

интерфейсов и передает их после централизованной обработки через интерфейс высокоскоростной магистрали.

Оборудование MA5100 может использоваться:

- в качестве оборудования DSLAM для реализации доступа абонентов ADSL.
- в качестве IP DSLAM для реализации доступа абонентов ADSL.
- для обеспечения связи по выделенной линии LAN для реализации сетевого соединения между штаб-квартирой и филиалами предприятия.
- для создания интеллектуальных сообществ ADSL, чтобы удовлетворить сетевым требованиям большого количества абонентов.
- для соединения с удаленной системой доступа через нисходящий интерфейс ATM со скоростью передачи STM-1.

Система может взаимодействовать при помощи стандартных интерфейсов с оборудованием других производителей, чтобы предоставлять различные услуги, в том числе услуги Интернет, VOD (Видео по запросу), услуги видеоконференции, дистанционной медицины, управление инженерными системами зданий, что дает новые возможности в сфере предоставления услуг сети связи.

Оборудование MA5100 поддерживает платы с 32 интерфейсами абонентского доступа ADSL и мульти-VLAN восходящих потоков, обеспечивает емкость коммутации 1,2 Гбит/с, поддерживает функцию распределенной коммутации и позволяет реализовать коммутацию услуг между различными портами услуг при помощи шины передачи ячеек.

Оборудование MA5100 имеет возможность доступа к Интернет посредством подключения к городской магистральной сети MAN через восходящие широкополосные интерфейсы. Также с помощью функции коммутации услуг можно реализовать взаимодействие между портами ADSL и LAN. Оборудование подходит для создания сети широкополосных интеллектуальных сообществ. Кроме того, данное оборудование реализует взаимосвязь по выделенной линии между двумя внутренними портами LAN, а также подходит для организации выделенной линии Ethernet предприятий.

MA5100 обеспечивает следующие услуги:

1) Доступ к услугам ADSL. Услуги ADSL используют методы модуляции DMT и асимметричную передачу данных для передачи услуг. Полоса частот восходящего потока данных — 26-138 кГц. Скорость передачи - до 640 кбит/с, полоса частот нисходящего потока - 138 кГц... 1,104 МГц, а скорость передачи - до 8 Мбит/с.

ADSL использует существующую абонентскую телефонную линию для передачи высокоскоростных данных и предоставляет абонентам различные типы услуг, включая высокоскоростной доступ к сети Интернет, VOD, TV и т.д. Поскольку полосы частот ADSL и 4 кГц POTS разделены, таким образом процесс предоставления широкополосных услуг не оказывает никакого влияния на предоставление традиционных услуг POTS. Система мультисервисного доступа MA5100 может применяться в качестве DSLAM,

чтобы удовлетворить требования по доступу ADSL.

2) Доступ к услугам LAN. Применяется с оборудованием доступа 10BASE-T/100BASE-T Ethernet, работающего по кабелю UTP-5 с расстоянием передачи менее 100 м. Доступ к услугам LAN обеспечивает доступ PPPOE через прозрачное соединение RFC1483B. Оно поддерживает для абонентов сети LAN, отделенных от сети VLAN, непосредственный вход в сеть Интернет при помощи существующего оборудования. Поскольку абоненты на малых и средних предприятиях (SME) не могут создать частную сеть или позволить создать сеть DDN, то им предоставляется доступ через выделенную широкополосную линию. При аренде выделенных линий ATM локальная сеть предприятия может подключаться к модулю MA5100 через оборудование радиодоступа 10/100M Ethernet или порт маршрутизатора после разделения с оборудованием брандмауэра (firewall). Таким образом, на основе существующей широкополосной сети возможно создание сети между филиалами предприятия, равно как и подключение предприятия к сети Internet. В то же время, соблюдаются требования к качеству предоставления услуг широкополосной сети, к временным задержкам и т.д. В этом случае, предприятие может создавать свои собственные виртуальные частные сети в сети общего пользования.

3) Ретрансляция кадров. Услуга ретрансляции кадров (FR) является услугой WAN. Оборудование доступа FR и группы пользователей FR, которые могу поддерживать передачу данных, факсимильных сообщений и речевых сообщений, в настоящее время получили быстрое развитие. В последние годы с развитием технологии ATM совместное существование FR и сети услуг ATM требует взаимодействия между FR и сетями ATM.

Взаимодействие сетей FR и ATM делится на два типа: на уровне сети и на уровне услуг. На уровне сети все терминалы используют один протокол, между сетями могут использоваться различные протоколы. Внутри сети имеет место двунаправленное преобразование протоколов. Более того, существование другого сетевого протокола в одной сети является прозрачным для абонентов терминала. На уровне услуг, два терминала могут использовать различные протоколы для создания соединения точка-точка. Преобразование протоколов осуществляется внутри сети.

Модуль MA5100 предоставляет функцию взаимодействия FR/ATM в соответствии с протоколами взаимодействия сети и услуг, определенными в FR FORUM. Взаимодействие на уровне сети обеспечивает передачу информации FR между терминалами FR по сети ATM. Терминалы FR могут быть подключены к сетям ATM или FR. Взаимодействие на уровне услуг позволяет производить прозрачную передачу между FR CPE в сети FR и ATM CPE в сети ATM, без преобразования на терминалах. Кроме того, плата интерфейса FR модуля MA5100 может обеспечивать функцию прозрачной передачи.

4) Доступ к услугам IP-DSLAM. Система MA5100 может предоставить режим применения сетевого доступа IP-DSLAM, используя интерфейс FE

платы LANC как интерфейс восходящего потока. Рабочие принципы такие же, как и при режиме передачи ячеек ADSL, т.е., установив RFC1483B PVC на ATU-R, в системе MA5100, установите PVC между портом ADSL и VLAN ячейки LANC при помощи внутренней кросс-коммутации. Плата LANC реализует PVC и протокол RFC1483B, и преобразует данные в пакеты для восходящего потока. Когда предоставляется услуга по восходящему потоку через интерфейс FE, модуль MA5100 выполняет функцию уровня 2, не включая обработку протокола уровня 3. Абонент ADSL получает доступ через выделенную межсетевую линию или в режиме PPPOE. Если абонент ADSL получает доступ в режиме PPPOE, у абонента персонального компьютера должно быть установлено программное обеспечение для набора номера PPPOE, вызов PPP выполняется на оборудовании BAS.

5) Услуга ретрансляции ячеек. Система мультисервисного доступа MA5100 поддерживает PVC в режиме передачи ячеек, а также взаимодействие между абонентами ADSL и LAN. В данном режиме Сервер ячеек осуществляет доступ через интерфейсы Ethernet платы LAN, а отдельные абоненты подключаются через порты ADSL. Затем они соединяются по PVC между VLAN платы LAN и портом ADL для получения информационных услуг или получения информации мониторинга из автозала или центра управления.

Оборудование MA5100 состоит из части доступа к услугам и системной части. Функциональная структура системы приведена на рис.6.16.

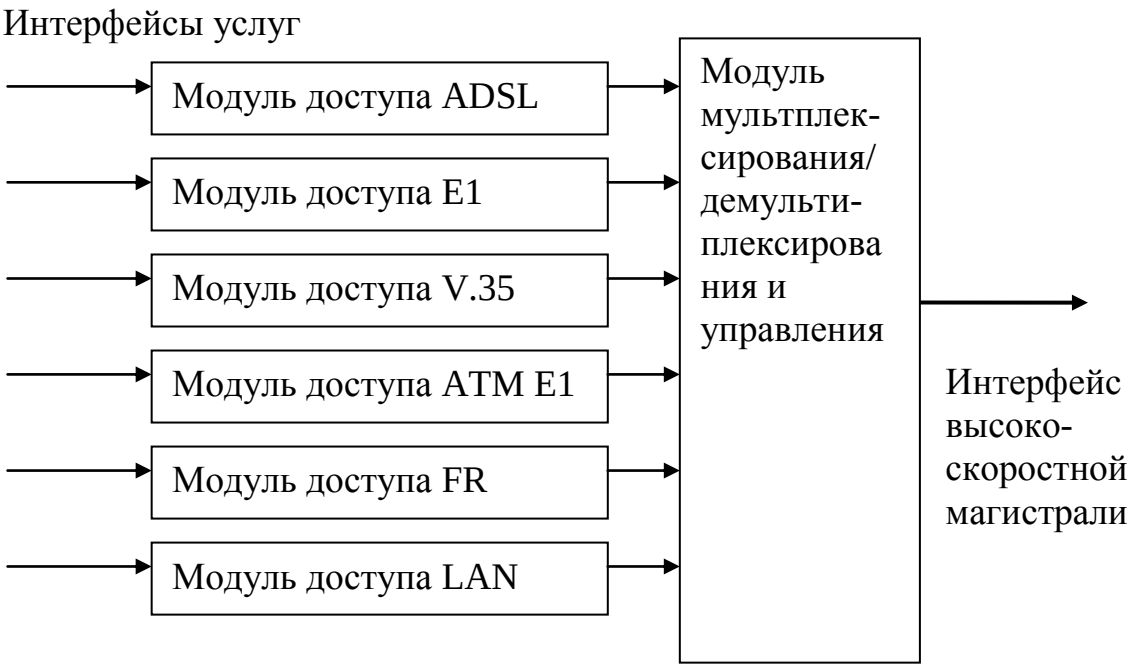


Рис.6.16. Структурная схема функциональных модулей системы DSLAM

Часть доступа к услугам состоит из следующих модулей:

- модуль доступа ADSL;
- модуль доступа CES E1;

- модуль доступа CES V.35;
- модуль доступа ATM E1;
- модуль доступа LAN;
- модуль доступа FR.

Системная часть состоит из двух основных модулей:

- модуль мультиплексирования/демультиплексирования;
- модуль управления системой.

Модули имеют следующие характеристики:

1. Модуль доступа ADSL предназначен для порта доступа услуг ADSL, использует алгоритм DMT и предоставляет методы доступа ADSL с улучшенными характеристиками. Этот модуль состоит из платы ADSL, сплиттера и других.

2. Модуль доступа CES E1 ориентирован на услуги эмуляции схемы интерфейса E1, независимые 8 или 16 каналов интерфейсов E1, а также поддерживает структурированные (SDT N×64K) или неструктурированные (UDT) услуги эмуляции схемы. Для соединения каналов применяется соединение PVC, по которым возможна передача различных типов услуг с низкой скоростью передачи, осуществление доступа к различным типам услуг PBX, DDN, видеоконференции, маршрутизации и др., что позволяет полностью использовать ресурсы существующей сети.

3. Модуль доступа CES V.35 определяет доступ к услугам передачи данных V.35N×64K. Плата CES предоставляет 8 независимых каналов интерфейса V.35, поддерживает рабочий режим DTE и DCE. Плата CES предоставляет доступ ATM для услуг V.35 через схему эмуляции. Плата CES предоставляет доступ к различным типам оборудования, использующего интерфейс V.35, включая маршрутизаторы доступа, DDN и др.

4. Модуль доступа ATM E1 обеспечивает услуги ретрансляции ячеек E1. Услуги ретрансляции ячеек E1 можно реализовать через стандартное оборудование ATM или при помощи низкоскоростного соединения между коммутаторами ATM по существующим линиям передачи E1 PDH без прокладывания новых линий, таким образом полностью используя существующие сетевые ресурсы.

5. Модуль доступа LAN предоставляет 8 самонастраивающихся интерфейсов 10M/100M Ethernet и обеспечивает соединение с Ethernet по выделенной линии через сеть ATM, реализуя прозрачное соединение RFC 1483B.

6. Модуль доступа FR предоставляет услуги ретрансляции кадров E1/T1/V.35. Интерфейс ретрансляции кадров E1/T1 поддерживает доступ ретрансляции кадров с разделением каналов и без разделения каналов, а также поддерживает взаимодействие между сетью и услугами, как это указано в форуме “Frame Relay Forum”.

7. Модуль для удаленного каскадного построения сети AIU контролирует интерфейсы ATM STM-1 и IMA и APON для реализации функции удаленного каскадного построения.

8. Модуль мультиплексирования/демультиплексирования обеспечивает функцию мультиплексирования/демультиплексирования потока услуг в системе, мультиплексирует поток данных из низкоскоростных сервисных плат в поток данных с более высокой скоростью и передает их в интерфейс высокоскоростной магистрали. Кроме того, модуль производит поиск адресов потока данных из интерфейса высокоскоростной магистрали и демультиплексирует их в различные низкоскоростные модули услуг.

9. Модуль управления системой выполняет функции технического обслуживания, управления, настройки конфигурации системы и т.д. Собирает информацию от других модулей, передает команды управления, настраивает конфигурацию данных и т.д. Кроме того, обеспечивает интерфейсы технического обслуживания, интерфейсы NMS и интерфейсы устранения неполадок.

6.6. BRAS маршрутизатор широкополосного удалённого доступа

Broadband Remote Access Server (BRAS или BBRAS) – маршрутизатор широкополосного удалённого доступа маршрутизирует трафик к/от мультиплексора доступа цифровой абонентской линии (DSLAM) или коммутатора в сетях интернет-провайдера.

BRAS находится в ядре сети провайдера и агрегирует пользовательские подключения из сети уровня доступа. Именно на BRAS’е провайдер может применять политику маршрутизации и качества обслуживания (QoS). Специфичными задачами BRAS являются:

- агрегация трафика клиентов от DSLAM'ов
- обеспечение пользовательских сессий по протоколам PPP или ATM
- применение политики качества обслуживания (QoS)
- маршрутизация трафика в магистральную сеть (backbone) провайдера

DSLAM собирает поток данных от множества пользователей в одну точку так, чтобы он мог быть загружен маршрутизатору через протоколы Frame Relay, ATM или Ethernet.

Маршрутизатор производит логическую терминацию туннелей точка-точка (PPP). Это могут быть инкапсулированные туннели PPP через Ethernet (PPPoE), PPP через ATM (PPPoA). Выступая точкой терминации BRAS отвечает за назначение параметров туннелей от пользователей, таких как IP-адрес. BRAS является первым хостом от клиента в Интернет, а также интерфейсом к системам аутентификации, авторизации и учёта трафика (например RADIUS).

Реализации BRAS делятся на аппаратные и программные. Аппаратные BRAS, производят, например, компании Cisco, Juniper, Huawei и др., в случае их использования оператор получает готовый комплект с предсказуемыми характеристиками, поддержкой вендора по техническим вопросам и обучению персонала. Программные решения существуют от Mikrotik,

BRASFil, MPD, accel, LISG и других производителей, в случае их использования настраивающий такое решение специалист берет всю ответственность за правильность настройки на себя.

Современные тенденции построения сетей стремятся к упрощению структуры, т.е. введению на сети одной особо интеллектуальной точки, и уменьшения до минимума функций оставшихся сетевых элементов. Вариантов реализации – всего два. Либо выносить все на абонентский порт, либо, наоборот, в ядро. Первый вариант оптимизирован в пользу быстродействия, исходя из парадигмы, что ядро должно именно передавать данные, а не заниматься функциями фильтрации и обработки.

Однако, ограничение стоимости абонентского порта в рамках 10дол. США за порт сводит на нет создание единой точки раздачи услуг из абонентского устройства, т.к. при этой стоимости абонентского порта невозможно гибко ограничивать полосу, например, раздельно на ресурсы двух разных типов, считать IP трафик.

На роль единой точки раздачи услуг претендует только центр сети. Либо локальные центры, в которых концентрируется достаточное количество пользователей для "тяжелого" оборудования. Рассмотрение схемы с туннелями PPPoE, PPtP, и подобными механизмами приводит к одному и тому же решению. Если взять от схемы туннелей избирательность "до каждого абонента", а от варианта подсчета на маршрутизации - беспроблемную работу на полной скорости. При этом тип туннеля становится не важным – он просто должен быть дешевым, и поддерживаться базовыми средствами Ethernet. На сегодня в этом качестве могут выступать только Vlan’ы 802.1q. С их помощью фактически можно включить каждого абонента в сервер доступа, а так как это нужно сделать на полной скорости, то и название должно стать BRAS (broadband remote access server) или BSR (broadband service router).

Все услуги контролируются на порту BRAS, в центре (или центрах) сети. Весь трафик без исключения проходит через BRAS, там он может учитываться, получать приоритеты.

Идеальным вариантом считается – избавиться от промежуточных уровней агрегации, делая узлы примерно на 100 волокон-домов (и соответственно на 3-4тыс. абонентов).

6.6.1. Оборудование BRAS MA5200F фирмы Huawei

Оборудование SmartAX MA5200F представляет собой широкополосный сервер удаленного доступа (BRAS) на базе протокола IP, применяющийся на уровне доступа широкополосных IP-сетей. MA5200F предоставляет полнофункциональные решения для доступа по Ethernet, обеспечивающие управление пользователями и услугами, безопасность сети и тарификацию [19]. Поддержка оборудованием MA5200F функций

распределенного BRAS полностью исключает перегрузки в сети, которые обычно возникают при использовании централизованного BRAS, и снижает вероятность неполадок в сети.

Ёмкость оборудования MA5200F:

- 4 слота FE, каждый из которых поддерживает 6 одномодовых или многомодовых интерфейсов FE или 6 интерфейсов 10/100 Base-T;
- 1 слот GE поддерживает 1 или 2 одномодовых или многомодовых интерфейса.

MA5200F имеет следующие особенности.

1. Усовершенствованное управление пользователями

Как BRAS на базе IP, оборудование MA5200F поддерживает различные режимы аутентификации и авторизации фиксированных и мобильных пользователей, такие как PPPoE, VLAN , VLAN+WEB и 802.1x. Позволяет ограничивать полосу пропускания пользователей значением N 64кбит/с. Ограничивает число пользователей, получающих доступ с каждого интерфейса и каждой учетной записи в диапазоне от 1 до 1000, эффективно блокирует доступ неавторизованных пользователей и предотвращает атаки на сервер DHCP. Благодаря встроенному серверу DHCP поддерживает 16 пулов IP-адресов и предоставляет пользователям возможность выбора из нескольких ISP.

2. Гарантия безопасности сети

Уникально идентифицирует пользователя с помощью связывания VLAN-ID, MAC и IP-адреса, предотвращает атаки на DHCP, незаконное присвоение адреса и учетной записи. Поддерживает изоляцию пользователей на 2-м уровне и контролируемый доступ пользователей. Поддерживает ограничение доступа к определенным узлам сети и фильтрацию адресов пользователей по ACL. Обеспечивает функцию брандмауэра для предотвращения несанкционированного доступа из внешних сетей.

3. Поддержка разнообразных услуг

Поддержка нескольких ISP и оптовой продажи полосы пропускания. Поддержка услуг Portal и услуг дополнительных доходов, предоставляемых ISP. Поддержка управляемых широковещательных услуг, предотвращение широковещательных штормов и несанкционированного доступа. Гарантия QoS при передаче VoIP. Поддержка услуги IP VPN позволяет строить частные сети IP с помощью прозрачной передачи VLAN.

Поддержка решения для гостиниц. Поддерживает сетевой процессор, позволяющий быстро и легко создавать новые услуги.

4. Гибкая система тарификации

Поддержка усовершенствованной стратегии тарификации пользователей: удаленный агент тарификации, поддерживаемый RADIUS и локальная немедленная тарификация. Гибкая тарификация пользователей по продолжительности сеанса и по трафику. Тарификация по IP-адресу назначения. При взаимодействии с сервером RADIUS обеспечиваются тарификация с предоплатой, немедленная тарификация и автоматическая

блокировка портов пользователей-неплательщиков. Автоматическое обнаружение отключения пользователя от сети и автоматическое разрывание бездействующих соединений.

5. Удобное управление сетью

Используя специализированный протокол HGMP, разработанный компанией Huawei, MA5200F обеспечивает удаленное управление и конфигурирование коммутаторов 2-го уровня компании Huawei, подключенных к MA5200F, включая автоматическое начало сеанса, пакетное конфигурирование и т.д. Управление обеспечивается системой централизованного управления сетью iManager™ N2000 производства компании Huawei, поддерживает функции SNMP и MML.

Оборудование SmartAX MA5200F применяется в двух вариантах.

1. Доступ корпоративных абонентов и индивидуальных пользователей в районах с высокой плотностью абонентов (см.рис.6.17).

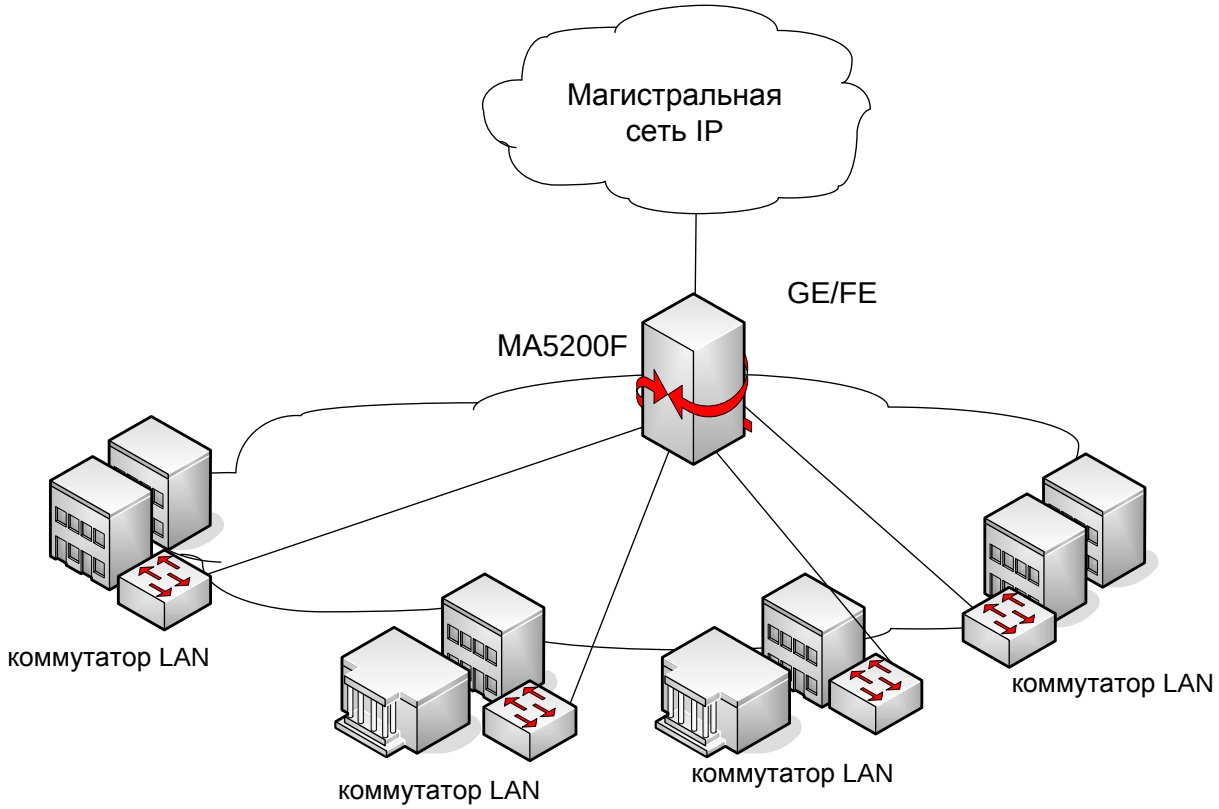


Рис.6.17. Доступ корпоративных абонентов и индивидуальных пользователей в районах с высокой плотностью абонентов

MA5200F располагается в жилом районе или бизнес-центре в качестве оборудования доступа и управления конечных пользователей и обеспечивает терминирование PPP и VLAN, управление пользователями, аутентификацию и тарификацию совместно с коммутаторами LAN серии Quidway, выпускаемыми компанией Huawei. При этом MA5200F обеспечивает большой набор услуг, таких как пакетная передача речи и доступ к

Интернету по широкополосным выделенным линиям для корпоративных абонентов, а также высокоскоростной доступ в к Интернету и VOD для индивидуальных абонентов.

2. Доступ к Интернету рассредоточенных индивидуальных пользователей (рис.6.18.)

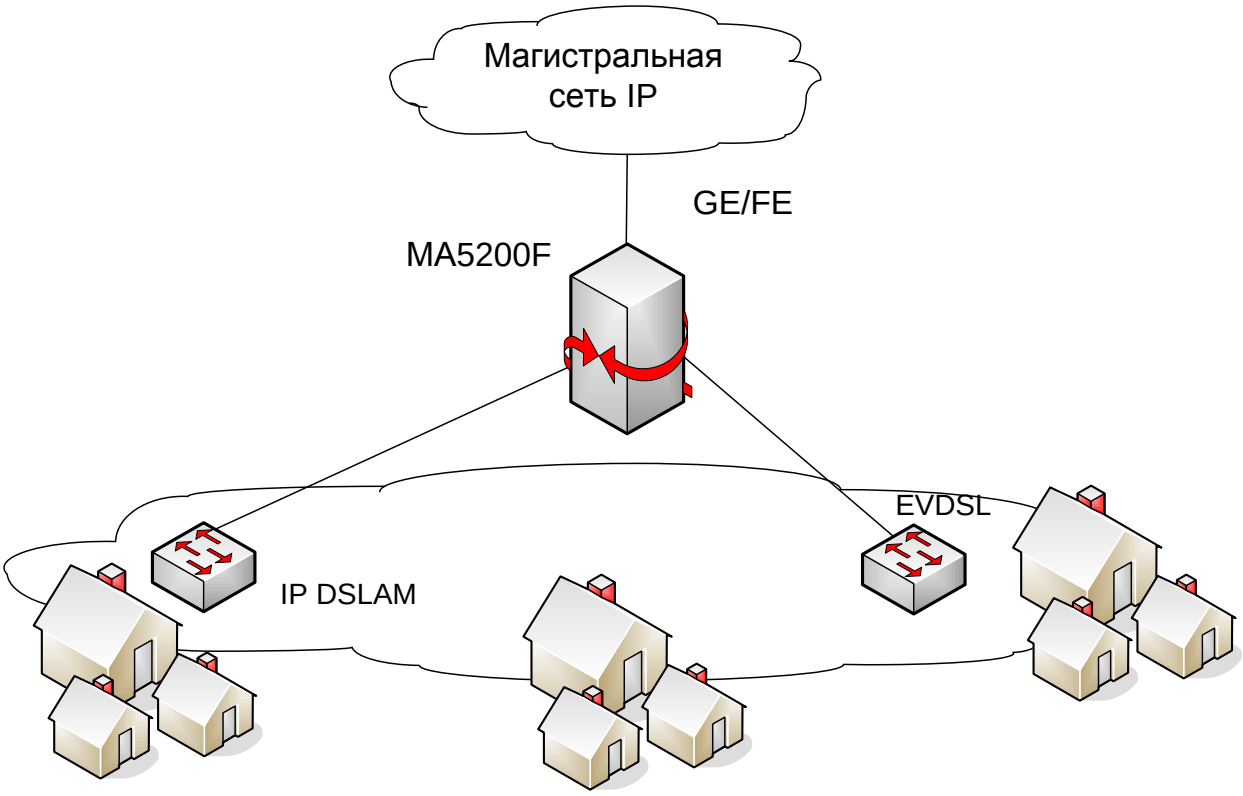


Рис.6.18. Доступ к интернет рассредоточенных индивидуальных пользователей

Совместно с мультиплексорами IP DSLAM MA51XX серии SmartAX и оборудованием доступа по EVDSL S3026V компании Huawei оборудование MA5200F обеспечивает различные методы доступа конечных пользователей и выполняет функции терминирования PPP и VLAN, управления пользователями, аутентификации и тарификации.

6.7. Назначение устройств интегрированного доступа (IAD)

На рис.6.19 показан пример реализации VoIP-сети, использующей сеть доступа с технологий DSL. Обычные аналоговые телефоны и любые устройства локальной сети Ethernet подключаются к устройству интегрированного доступа IAD абонента, которое обрабатывает и передает абонентскую сигнальную информацию по IP-сети или через мультиплексор доступа DSLAM к Softswitch. Что касается речевой информации, то IAD оцифровывает ее, пакетирует и переносит в виде пакетов RPT по IP-сети.

Эти три примера иллюстрируют базовое свойство сетей ССП – интеграцию передачи речи, данных и видеоинформации, включая объединение оборудования и функциональных возможностей как на уровне опорной сети (Core Network), так и на уровне сети доступа (Access Network).

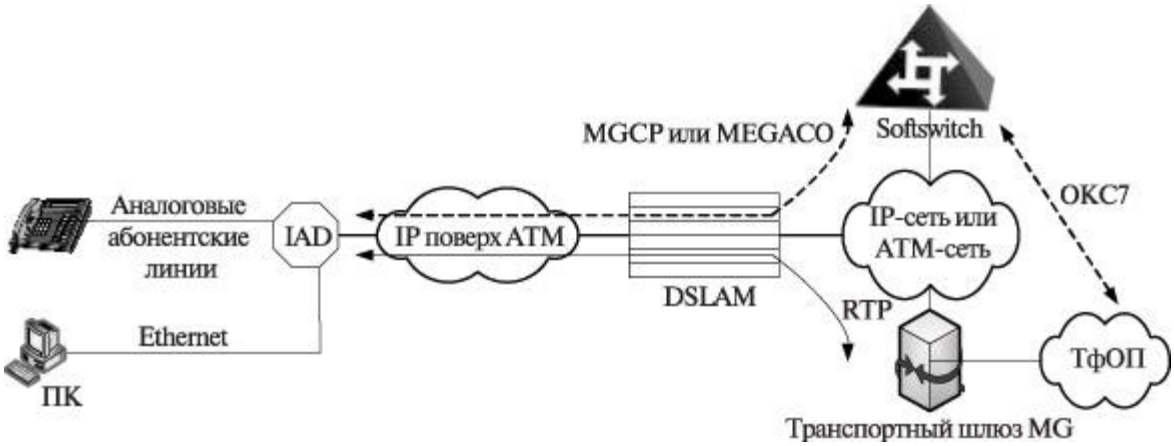


Рис.6.19. Архитектура ССП с IAD и DSLAM

Комбинированные подключения с передачей речи и данных предлагают простое решение по обеспечению широкополосной связью конечных пользователей из небольших и средних компаний.

Важным фактором в распространении технологий «речь по DSL» (VoDSL) и «речь по кабелю» (VoCable) являются интегрированные устройства доступа (Integrated Access Device, IAD). Установленные в помещении клиента, они позволяют поставщикам услуг интегрировать речь, данные и Internet в одном сетевом соединении. Назначение устройства состоит в подключении стандартных телефонов (в идеале — подсоединенных к нескольким линиям) к линии передачи данных. Затем IAD разбивает трафик на пакеты и мультиплексирует его в сеть по высокоскоростному соединению.

Обычно интегрированные устройства доступа применялись с уже имеющимися УАТС или мини-АТС и предшествовали технологиям DSL и кабельным подключениям. Новое поколение оборудования IAD и других аппаратных средств позволило поставщикам услуг привлечь частных пользователей, небольшие и средние компании — заказчиков, пока не определившихся с выбором услуг широкополосной связи.

В США поставщики услуг ориентируются на тех клиентов, которые не способны позволить себе линию T1 за 1000 долларов. У крупных операторов нет предложений для подобного рынка, поэтому таким клиентам приходится использовать коммутируемый доступ в Internet и обычные телефонные линии». С помощью VoDSL пользователи получат пропускную способность линии T1 наряду с несколькими каналами передачи речи и, возможно,

некоторыми расширенными услугами за значительно более низкую абонентскую плату.

Небольшим компаниям редко требуется много каналов передачи речи в дополнение к каналам передачи данных. По данным американских ТК компаний, оптимальное количество необходимых линий для применения VoDSL — от 4 до 20. Это может быть как компания с одним офисом, так и крупная — с множеством небольших филиалов и потребностью в постоянных услугах по передаче речи и данных. Одно из действительно интересных применений VoDSL — интеграция с мини-АТС, поскольку таким системам требуется обычно от 4 до 20 линий.

Комбинированные подключения с передачей речи и данных предлагают простое решение по обеспечению широкополосной связью конечных пользователей из небольших и средних компаний. Вместо того чтобы обращаться к нескольким поставщикам, они могут получать все телекоммуникационные услуги, включая аппаратные и программные средства, от одной местной телекоммуникационной компании. Устройства IAD, осуществляя функции маршрутизаторов, позволяют экономить финансовые ресурсы. Кроме того, они достаточно гибки. Множество устройств IAD старшего класса предусматривают возможность расширения с помощью программных коммутаторов или за счет дополнительных плат. А поскольку сторонняя поддержка имеет большое значение (для экономии и ускорения ремонта), интегрированные устройства доступа снабжаются программным обеспечением для проведения удаленной диагностики и осуществления технической поддержки по протоколам ftp и telnet.

Возможности передачи речи со стороны DSL обычно включают возможность взаимодействия со стандартными функциями службы автоматической телефонной связи Centrex, в том числе идентификацию абонента, ожидание вызова, тональный набор и отправление вызовов. Устройства IAD также обладают полезной функцией распознавания входящих вызовов факса и умеют работать со специальным методом сжатия, используемым в факсимильных аппаратах.

Другими отличительными особенностями являются возможность взаимодействия с различным оборудованием и шлюзами DSLAM, функции резервного копирования, а также поддержка ряда форматов DSL. Для постоянных широкополосных соединений важно, что большинство интегрированных устройств доступа поддерживают такие средства безопасности, как встроенные брандмауэры и защищенные сети VPN.

6.7.1. Устройства IAD фирмы Huawei

IAD представляет собой медиашлюз для передачи по IP-протоколу голоса (технология VoIP) и факсимильных сообщений (технология FoIP),

обеспечивающий эффективную и качественную передачу голоса по глобальной пакетной сети IP (Internet и различные Intranet).

Шлюз VoIP предоставляет аналоговые голосовые интерфейсы для соединения с существующими телефонными аппаратами корпоративных пользователей или учрежденческой АТС, а также интерфейс Ethernet для соединения с магистральной сетью провайдера услуг IP.

IAD поддерживает протокол MGCP, соответствующий стандартам IETF RFC2705 V0.1 и V1.0. Данное оборудование может функционировать совместно с решениями SoftSwitch крупнейших поставщиков с целью развертывания для провайдеров услуг полного решения VoIP с функциями биллинга, учета использования ресурсов и сетевого управления.

Серия IAD включает в себя:

Серия 1 (POTS + малая емкость услуг передачи данных): 16, 24, 32 порта
Серия 2 (интеграция доступа к услугам передачи речи и данных): 8, 12, 24
Настольная серия: 1, 2 и 4 интерфейса; Ephone; SoftPhone
Разделитель DVC для разделения и объединения речевых услуг по UTP5.
В таблице 6.5 приведены характеристики IAD серии U-SYS.

Серия IAD104 может обеспечить 4 канала для простых пользователей ТфОП, использующих доступ VIoP и 1 10/100Base-T интерфейс сети передачи данных.

Таблица 6.5.

Характеристики IAD серии U-SYS

Наимен. продукции	Интерфейс сети	Интерфейс пользователя			Прим.
		POTS	Ethernet	протоколы	Телеф. линия
IAD104E	1 10M/100M	4FXS	1	MGCP	подкл 4 ТА
IAD108	1 10M/100M	8FXS	1	MGCP	подкл 8 ТА
IAD208E	1 10M/100M	8FXS/FXO	2	MGCP/H.248	
IAD132E	1 10M/100M	32 FXS/FXO	4	MGCP/H.248	подкл 8,16,24,32 ТА

Серия IAD108 может обеспечить 8 каналов для простых пользователей ТфОП использующих доступ VIoP и 2 10/100Base-T интерфейса сети передачи данных. Согласно различным интерфейсам серия IAD108 имеют следующие три модели:

- IAD108A(T), обеспечивающая интерфейсы для ADSL
- IAD108E(T), обеспечивающая интерфейсы для Fast Ethernet (FE)
- IAD108V(T), обеспечивающая интерфейсы для Very-high-data-rate Digital User Line (VDSL)

Серия IAD208 может обеспечить смешанный доступ к VIoP сервисам для 8 абонентов ТфОП и 7 абонентов передачи данных. По стандартному кабелю 5 класса, интергированный порт данных и голоса реализует доступ

широкополосных абонентов и голосовых абонентов. Согласно различным панелям интерфейсов серия IAD208 имеет следующие 3 модели:

- IAD208A(T), обеспечивающая интерфейсы для ADSL
- IAD208E(T), обеспечивающая интерфейсы для FE
- IAD208V(T), обеспечивающая интерфейсы для VDSL

Отличие между сериями IAD108 и IAD208 заключается в типе интерфейсов и их количестве на панели интерфейсов. На задней панели серии IAD108, 8 телефонных портов, 2 порта передачи данных, один локальный серийный порт и один восходящий интерфейс. На задней панели серии IAD208 7 портов, которые поддерживают гибридный доступ голосовых абонентов и абонентов передачи данных, один порт только для предоставления доступа телефонным абонентам, один локальный серийный порт и один восходящий порт.

Серия оборудования IAD108/208 поддерживает стандартный голосовой метод компрессии, алгоритмы модуляции/демодуляции для кодирования декодирования голосовых сигналов, сигналов факсов ТФоП. IAD преобразует сигналы в IP пакеты и посылает их по направлению к медиа шлюзу IP. Когда IP пакеты достигнут своей цели назначения они будут опять преобразованы в первоначальный вид. IAD взаимодействует с коммутатором SoftSwitch по средством протокола H.248 или Media Gateway Control Protocol (MGCP), IAD устанавливает соединение между вызывающим и вызываемым абонентами под контролем SoftSwitch. Положение устройств серии IAD108/208 в структуре NGN показано на рис.6.20.

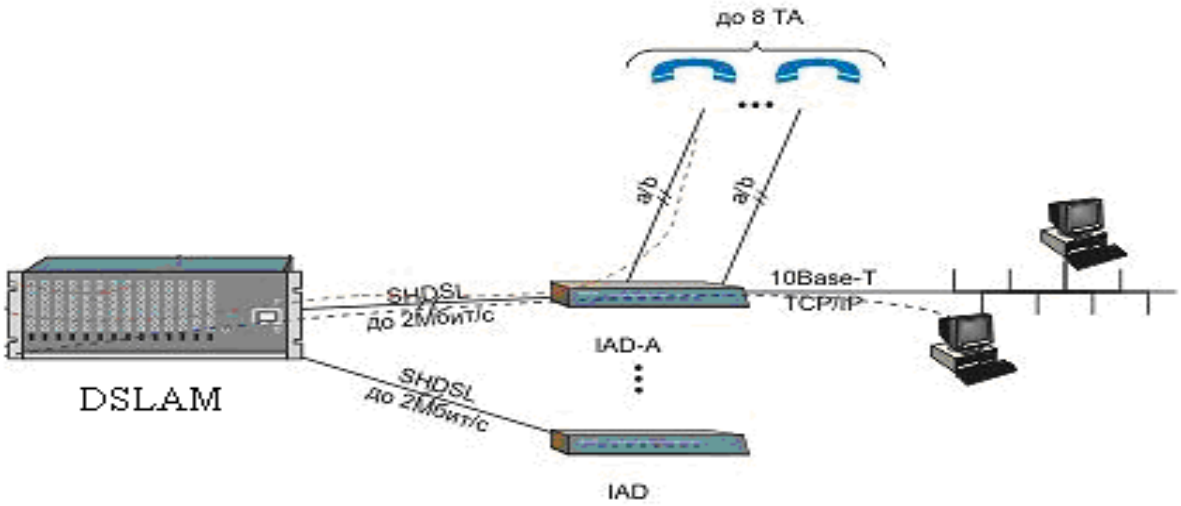


Рис.6.20. Типичный пример применения IAD108/208

IAD132E-T поддерживает усовершенствованный протокол управления медиашлюзом (MGCP), соответствующий стандартам IETF RFC2705 V0.1 и V1.0. Данное оборудование может функционировать совместно с решениями SoftSwitch крупнейших поставщиков с целью развертывания для провайдеров услуг полного решения VoIP с функциями биллинга, учета использования ресурсов и сетевого управления.

IAD132E-T использует стандарт Ethernet 10/100 Base-T для соединения с IP-сетью через маршрутизатор или оборудование передачи данных. Поддерживая высокоэффективный протокол MGCP, IAD132E-T в комбинации с программным коммутатором Softswitch предоставляет конечным пользователям услуги телефонной связи. В целях соответствия требованиям провайдеров услуг, IAD132E-T обеспечивает возможность предоставления коммутатором SoftSwitch комплексного и полного обслуживания, включая функции биллинга и управления сетью. На рис.6.21 изображены места установки оборудования IAD132E-T.

IAD132E-T имеет высокую плотность голосовых интерфейсов для соединения с пользовательскими телефонными аппаратами и факсами. Речевой модуль FXS и дополнительный модуль FXS обеспечивают по 8 голосовых FXS интерфейсов. С помощью установки речевых модулей IAD132E-T может поддерживать 8, 16, 24, или 32 порта речевых интерфейсов для пользователей, имеющих высокий голосовой трафик, например, в жилых домах, офисах, на предприятиях.

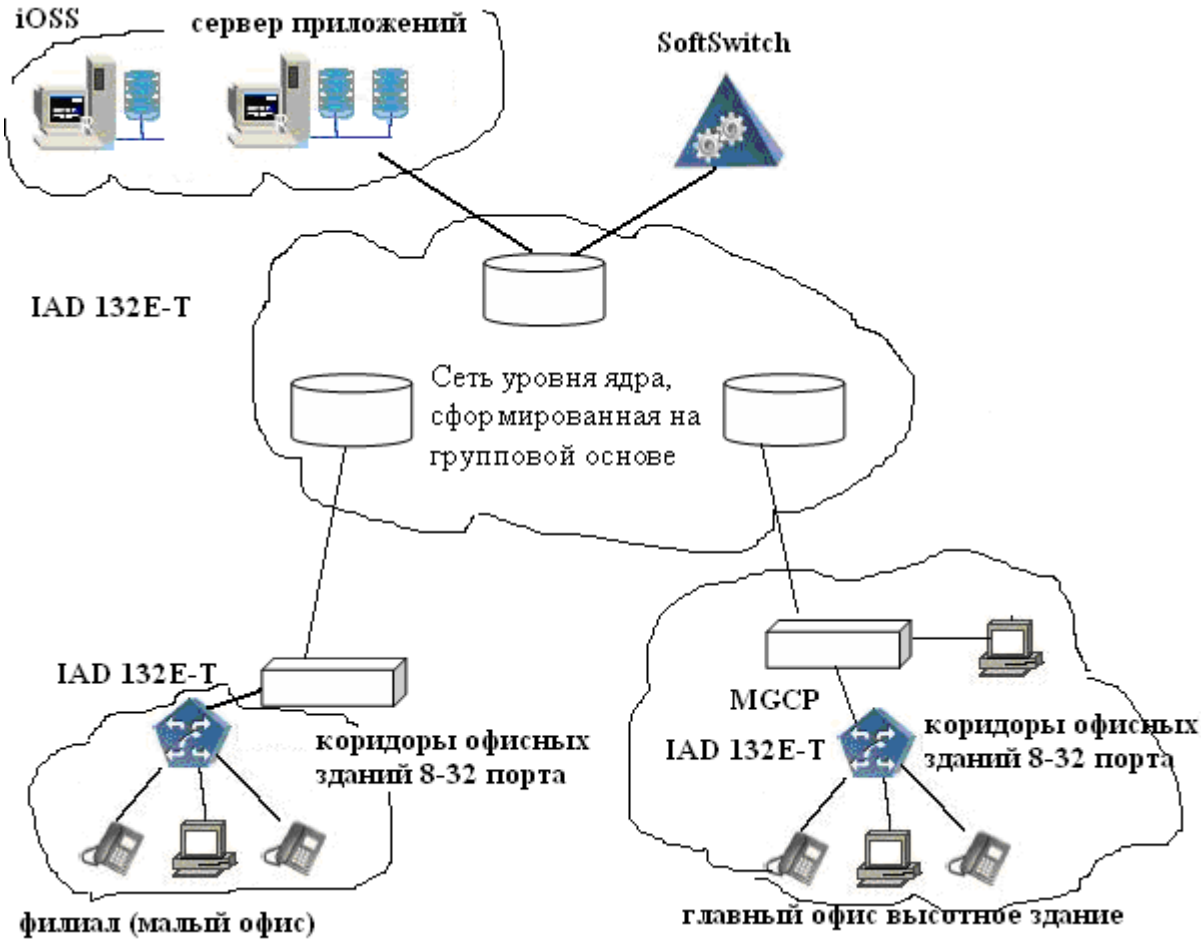


Рис.6.21. Типичный пример применения IAD132E-T

6.8. Узел мультисервисного абонентского доступа MSAN

MSAN – Multiservice Access Node – это интегрированный продукт для обеспечения сетевого доступа и предоставления услуг. В MSAN существует возможность выбора интерфейсов - волоконно-оптическими интерфейс, интерфейсы VDSL2, ADSL2+, SHDSL, интерфейсы мобильной и стационарной связи WiMAX. К услугам, предоставляемым MSAN относятся:

- голосовые услуги
- услуги передачи данных
- мультимедийные услуги
- Centrex
- услуги безопасности и др.

Предлагаемое на рынке оборудование можно разделить на два класса:

- решения для большой емкости (до нескольких тысяч абонентов) предоставляется фирмами Alcatel, Siemens, НТЦ «Протей», Huawei, ADC (Teledata Networks) (Израиль), Iskratel, Samsung, Lucent (США).
- решения для малой емкости (до нескольких десятков абонентов) предоставляется фирмами AudioCodes (Израиль), Boscom (Израиль), НТЦ «Протей»

Считается, что MSAN разработан для технологии FTTC, это не совсем корректное утверждение, требующее пояснений. Рассмотрим схемы организации сети доступа на базе оборудования MSAN.

6.8.1. Развитие сети доступа на базе оборудования MSAN (FTTC)

Схема организации сети доступа на базе оборудования MSAN фирмы Huawei по технологии FTTC приведена на рис.6.22.

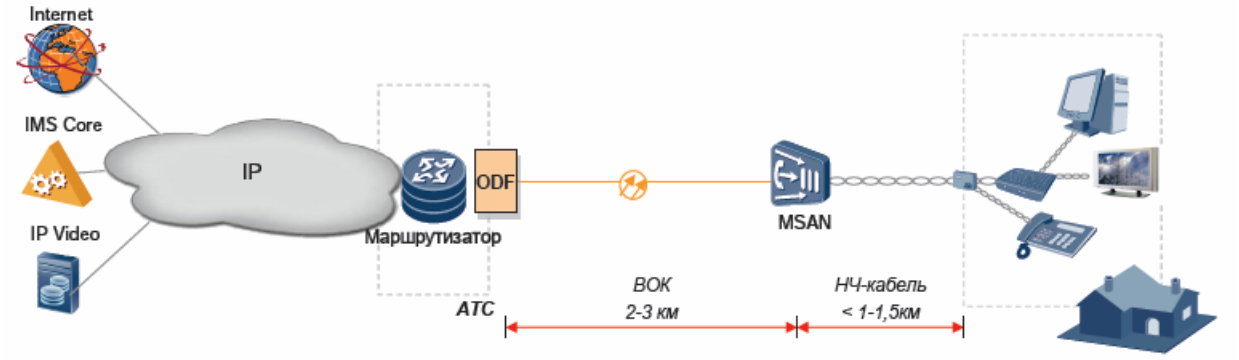


Рис.6.22. Схема организации сети доступа на базе оборудования MSAN

Техническими особенностями данной схемы являются:

- Короткое расстояние до абонента – высокое качество НЧ телефонии
- Скорость ADSL2+ 10-15Мбит/с
- Возможность управления ШПД по SHDSL, VDSL2, FE

– Решение класса FTTC. Возможность миграции к GPON, FTTB.

С помощью этой схемы имеется возможность предоставления высокоскоростного доступа в Интернет и услуги Triple-Play. Поддержка всех дополнительных услуг, предоставляемых NGN. Для корпоративных клиентов возможно предоставление с MSAN интерфейсов FE, E1, ISDN BRI PR.

С точки зрения финансовых показателей необходимо отметить среднюю стоимость внедрения ШПД и экономию средств из-за отсутствия магистрального медного кабеля. Высокая скорость и качество услуг дают возможность получения новых прибылей

Технология MSAN является оптимальным способом снижения OPEX и запуска Triple-Play для оператора, ориентированного на голосовые услуги.

6.8.2. Развитие сети доступа на базе оборудования mini-MSAN (FTTB-xDSL)

Более продвинутым решением является решение сети доступа на базе оборудования mini-MSAN, в котором будет использована комбанация технологий FTTB-xDSL (см.рис.6.23).

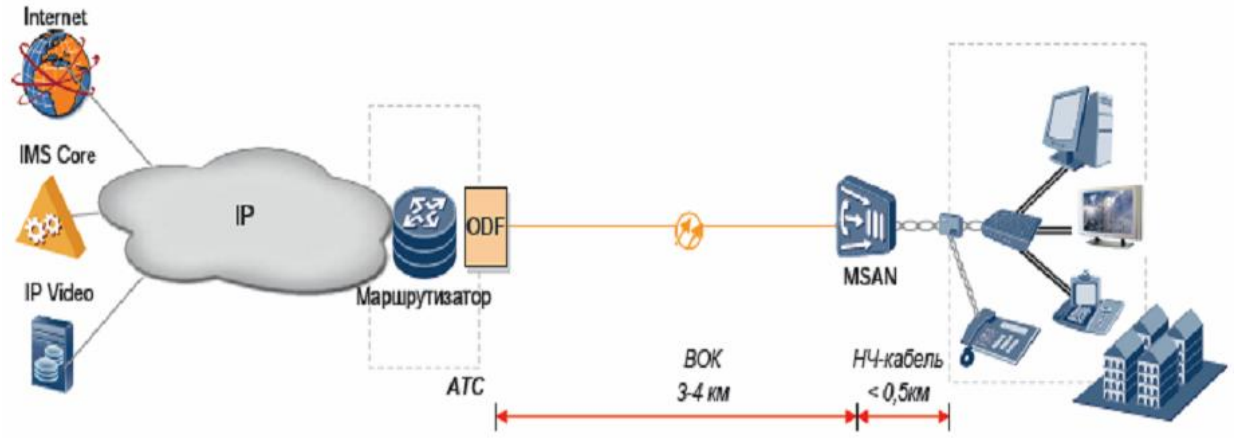


Рис.6.23. Развитие сети доступа на базе оборудования mini-MSAN (FTTB-xDSL)

Технические характеристики:

– Кратчайшее расстояние до абонента – высокое качество НЧ телефонии
– Целесообразно использовать VDSL2 со скоростью 80-100Мбит/с
– Возможность миграции к GPON, FTTB

Предоставляемые услуги

– Multi-Play
– Поддержка всех дополнительных услуг, предоставляемых NGN
– Для корпоративных клиетов предоставление интерфейсов FE, E1, ISDN BRI PRI
– Использование в качестве УАТС

Однако с финансовой точки зрения необходимо отметить:

- Высокая первоначальная стоимость внедрения ШПД
- Экономия средств из-за отсутствия магистрального медного кабеля
- Ultra Broadband и Multiplay исключительные услуги для рынка – максимальная прибыль

Технология используется для построения распределённой сети оператора, ориентированного на полный спектр IP услуг с максимальной защитой инвестиций.

6.8.3. Структура и назначение MSAN ONU-F01D1000 фирмы Huawei

MSAN ONU-F01D1000 – это интегрированный продукт для обеспечения сетевого доступа и предоставления услуг, в нём существует возможность выбора интерфейсов - волоконно-оптическими интерфейс, интерфейсы VDSL2, ADSL2+, SHDSL, интерфейсы мобильной и стационарной связи WiMAX.

На рис.6.24 представлена общая структура сети доступа с интеграцией услуг HONET, разработанная компанией Huawei. На рис.6.25 вариант построения сети с использованием MSAN.

HONET – это оптическая широкополосная сеть, которая использует некоторые технологии:

- «широко/узкополосная платформа»,
- «распределение по ресурсам нескольких шин»
- «кольцевое построение сети VP Ring»,

HONET имеет типичную двухуровневую структуру (OLT+ONU) оптической сети доступа. OLT - Терминал (окончание) оптической линии находится на станции, выполняет обработку протоколов, транспортировку и распределение потоков информации услуг. ONU - Оптический сетевой блок находится на стороне сети доступа и служит для предоставления абонентам доступа к сети. OLT и ONU соединяются через оптическую систему передачи, OLT управляет ONU. OLT может иметь доступ к нескольким ONU.

ONU-F01D1000 представляет собой статив устанавливаемого вне (см.рис.27.5). помещения оборудования интегрального доступа средней ёмкости и высокой плотности, максимум 1200 внутренних линий при коэффициенте сходимости между внутренними и внешними линиями до 1:1,5. ONU-F01D1000 может предоставлять интегральные узкополосные и широкополосные услуги, имеет размеры 1650 мм (высота) x 1900 мм (ширина) x 550 мм (глубина). На рис.6.26 показан внешний вид MSAN ONU-F01D1000, на рис.6.27 приведена архитектура системы MSAN ONU-F01D1000. Контейнер имеет следующее содержимое:

- Встроенное оборудование питания (устройство грозозащиты, система питания, аккумуляторная батарея),
- полка услуг, оборудование передачи,

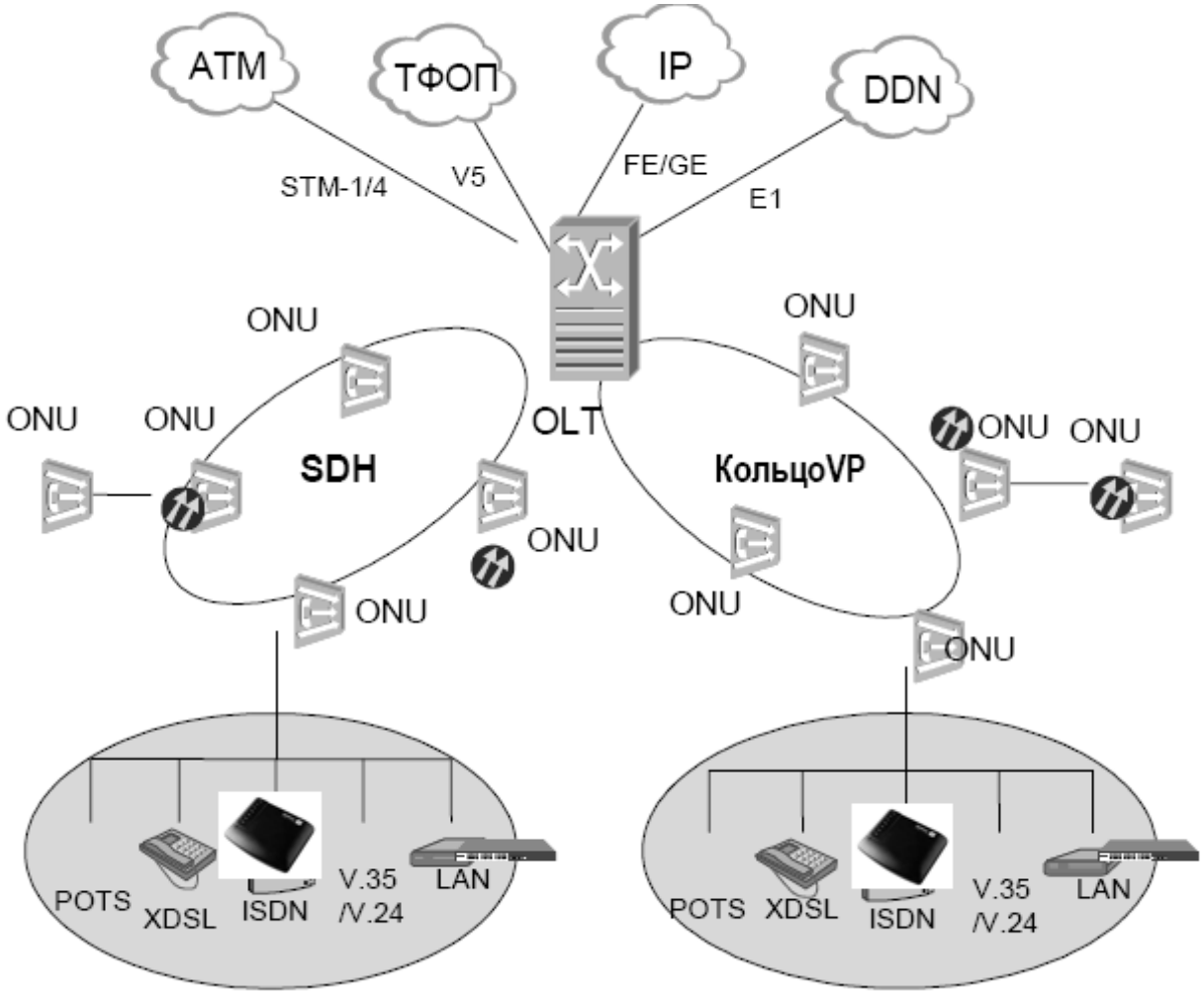


Рис.6.24. Общая структура сети доступа с интеграцией услуг HONET

- MDF,
- оптический кросс ODF,
- цифровой кросс DDF,
- оборудование терморегулирования (кондиционер или теплообменник)
- 1650 мм (высота) х 1900 мм (ширина) х 550 мм (глубина)

MSAN ONU-F01D1000 поддерживаемые интерфейсы – интерфейс ТфОП (POTS), базовый доступ ISDN (2B+D); первичный доступ ISDN (30B+D); E1; ADSL, SHDSL (TDM/ATM), VDSL, IMA E1, E3.

ONU-F01D1000 оборудуется гибридным блоком передачи, поддерживающим несколько способов построения сети – «цепь», «дерево», «звезда», «кольцо» и «кольцо с ответвлениями», «касательные» и «пересекающиеся кольца». MSAN может связываться с любой станцией по стандартному интерфейсу V5, либо связываться с терминалом оптической линии (OLT) средствами частного протокола или протокола V5, подключаться к широкополосной магистральной сети ATM через интерфейсы восходящего направления VP Ring, STM-1 ATM и IMA E1, может подключаться к широкополосной

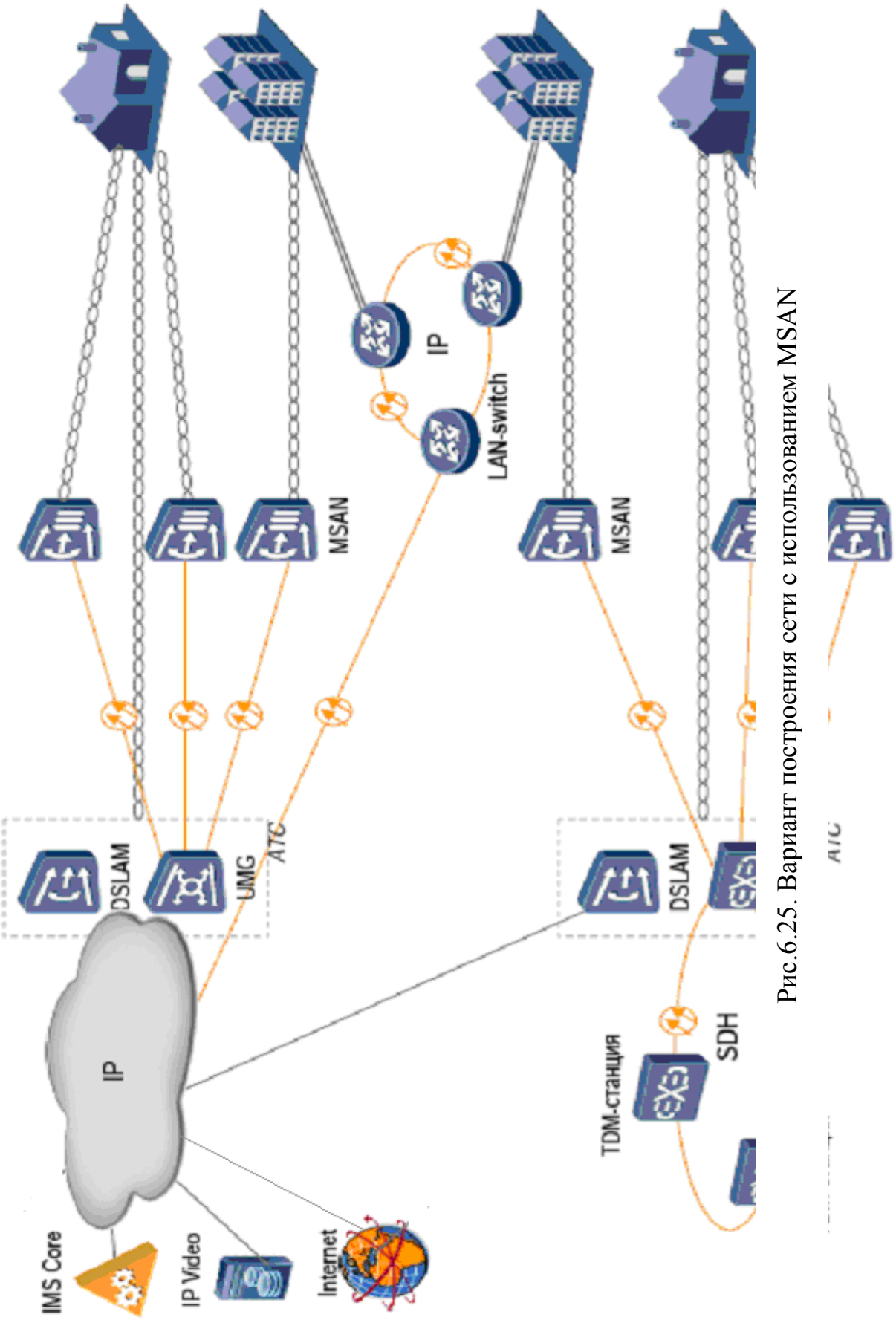


Рис.6.25. Вариант построения сети с использованием MSAN

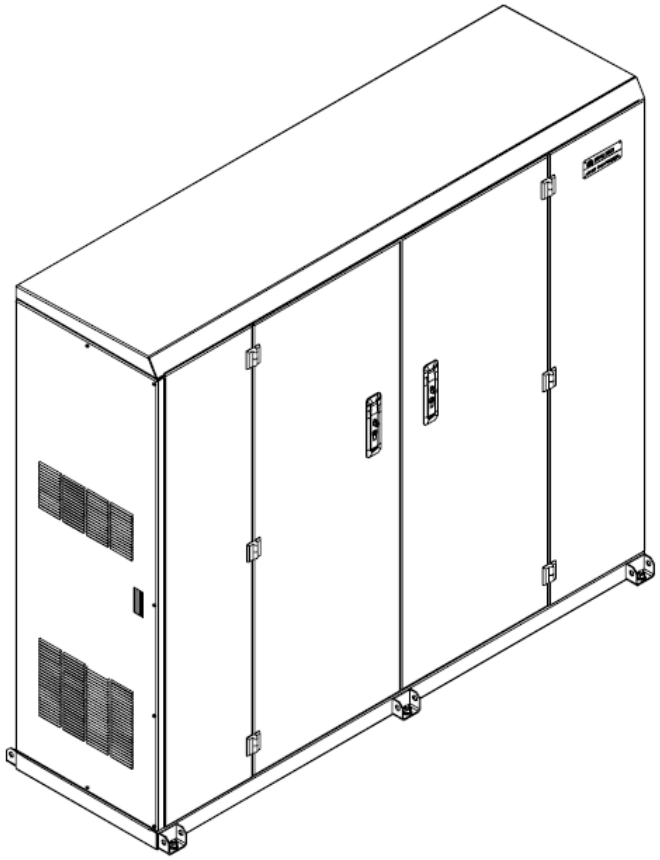


Рис.6.26. Внешний вид MSAN ONU-F01D1000

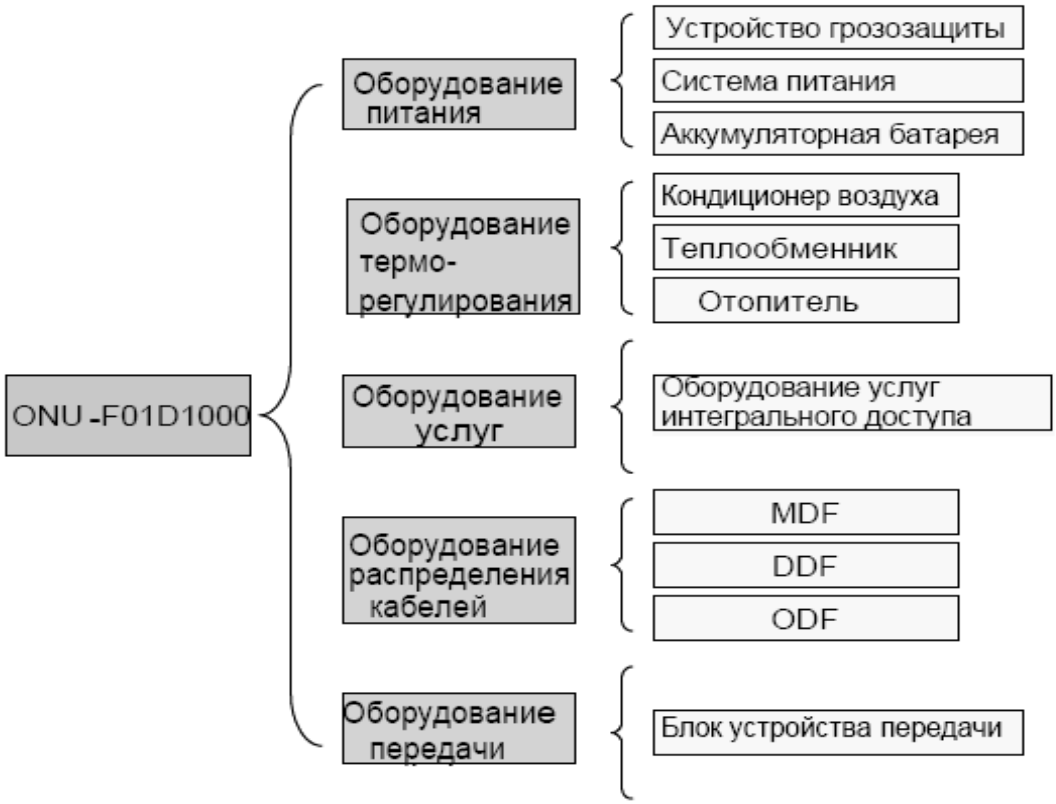


Рис.6.27. MSAN архитектура системы

магистральной сети IP по интерфейсам восходящего направления Gigabit Ethernet/Fast Ethernet.

6.8.4. Эволюция MSAN - MSAG

Следующим этапом развития MSAN является шлюз мультисервисного доступа – Multiservice Access Gateway MSAG, полностью адаптированный под IP сеть. Рассмотрим MSAG ZXMSG5200 фирмы ZTE. MSAG поддерживает следующие протоколы:

- H.248 или MGCP
- Real time transport protocol RTP/RTCP
- кодеки G.711,G.729, G.723.1.
- доступ к широкополосным интерфейсам ADSL/ADSL2+, VDSL, SHDSL и Ethernet
- поддержка сервисов ТфОП, ISDN, факсимильной связи, интерфейсов V.5 и xDSL.

Ёмкость MSAG ZXMSG5200 – 1856 аналоговых АЛ, 928 пользователей ADSL, минимум портов 240VoIP. MSAG поддерживает кодеки G.711, G.729a, G.723.1. В MSAG введена поддержка функций Hair-pin и self-switch.

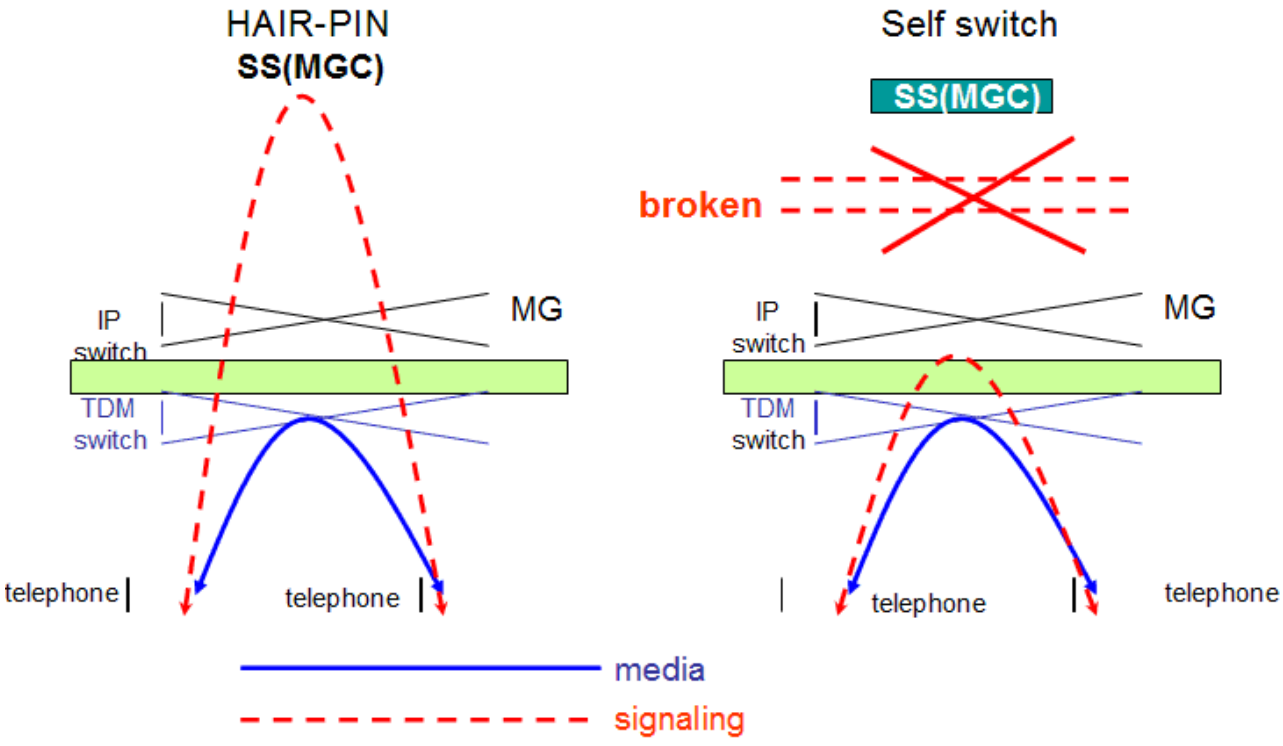


Рис.6.28. Функции Hair-pin и self-switch

На рис.6.29. показана структура полок MSAG. В полке имеются следующие платы:

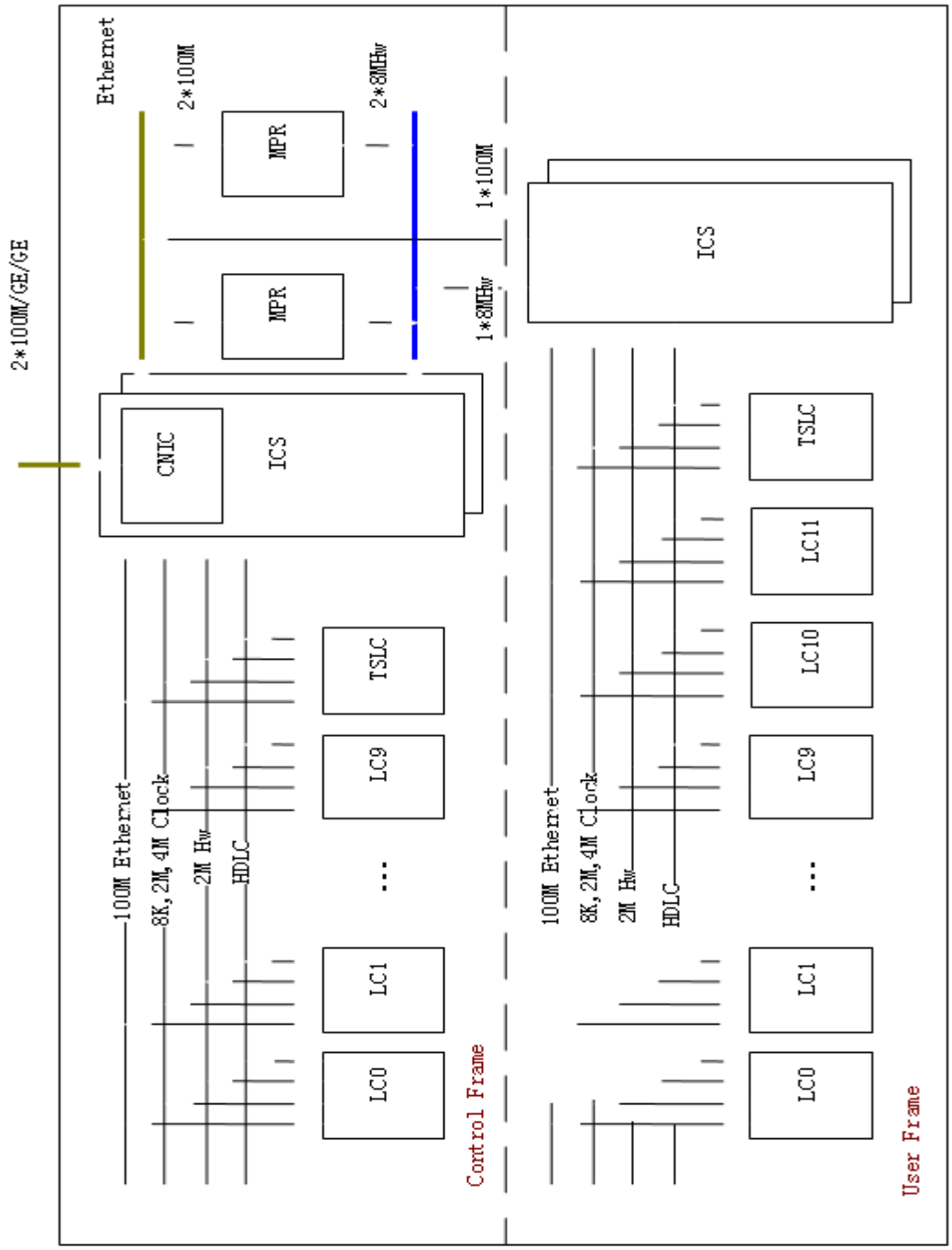


Рис. 6.29. Структура полки MSAG

ICS: Integrated Control and Switching Card – плата управления и коммутации
MPR: Packet Processing and Resource Card – плата пакетной обработки и распределения ресурсов
ULC: user line card – плата абонентской линии
TSLC :narrowband subscriber test card – плата тестирования узкополосной АЛ

Контрольные вопросы

1. В чем заключаются особенности построения перспективных телекоммуникационных сетей?
2. Какие требования предъявляются к современному оборудованию на телекоммуникационных сетях?
3. В чем преимущества использования пакетных способов передачи информации на сети доступа?
4. Какое оборудование применяют на сетях доступа с пакетной коммутацией?
5. В чем заключаются принципы взаимодействия абонентов телефонной и пакетной сети?
6. Каково назначение Softswitch?
7. Чем можно объяснить различную производительность Softswitch при обслуживании вызовов от различных источников?
8. Что реализует оборудование шлюзов?
9. Как называется оборудование, используемое для предоставления голосовых и мультимедийных услуг в пакетных сетях?
10. Какой тип шлюза реализует функции MG и SG одновременно?
11. Какое оборудование выполняет функции уровня услуг?
12. Что представляет собой IAD? Для чего он предназначен?
13. Что представляет собой технология VoIP?
14. Что представляет собой технология FoIP?
15. Какие типы существуют IAD?
16. Какие модели IAD выпускает фирма Huawei?
17. Что такое 10/100Base-T интерфейс?
18. Каково назначение MSAN?

7. ПРОГРАММНЫЙ КОММУТАТОР SOFTSWITCH

7.1. Декомпозиция АТС и Softswitch

Термин "Softswitch " был придуман при разработке интерфейса между интерактивной речевой системой (IVR) и АТС с коммутацией каналов в операторской компании MCI. На данном этапе развития *Softswitch* исполнял функции контроллера транспортного шлюза MGC (Media Gateway Controller) и Call Agent. Также на базе разработок специалистов из компаний Bellcore и Level3 Communication в IETF была создана первая спецификация протокола управления шлюзами MGCP (Media Gateway Control Protocol), которая является одной из ветвей родословной *Softswitch*. Другой предшественник *Softswitch* – привратник GK. На сегодняшний момент существует достаточное количество определений *Softswitch*, поэтому, для лучшего понимания, разумнее перечислить *основные функции Softswitch*.

- Управление обслуживанием вызовов, т.е. установлением и разрушением соединений путем выполнения функции Call Agent. Данные функции гарантируют, что соединение сохранится до тех пор, пока не даст отбой вызвавший или вызываемый абонент. Также в число функций входят распознавание и обработка цифр номера, распознавание момента ответа вызываемой стороны, момента, когда один из абонентов кладет трубку, и регистрация этих действий для начисления платы.
- Управление транспортными шлюзами и шлюзами доступа по протоколу H.248 и ему подобными.
- Координация обмена сигнальными сообщениями между сетями, т.е. поддержка функций SG (Signaling Gateway). Иначе говоря, *Softswitch* координирует действия, обеспечивающие соединение с логическими сетями в разных сетях и преобразует информацию в сообщениях, чтобы они были поняты на обеих сторонах несхожих сетей.

Дорогостоящие традиционные АТС в единой структуре объединяют функции коммутации, функции управления обслуживанием вызовов, услуги

и приложения, а также функции биллинга. Такая АТС представляет собой монолитную, закрытую системную структуру, как правило, не допускающую расширения или модернизации на базе оборудования других производителей. Революционное изменение принес *Softswitch*. Он в корне изменил традиционную закрытую структуру систем коммутации, используя принципы компонентного построения сети и открытые стандартные интерфейсы между тремя основными функциями: коммутации, управления обслуживанием вызовов, услуг и приложений. В такой открытой, распределенной структуре могут применяться функциональные компоненты разных производителей рис.7.1.

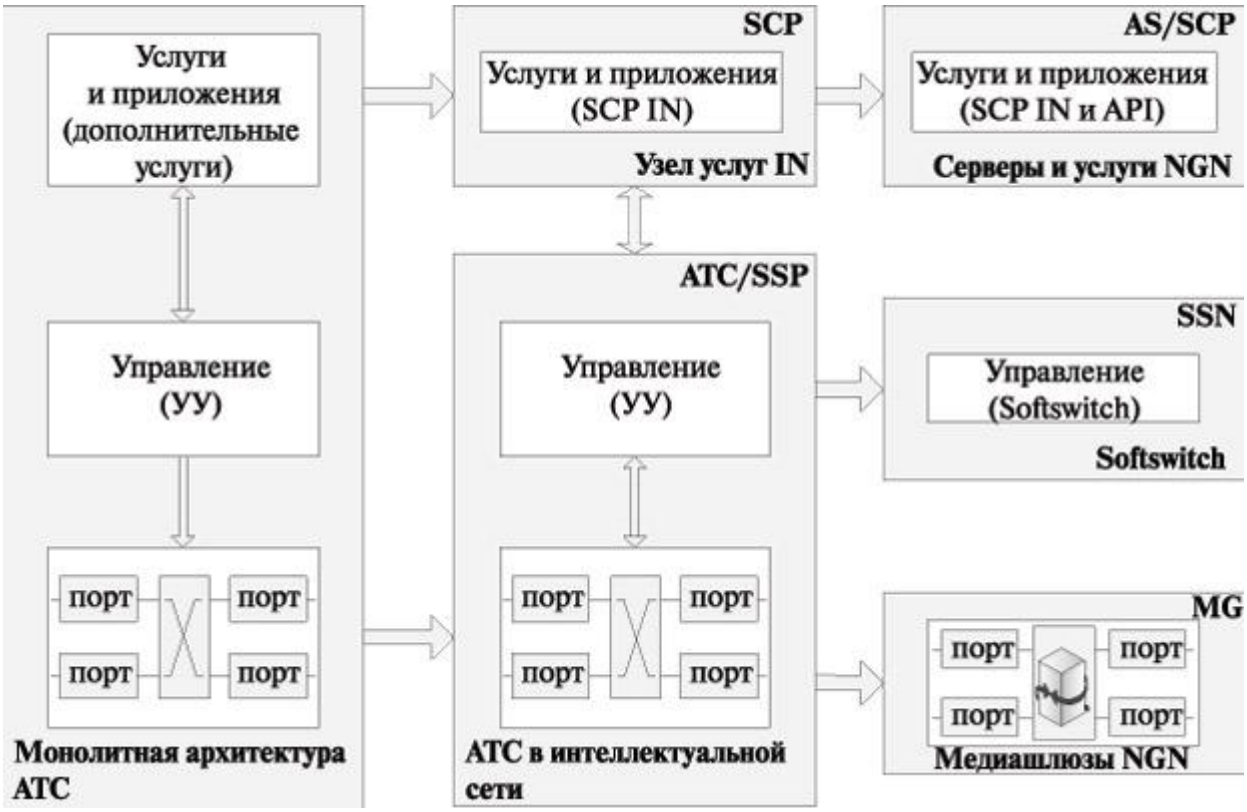


Рис. 7.1. Декомпозиция АТС и Softswitch

7.2. Эталонная архитектура Softswitch

Согласно эталонной архитектуре *Softswitch*, разработанной консорциумом IPCC (International Packet Communication Consortium), в ней предусматривается четыре представленные на рис.7.2 функциональные плоскости:

- транспортная;
- управления обслуживанием вызова и сигнализации;
- услуг и приложений;
- эксплуатационного управления.

Транспортная плоскость (Transport Plane) отвечает за транспортировку

Рис. 7.2. Эталонная архитектура Softswitch

сообщений по сети связи. Этими сообщениями могут быть сообщения сигнализации, сообщения маршрутизации для организации тракта передачи информации или непосредственно пользовательские речь и данные. Расположенный под этой плоскостью физический уровень переноса сообщений может базироваться на любой технологии, которая соответствует требованиям к пропускной способности для переноса трафика этого типа. Транспортная плоскость обеспечивает также доступ к сети IP-телефонии сигнальной и/или пользовательской информации, поступающей со сторонымдругих сетей или терминалов. Как правило, устройствами и функциями транспортной *плоскости управляют функции плоскости управления обслуживанием вызова и сигнализации*. Сама транспортная плоскость делится на три домена:

- домен транспортировки по протоколу IP;
- домен взаимодействия;
- домен доступа, отличного от IP.

Домен транспортировки по протоколу IP (IP transport domain) поддерживает магистральную сеть и маршрутизацию для транспортировки пакетов через сеть IP-телефонии. К этому домену относятся такие устройства, как коммутаторы, маршрутизаторы, а также средства обеспечения качества обслуживания (QoS).

Домен взаимодействия (Interworking Domain) включает в себя устройства преобразования сигнальной или пользовательской информации, поступающей со стороны внешних сетей, в вид, пригодный для передачи по сети IP-телефонии, а также обратное преобразование. В этот домен входят

такие устройства, как шлюзы сигнализации (Signaling Gateways), обеспечивающие преобразование сигнальной информации между разным транспортными уровнями; транспортные шлюзы, или медиашлюзы (Media Gateways), выполняющие функции преобразования пользовательской информации между разными транспортными сетями и/или разными типами мультимедийных данных; шлюзы взаимодействия (Interworking Gateways), обеспечивающие взаимодействие различных протоколов сигнализации на одном транспортном уровне.

Домен доступа, отличного от IP (Non-IP Access Domain), предназначен для организации доступа к сети IP-телефонии различных IP-несовместимых терминалов. Он состоит из шлюзов Access Gateways для подключения учрежденческих АТС, аналоговых кабельных модемов, линий xDSL, транспортных шлюзов для мобильной сети радиодоступа стандарта GSM/3G, а также устройств интегрированного абонентского доступа IAD (Integrated Access Devices) и других устройств доступа. IP-терминалы непосредственно подключаются к домену транспортировки по протоколу IP без участия Access Gateway.

Плоскость управления обслуживанием вызова и сигнализации (Call Control & Signaling Plane) управляет основными элементами сети IP-телефонии и в первую очередь теми, которые принадлежат транспортной плоскости. Она управляет обслуживанием вызова на основе сигнальных сообщений, поступающих из транспортной плоскости, устанавливает и разрушает соединения для передачи пользовательской информации по сети. Эта плоскость включает в себя такие устройства, как контроллер медиашлюзов MGC (Media Gateways Controller), сервер обслуживания вызова Call Agent, привратник Gatekeeper и LDAP-сервер.

Плоскость услуг и приложений (Service & Application Plane) содержит логику выполнения услуг и/или приложений в сети IP-телефонии и управляет этими услугами путем взаимодействия с устройствами, находящимися в плоскости управления обслуживанием вызова и сигнализации. Плоскость услуг и приложений состоит из таких устройств, как серверы приложений Application Servers и серверы дополнительных услуг Feature Servers. Она может также управлять специализированными компонентами передачи пользовательской информации, например, медиасерверами, которые выполняют функции конференц-связи, IVR и т.п.

Плоскость эксплуатационного управления (Management Plane) обеспечивает функции включения/выключения абонентов и услуг, эксплуатационной поддержки, биллинга и другие функции технической эксплуатации сети. Плоскость эксплуатационного управления может взаимодействовать с некоторыми или со всеми другими тремя плоскостями либо по стандартному протоколу (например по протоколу SNMP), либо по внутренним протоколам и через интерфейсы API.

7.3. Функциональные объекты

Функциональными объектами рассмотренной выше эталонной модели архитектуры *Softswitch* являются логические объекты сети IP-телефонии. В рамках предложенного Консорциумом подхода выделяются 12 основных функциональных объектов, относительно которых следует прежде всего подчеркнуть, что это суть функции, а не физические продукты. Последнее означает, что разные функциональные объекты могут физически располагаться в разных автономных устройствах или на многофункциональных платформах и что существует практически неограниченное число способов размещения функциональных объектов в физических объектах. Изменим рис.7.2 таким образом, чтобы разместить эти 12 автономных функциональных объектов (ФО) на плоскостях эталонной архитектуры *Softswitch* рис.7.3.

Рис. 7.3. Функциональные объекты эталонной архитектуры Softswitch

ФО контроллера медиашлюзов (MGC-F)

ФО контроллера медиашлюзов MGC-F (Media Gateways Controller Function) представляет собой конечный автомат логики обслуживания вызова и сигнализации управления его обслуживанием для одного или более транспортных шлюзов. MGC-F определяет состояние процесса обслуживания каждого вызова в медиашлюзе и состояния информационных каналов

интерфейсов MG-F, передает информационные сообщения пользователя от одного MG-F к другому, а также от/к MG-F к/от IP-телефонам или терминалам, отправляет и принимает сигнальные сообщения от портов, от других MGC-F и от внешних сетей, взаимодействует с AS-F для предоставления услуг пользователю, имеет возможность управлять некоторыми сетевыми ресурсами (например портами MGF, полосой пропускания и т.д.) и устанавливать правила для портов пользователя, взаимодействует с R-F и A-F для обеспечения маршрутизации вызова, аутентификации и учета, а также может участвовать в задачах эксплуатационного управления в мобильной среде (т.к. управление мобильностью обычно является частью CA-F). Функциональный объект MGC-F обычно использует протоколы H.248 и MGCP.

ФО устройства управления и взаимодействия (CA-F) и функциональный объект взаимодействия (IW-F)

ФО устройства управления шлюзом CA-F (Call Agent Function) и функциональный объект взаимодействия IW-F (Interworking Function) являются подмножествами MGC-F. Первый из них, CA-F, существует, когда MGC-F управляет обслуживанием вызова и определяет состояния процесса его обслуживания. Протоколами этого функционального объекта могут являться SIP, SIP-T, BICC, H.323, Q.931, Q.SIG, INAP, ISUP, TCAP, BSSAP, RANAP, MAP и CAP, а в качестве интерфейсов API используются любые открытые API типа JAIN или Parlay. Второй функциональный объект, IW-F, существует, когда MGC-F обеспечивает взаимодействие между разными сетями сигнализации, например, IP и ATM, ОКС7 и SIP/H.323 и т.п.

ФО маршрутизации и учета стоимости (R-F и A-F)

ФО маршрутизации и учета стоимости R-F и A-F (Call Routing и Accounting Functions) работают следующим образом. Функциональный объект R-F предоставляет информацию о маршрутизации вызова функциональному объекту MGC-F. Функциональный объект A-F собирает учетную информацию о вызовах для целей биллинга, а также может выполнять более широкий спектр функций AAA, т.е. обеспечивать аутентификацию, идентификацию и учет в удаленных сетях. Основная роль обоих объектов – реагировать на запросы, поступающие от одного или более MGC-F, направляя вызов или учетную информацию о нем к входящим портам (другим MGC-F) или услугам (AS-F). Функциональный объект R-F/A-F обеспечивает маршрутизацию локальных и межсетевых вызовов (R-F), фиксирует детали каждого сеанса связи для целей биллинга и планирования (A-F), обеспечивает управление сеансом и управление мобильностью, может узнавать о маршрутной информации от внешних источников, может взаимодействовать с AS-F для предоставления услуги пользователю, может функционировать прозрач но для других элементов в тракте сигнализации. Здесь R-F и A-F могут сцепляться друг с другом последовательно или иерархически и к тому же R-F/A-F часто объединяется с MGC-F, причем объединенный R-F/A-F/MGC-F может также запрашивать услуги внешнего

R-F/A-F. Сам A-F собирает и передает учетную информацию по каждому вызову, а AS-F передает учетную информацию по предоставлению дополнительных сервисов, таких как конференц-связь или платные информационные услуги. Функция маршрутизации локальных и межсетевых вызовов R-F может использовать протоколы ENUM и TRIP, а функция стоимости вызовов A-F может использовать протоколы RADIUS и AuC (для сетей подвижной связи).

ФО SIP-прокси-сервера (SPS-F)

ФО SIP-прокси-сервера SPS-F (SIP Proxy Server Function) выделен в отдельный функциональный объект по той причине, что чаще всего R-F и A-F конструктивно оформляются в виде прокси-сервера SIP. ФО шлюза сигнализации SG-F (Signaling Gateway Function) поддерживает обмен между сетью IP-телефонии и ТфОП u1089 сигнальной информацией, которая может передаваться, например, на базе ОКС7/TDM или BICC/ATM. Для беспроводных сетей подвижной связи SG-F также поддерживает обмен сигнальной информацией между транзитной пакетной IP-сетью и сетью сотовой подвижной связи (СПС) с коммутацией каналов на базе стека ОКС7. Основная роль SG-F заключается в пакетировании и транспортировке информации протоколов сигнализации ОКС7 в ТфОП (ISUP или INAP) или в СПС (MAP или CAP) по сети с коммутацией пакетов IP. Для этого функциональный объект SG-F пакетирует и транспортирует сигнализацию ОКС7 к MGC-F или другому SG-F, используя методы SIGTRAN. Один SG-F может обслуживать много MGC-F, а интерфейсом между SG-F и другими функциональными объектами служат протоколы SIGTRAN типов TUA, SUA и M3UA over SCTP, за исключением ситуаций, когда SG-F и MGC-F или другой SG-F объединены.

ФО сигнализации шлюза доступа (AGS-F)

ФО сигнализации шлюза доступа AGS-F (Access Gateway Signaling Function) поддерживает обмен сигнальной информацией между сетью IP-телефонии и сетью доступа с коммутацией каналов на базе интерфейсов V5.1/V5.2. Для беспроводных сетей подвижной связи AGS-F поддерживает также обмен сигнальной информацией между транзитной сетью подвижной связи с коммутацией пакетов и сетью СПС на базе TDM или ATM. Основная роль AGS-F заключается в пакетировании и транспортировке информации протоколов сигнализации интерфейсов V5 или ISDN (для проводных сетей), или BSSAP или RANAP (для беспроводных сетей) по сети с коммутацией пакетов IP. AGS-F пакетирует и транспортирует к MGC-F эту информацию протоколов сигнализации V5, ISDN или ОКС7, используя протоколы SIGTRAN типов M3UA, IUA и V5UA over SCTP.

ФО сервера приложений (AS-F)

ФО сервера приложений AS-F (Application Server Function) поддерживает логику и выполнение услуг для одного или более приложений. AS-F может запрашивать у MGC-F прекращение вызовов или сеансов связи для определенных приложений (например речевой почты или конференц-связи),

запрашивать у MGC-F повторное инициирование услуг связи (например сопровождающего вызова или вызовов по предоплаченной телефонной карте), может изменять описания u1087 потоков пользовательских данных, участвующих в сеансе, используя протокол SDP, может управлять MS-F для обслуживания потоков пользовательской информации, может компоноваться с web-приложениями или иметь web-интерфейсы, может использовать открытые API типа JAIN или Parlay для создания услуг, может иметь внутренние интерфейсы алгоритма распределения ресурсов, биллинга и регистрации сеансов, взаимодействовать с функциональными объектами MGC-F или MS-F, вызывать другой AS-F для предоставления дополнительных услуг или для построения составных сервисов, ориентированных на компоненты приложений, использовать функциональные возможности MGC-F для управления внешними ресурсами. Для всех этих целей применяются протоколы SIP, MGCP, H.248, LDAP, HTTP, CPL и XML. Совместное использование функциональных объектов AS-F и MGC-F обеспечивает поддержку составных услуг, таких как сетевые записанные объявления, трехсторонняя связь, уведомление о поступлении нового вызова и т.д. В ситуациях, когда AS-F и MGC-F реализованы в одной системе, вместо подключения AS-F к MGC-F по одному из вышеуказанных протоколов производители часто используют API типа JAIN или Parlay. При такой организации AS-F называют сервером дополнительных услуг (Feature Server).

ФО управления услугами (SC-F)

ФО управления услугами SC-F (Service Control Function) существует, когда AS-F управляет логикой услуг. SC-F использует протоколы INAP, CAP и MAP, а также открытые API типа JAIN и Parlay. ФО медиашлюза MG-F (Media Gateway Function) обеспечивает сопряжение IP-сети с портом доступа, соединительной линией либо с совокупностью портов и/или соединительных линий, т.е. служит шлюзом между пакетной сетью и внешними сетями с коммутацией каналов, такими как ТфОП, СПС или АТМ. Его основная роль состоит в преобразовании пользовательской информации из одного формата в другой, чаще всего – из канального вида в пакетный и обратно, из ячеек АТМ в пакеты IP и обратно. MG-F имеет следующие характеристики:

- всегда состоит в отношениях "ведущий/ведомый " с MGC-F, используя протокол управления MGCP или MEGACO/H.248;
- может выполнять функции обработки пользовательской информации, такие как кодирование, пакетирование, компенсацию эха, управление буферами, устранения джиттера, корректирующие действия при потерях пакетов и др.;
- может выполнять функции обслуживания пользовательских соединений, такие как генерирование акустических сигналов, генерирование сигналов DTMF, генерирование комфортного шума и др., а также выполнять анализ цифр на базе таблицы, загружаемой от MGC-F;

- может выполнять функции сигнализации и обнаружения событий, такие как обнаружение сигналов DTMF, обнаружение состояний отбоя/ответа абонента, детектирование наличия речевых сигналов и др.

Таким образом, MG-F обеспечивает механизм, позволяющий MGC-F контролировать состояние и функциональные возможности портов, а сам не требует знать состояния процессов обслуживания вызовов, проходящих через него, поддерживая только состояния соединений. Используемые протоколы: RTP/RTCP, TDM, H.248 и MGCP. Кстати, SIP-телефон или шлюз с поддержкой SIP с этой точки зрения представляет собой MG-F и MGC-F в одном блоке.

ФО медиасервера MS-F

ФО медиасервера MS-F (Media Server Function) обеспечивает управление обработкой пользовательского пакетного трафика от любых приложений. В основном он функционирует в качестве сервера, обслуживающего запросы от AS-F или MGC-F, касающиеся обработки пользовательской информации в пакетированных потоках мультимедиа. MS-F поддерживает различные кодеки и схемы кодирования, может управляться либо AS-F или MGC-F непосредственно (управление ресурсами), либо косвенно (вызов функции) с использованием протоколов SIP, MGCP и H.248.. Функциональный объект MA-F может параллельно поддерживать обнаружение набираемых цифр, генерирование и передачу акустических сигналов и записанных сообщений, регистрацию и запись мультимедийных потоков, распознавание речи, речевое воспроизведение текста, микширование для конференц-связи, обработку факсимильных сообщений, определение наличия речевых сигналов и передачу информации о громкости.

7.4. Реализация Softswitch – сетевая конфигурация, предложенная консорциумом IPCC

Общими задачами *ССП*, определенными ITU и ETSI, являются разделение функций переноса информации через сеть, а также отделение функций услуг и приложений от собственно связных функций. Таким образом, речь идет о распределенной архитектуре, в которой связь между компонентами осуществляется исключительно через открытые интерфейсы.

Первый пример сетевой конфигурации, предложенный консорциумом IPCC, представлен на рис.7.4. Элементами изображенной на этом рисунке сети являются *Softswitch*, сервер приложений AS (Application Server), шлюз между ТфОП и IP-сетью TG (Trunk Gateway), шлюз доступа AG (Access Gateway), шлюз сигнализации SG (Signaling Gateway) и транспортный медиасервер MS (Media Server).

Softswitch в данном примере выполняет функции MGC-F, R-F и A-F, обсуждавшиеся в лекции 12, обрабатывает всю сигнализацию, управляет TG, AG и соответствующим выделением медиаресурсов, а также обеспечивает

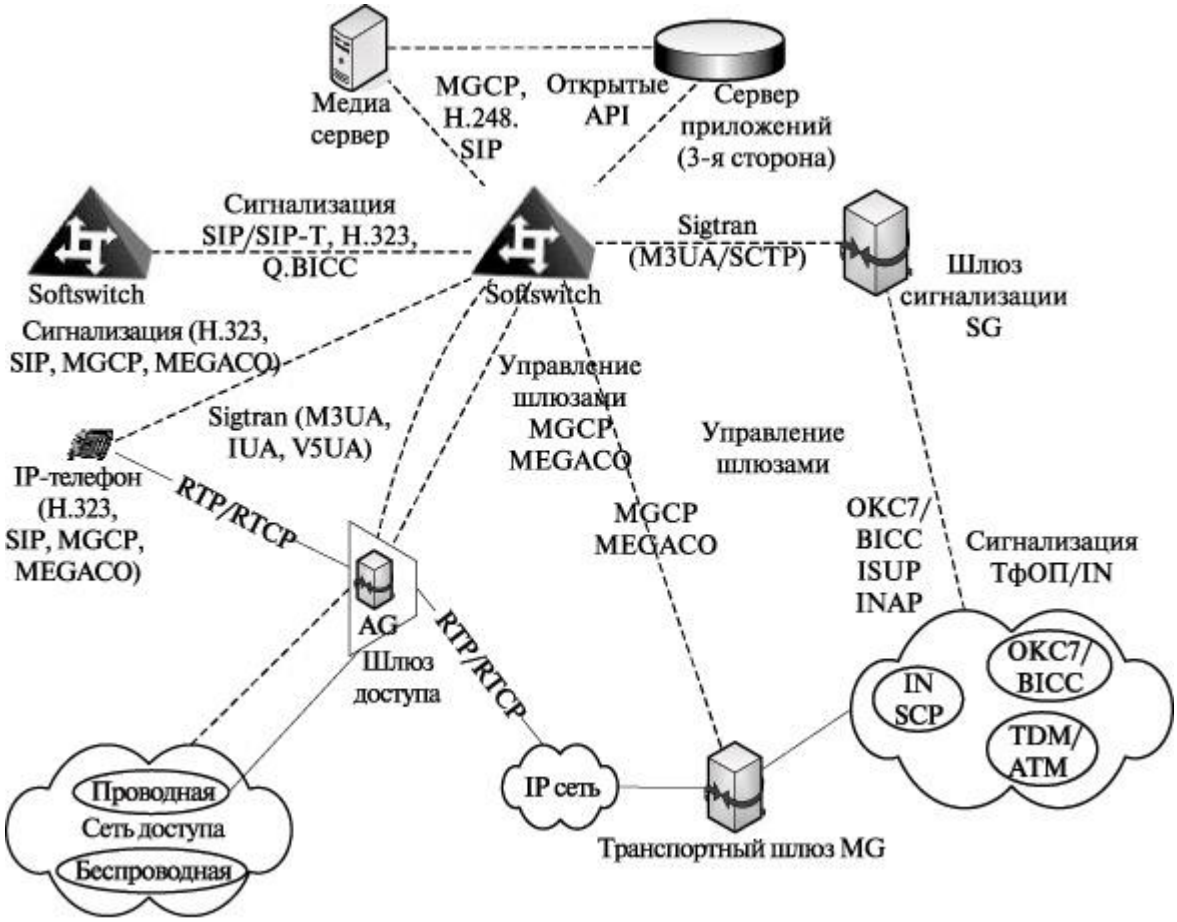


Рис. 7.4. Пример архитектуры ССП

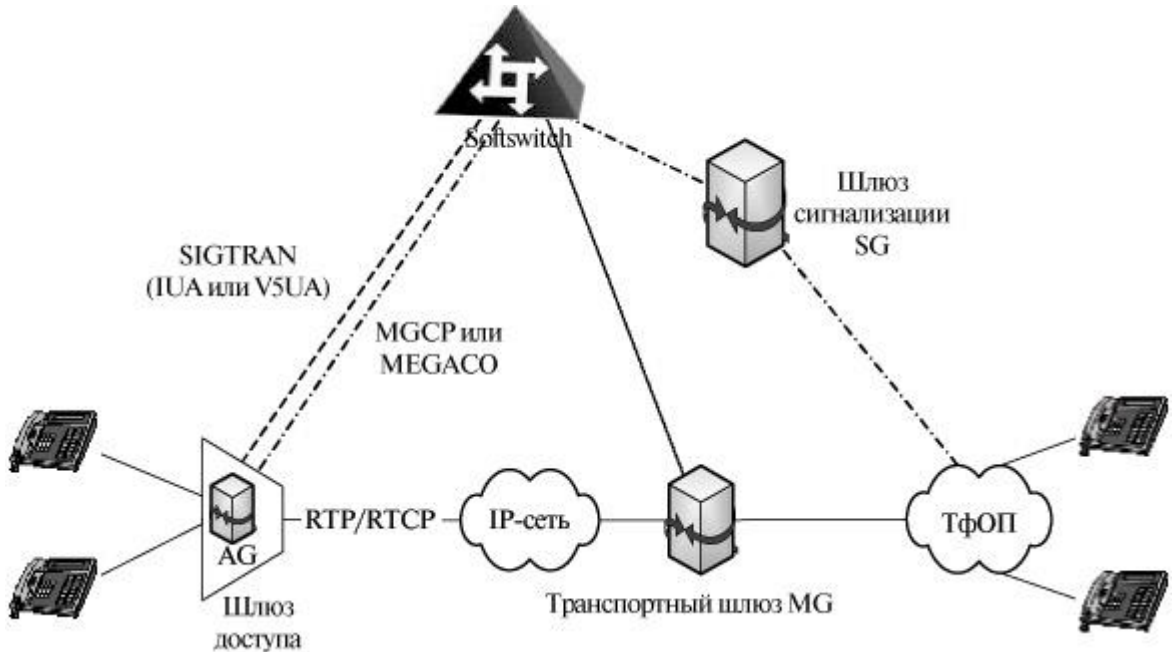


Рис. 7.5. Пример с ISDN и V5

получение учетной информации. Кроме того, каждый *Softswitch* взаимодействует с другими *Softswitch* по протоколам SIP/SIP-T, H.323 или BICC.

Сервер приложений AS реализует логику услуг. Вызов, который требует дополнительную услугу, либо может быть передан от *Softswitch* к AS для дальнейшего управления этой услугой, либо сам *Softswitch* может получать информацию от AS, необходимую для выполнения логики услуги. Сервер приложения AS может сам управлять MS или передать управление им *Softswitch*.

На *транспортный шлюз* TG поступают потоки пользовательской (речевой) информации со стороны ТфОП, он преобразует эту информацию в пакеты и передает ее по протоколу IP в сеть с маршрутизацией пакетов, причем делает все это под управлением *Softswitch*.

Шлюз доступа AG служит интерфейсом между IP-сетью и проводной или беспроводной сетью доступа, передает сигнальную информацию к *Softswitch*, преобразует пользовательскую информацию и передает ее либо к другому порту этой же IP-сети, либо в другую сеть с коммутацией пакетов, либо к TG для последующей передачи в сеть с коммутацией каналов. Функциональным объектом MG-F в составе AG также управляет *Softswitch*. Сигнальный шлюз SG обеспечивает доставку сигнальной информации, поступающей со стороны ТфОП, а также перенос сигнальной информации в обратном направлении.

Медиасервер MS может выполнять такие задачи, как, например, передачу записанных объявлений и накопление цифр номера, хотя в большинстве случаев цифры накапливает шлюз AG. Сервером MS может управлять либо *Softswitch*, либо AS, либо оба этих сетевых элемента. На рис.7.5 показан пример сети доступа на базе протокола V5 и ISDN.

Шлюз доступа AG обменивается сигнальной информацией V5 или ISDN с сетью доступа и является окончанием физического соединения, по которому переносится сигнальная информация V5 или ISDN. Затем он передает эту информацию по IP-сети к *Softswitch* с помощью протоколов сигнализации SIGTRAN (V5UA или IUA). Речевую информацию AG преобразует в пакетную форму и пересылает ее в виде пакетов устройству, преобразующему пакетированную речь обратно в TDM-форму и затем передающему ее в сеть ТфОП.

На рис.7.6 показан пример реализации VoIP-сети, использующей сеть доступа с технологий DSL. Обычные аналоговые телефоны и любые устройства локальной сети Ethernet подключаются к устройству интегрированного доступа IAD абонента, которое обрабатывает и передает абонентскую сигнальную информацию по IP-сети или через мультиплексор доступа DSLAM к *Softswitch*. Что касается речевой информации, то IAD оцифровывает ее, пакетирует и переносит в виде пакетов RPT по IP-сети.

Эти три примера иллюстрируют базовое свойство сетей *ССП* – интеграцию передачи речи, данных и видеоинформации, включая

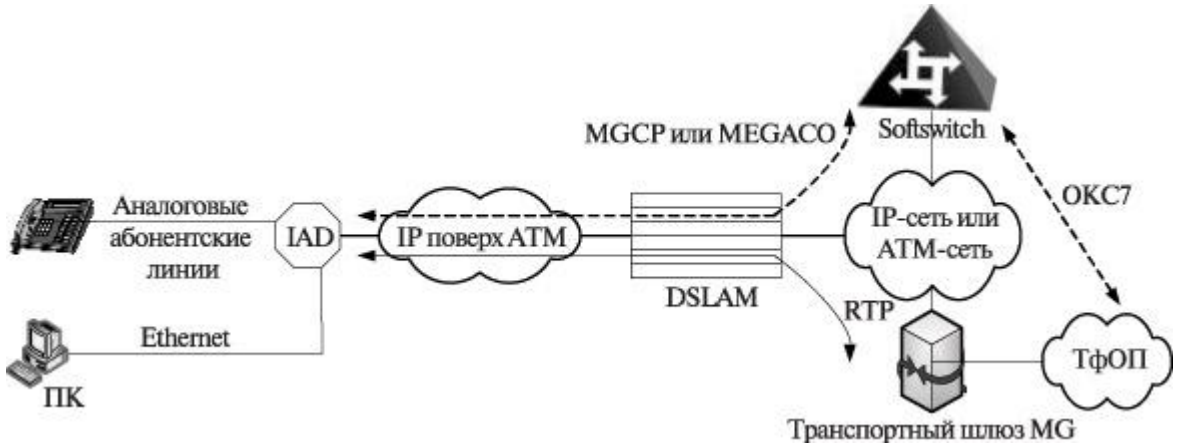


Рис.7.6. Архитектура ССП с IAD и DSLAM

объединение оборудования и функциональных возможностей как на уровне опорной сети (Core Network), так и на уровне сети доступа (Access Network).

7.5. Взаимодействие Softswitch и ОКС7

Концепция SIGTRAN нацелена на надежный перенос сигнальной информации ОКС7 через IP-сеть. Для этого *Softswitch* взаимодействует с рядом шлюзов MG, расположенных поблизости от источников и приемников информации в ТфОП (на границах IP-сети). Взаимодействие обычно обеспечивается при наличии по крайней мере двух сигнальных шлюзов SG, в которые включены сигнальные звенья ОКС7. Эта архитектура показана на рис.7.7, причем в число используемых протоколов входят SCTP, M3UA или M2UA.

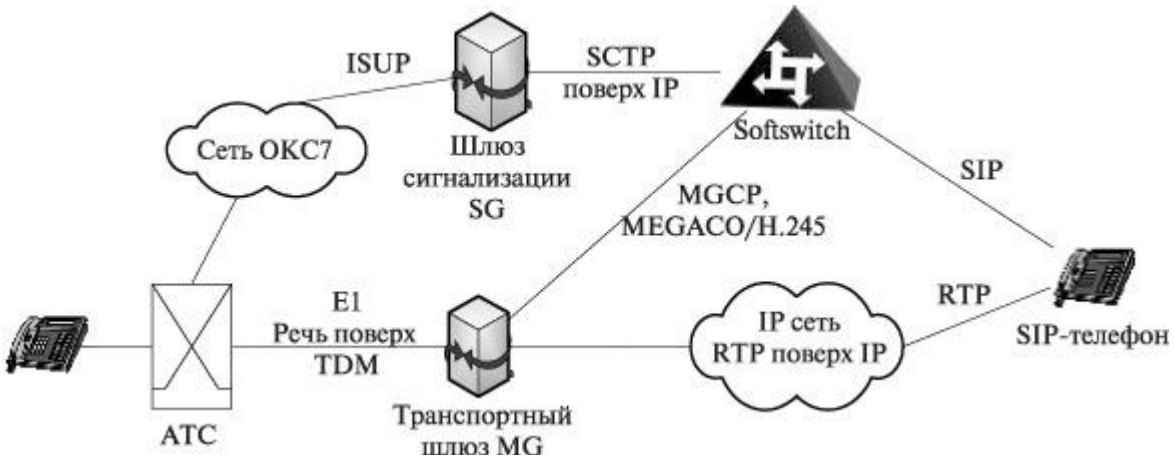


Рис. 7.7. Взаимодействие ОКС7 и архитектуры Softswitch

7.6. Оборудование Softswitch в качестве транзитной станции

В зоновых сетях связи, в которых имеется сегмент транспортной сети на базе технологии коммутации пакетов, оборудование *Softswitch* может использоваться для обеспечения транзита внутризонового трафика в пределах телефонной зоны или для транзита голосового трафика в местной сети связи. При внедрении технологии *Softswitch* обеспечивается повышение эффективности использования существующей транспортной сети с коммутацией пакетов за счет организации передачи по ней голосового трафика.

Внедрение технологии *Softswitch* и технологии пакетной коммутации позволяет параллельно существующей инфраструктуре с коммутацией каналов создать сегмент телефонной сети на базе коммутации пакетов. Вначале этот сегмент может использоваться, например, для пропуска пиковой нагрузки или для организации резервных маршрутов. Также это позволяет отказаться от использования устаревших транзитных станций коммутации и заменить их коммутацией пакетов. Кроме того, при строительстве новых станций коммутации передача транзитной нагрузки между ними также может осуществляться по сети с коммутацией пакетов.

К *основным преимуществам* внедрения технологий пакетной коммутации и технологии *Softswitch* для организации телефонной нагрузки следует отнести создание сетевой инфраструктуры, которая может стать основой для организации распределенной станции коммутации и платформы для предоставления дополнительных услуг, в том числе для пользователей, подключенных к сети связи по IP. Кроме того, при использовании *Softswitch* возможно уменьшение числа пунктов сигнализации, включая транзитные пункты, в сети ОКС №7.

7.7. Оборудование Softswitch в качестве распределенной оконечной станции коммутации

Оборудование *Softswitch* может использоваться для подключения сетей абонентского доступа или оконечного (пользовательского) оборудования. Как правило, обеспечивается возможность подключения аналоговых телефонов, ISDN-телефонов, SIP/H.323-телефонов. Оборудование *Softswitch* большинства производителей позволяет обеспечить подключение по интерфейсу V5.

Функции по управлению вызовом – прием и обработка сигнальной информации, ведение учета стоимости, сбора статистики — обеспечиваются со стороны контроллера управления шлюзами. Функции по коммутации пользовательских соединений обеспечиваются со стороны шлюзов доступа или со стороны оборудования IP-концентраторов в случае SIP/H.323-телефонов.

Оконечные станции коммутации местной сети могут быть заменены оптическими сетями доступа, что дает возможность развивать услуги на базе IP.

К основным преимуществам организации распределенной оконечной станции на базе оборудования *Softswitch* и технологий коммутации пакетов можно отнести следующие:

- расширение перечня предоставляемых дополнительных услуг связи, в том числе за счет возможности предоставления услуг IP-Centrex, конвергированных услуг связи, реализуемых на базе шлюзов Parlay и/или серверов приложений;
- возможность создания выносов, которые обеспечивают не только концентрацию абонентских линий, но также высокоскоростной доступ к Интернету и предоставление различных дополнительных и интеллектуальных услуг связи, реализуемых на базе шлюзов Parlay и/или серверов приложений;
- возможность предоставления пользователям делового сектора услуг передачи голосовой информации с использованием технологий VoIP или VoATM. Эти технологии могут использоваться при организации корпоративных сетей и позволяют за счет реализации в шлюзах алгоритмов компрессии речи уменьшить требуемую полосу пропускания в 1,5-4 раза в зависимости от типа используемого кодека;
- возможность предоставления пользователям делового сектора услуг VPN;
- увеличение до необходимого количества точек присоединения для присоединения телефонных сетей взаимодействующих операторов путем установки дополнительных шлюзов;
- упрощение реализации гибкой тарифной политики. Поскольку оборудование *Softswitch* базируется на централизованном управлении установлением/разъединением соединений, существует возможность обеспечить применение гибких тарифных планов в отношении абонентов всей сети, построенной на базе оборудования *Softswitch*, из одной точки.

7.8. Оборудование Softswitch в качестве распределенного SSP

Оборудование *Softswitch* базируется на технологии распределенной коммутации и позволяет организовать распределенный узел коммутации услуг SSP, который обеспечивает доступ пользователей к интеллектуальным услугам, реализованным в существующих SCP. Функция коммутации услуг (SSF) реализуется за счет совместного функционирования шлюзов и контроллера шлюзов (MGC).

При этом функция интерфейса с SCP и функция управления установлением соединения при предоставлении интеллектуальных услуг реализуются в MGC. В качестве протокола взаимодействия между SSP и SCP должен использоваться INAP-R.

По сравнению с построением интеллектуальной сети связи на базе классической платформы ИСС организация распределенного SSP на базе оборудования *Softswitch* имеет следующие преимущества:

- минимизация инвестиций на внедрение функции SSF. В "классическом" варианте необходимо либо модернизировать все станции коммутации, в которых должна осуществляться обработка вызовов от пользователей интеллектуальными услугами, либо устанавливать оборудование выделенного SSP в нескольких сетевых точках;
- минимизация инвестиций на расширение функций SSF в случае модернизации или внедрения новых интеллектуальных услуг. В "классическом" варианте модернизировать приходится все точки SSP, в случае распределенного SSP – только функциональность MGC;
- возможность организации доступа к интеллектуальным услугам, реализованным как в сетях, базирующихся на технологии коммутации пакетов, так и в сетях, базирующихся на коммутации каналов, в рамках единой сетевой инфраструктуры;
- возможность предоставления расширенного списка интеллектуальных услуг за счет серверов приложений, управляемых со стороны оборудования *Softswitch*;
- возможность предоставления дополнительных (интеллектуальных) услуг, включая персональную мобильность, конвергированные услуги, требующие интеграции сетей связи.

7.9. Оборудование Softswitch в качестве распределенного узла телематических служб

В качестве распределенного узла телематических служб оборудование *Softswitch* позволяет:

- создать точки доступа в Интернет;
- предоставлять доступ к услугам местной и внутризоновой передачи голосовой информации по сетям передачи данных с использованием нумерации телефонной сети;
- организовать передачу информации по сети передачи данных без использования нумерации телефонной сети (SIP-телефония);
- предоставлять услуги мультимедиа и т.д.

Точки доступа (POP) в сеть Интернет реализуются в шлюзах, обеспечивающих терминацию коммутируемого соединения на сеть передачи данных. Задачей шлюзов в этом случае является преобразование информации, передаваемой в режиме коммутируемого соединения (dial-up) по сети с коммутацией каналов, в пакеты IP. Сервер авторизации доступа (RAS) может входить в состав оборудования *Softswitch* либо может быть реализован как отдельное оборудование.

Доступ к услугам местной и внутризоновой передачи голосовой

информации по сетям передачи данных с использованием нумерации телефонной сети может быть организован с использованием телефонных карт. В этом случае в оборудовании *Softswitch* должен быть реализован алгоритм распознавания дополнительной адресной информации, применяемой для идентификации вызываемого абонента.

Для предоставления услуг передачи информации по сети передачи данных без использования нумерации телефонной сети (IP-телефонии) необходимо обеспечить преобразование имен или адресов пользователей в адреса IP. Для этого может быть использована система ENUM (система единых коммуникационных номеров), позволяющая по URI (единообразный идентификатор ресурсов) определить адрес IP.

Предоставление услуг мультимедиа ориентировано на пользователей, использующих терминалы мультимедийных сетей (SIP/H.323). Основными приложениями мультимедиа в настоящее время являются: мультимедийные конференции, услуги аудио и видео по запросу, игры. Предоставление услуг мультимедиа реализуется за счет использования серверов мультимедиа, устанавливаемых в сети на базе коммутации пакетов.

Основным преимуществом использования решений на базе *Softswitch* при построении распределенного узла телематических служб является возможность использования единой сетевой инфраструктуры для предоставления существующих и перспективных телематических услуг. При этом обеспечивается:

- возможность гибкого внедрения новых дополнительных услуг за счет наличия в шлюзах Parlay стандартных прикладных интерфейсов;
- возможность обеспечения роуминга услуг за счет взаимодействия шлюзов Parlay, установленных в разных сетях с сервером приложений, в котором реализована услуга;
- возможность гибкой тарифной политики;
- централизованный сбор тарифной и статистической информации;
- уменьшение эксплуатационных расходов за счет централизации точки контроля за предоставлением услуг.

Необходимо отметить, что в зависимости от производителя оборудование *Softswitch* может быть ориентировано на одно или на несколько из вышеперечисленных применений. Наибольший эффект от сети на базе оборудования *Softswitch* может достигаться только при наличии сети с коммутацией пакетов, обеспечивающей гарантированное качество обслуживания при передаче голосовой информации. При этом оборудование *Softswitch* должно позволять использовать его в нескольких сетевых сценариях, а именно, в качестве транзитной станции коммутации и местной оконечной станции коммутации и также в качестве платформы для предоставления дополнительных (интеллектуальных и телематических) услуг.

Контрольные вопросы

1. Перечислите функциональные плоскости эталонной архитектуры Softswitch, разработанной консорциумом IPCC.
2. Какая функциональная плоскость отвечает за транспортировку сообщений по сети связи?
3. Какой домен транспортной плоскости поддерживает магистральную сеть и маршрутизацию для транспортировки пакетов через сеть IP-телефонии?
4. Какая функциональная плоскость управляет обслуживанием вызова на основе сигнальных сообщений, поступающих из соседней плоскости, устанавливает и разрушает соединения для передачи пользовательской информации по сети?
5. В какой функциональной плоскости находятся серверы приложений Application Servers и серверы дополнительных услуг Feature Servers?
6. Какая функциональная плоскость поддерживает функции включения/выключения абонентов и услуг, эксплуатационной поддержки, биллинга и другие функции технической эксплуатации сети?
7. Кто обеспечивает функции по коммутации пользовательских соединений в случае применения Softswitch в качестве распределенной оконечной станции коммутации?
8. Каковы недостатки применения Softswitch в качестве распределенного SSP?
9. Каковы преимущества применения Softswitch в качестве распределенного SSP?

8. IMS - IP MULTIMEDIA SUBSYSTEM

8.1. Стандартизация IMS
8.2. Архитектура IMS
8.3. Сравнение Softswitch и IMS

Несмотря на постоянно растущую сложность телекоммуникационных устройств и систем, протоколов и приложений, работы в направлении создания универсальной сетевой инфраструктуры продолжаются, проходя последовательно этапы узкополосных цифровых сетей интегрального обслуживания (сетей ISDN), широкополосных сетей ISDN (B-ISDN), сетей следующего поколения (ССП). Наконец, создание концепции IMS – мультимедийной IP-ориентированной подсистемы связи, – по мнению разработчиков оборудования, операторов и организаций стандартизации, открывает путь к построению такой универсальной сетевой инфраструктуры.

Ключевыми факторами перехода к IMS являются следующие..

Концепция IP Multimedia Subsystem (IMS) описывает новую сетевую архитектуру, основным элементом которой является пакетная транспортная сеть, поддерживающая все технологии доступа и обеспечивающая реализацию большого числа инфокоммуникационных услуг. Ее авторство принадлежит международному партнерству Third Generation Partnership Project (3GPP), объединившему European Telecommunications Standartization Institute (ETSI) и несколько национальных организаций стандартизации.

IMS изначально разрабатывалась применительно к построению мобильных сетей 3-го поколения на базе протокола IP. В дальнейшем концепция была принята Комитетом ETSI-TISPAN, усилия которого были направлены на спецификацию протоколов и интерфейсов, необходимых для поддержки и реализации широкого спектра услуг в стационарных сетях с использованием стека протоколов IP.

В настоящее время архитектура IMS рассматривается многими операторами и сервис-провайдерами, а также поставщиками оборудования как возможное решение для построения сетей следующего поколения и как основа конвергенции мобильных и стационарных сетей на платформе IP.

Причину возникновения концепции IMS именно в среде разработчиков стандартов для мобильных сетей можно объяснить следующим образом. В последние годы операторы стационарных сетей активно поддерживают переход от традиционных телефонных сетей к ССП, связывая с ними определенные надежды на сокращение операционных расходов и капитальных вложений, а также на развитие новых услуг, ожидая, как следствие, существенного повышения доходов.

Естественно, идея построения ССП оказалась привлекательной и для мобильных операторов, которые в последние годы столкнулись с резким падением доходов, что связано, в том числе, и с дерегулированием рынка, ростом конкуренции, тарифными войнами, высоким оттоком абонентов и т.д.

Однако следует признать, что основная технологическая идея ССП – разделение транспортных процессов и процессов управления вызовами и сеансами на базе элементов платформы Softswitch – не была поддержана своевременной разработкой соответствующего набора стандартов. Это привело к тому, что основные сетевые элементы ССП, поставляемые различными производителями, зачастую оказываются несовместимыми между собой.

В сетях мобильных операторов, где одним из основных источников доходов является роуминг, такая несовместимость оказывается куда более значительным недостатком, чем в стационарных сетях. Именно это и определило активность международных организаций (в первую очередь ETSI и 3GPP), которые начали разработку новых принципов построения и стандартов мобильных сетей 3G, основываясь на уровневой архитектуре ССП.

По существу концепция IMS возникла в результате эволюции сетей UMTS, когда область управления мультимедийными вызовами и сеансами на базе протокола SIP добавили к архитектуре сетей 3G. Среди основных свойств архитектуры IMS можно выделить следующие:

- многоуровневость – разделяет уровни транспорта, управления и приложений;
- независимость от среды доступа – позволяет операторам и сервис-провайдерам конвергировать фиксированные и мобильные сети;
- поддержка мультимедийного персонального обмена информацией в реальном времени (например голос, видео-телефония) и аналогичного обмена информацией между людьми и компьютерами (например игры);
- полная интеграция мультимедийных приложений реального и нереального времени (например потоковые приложения и чаты);
- возможность взаимодействия различных видов услуг;
- возможность поддержки нескольких служб в одном сеансе или организации нескольких одновременных синхронизированных сеансов.

20.1. Стандартизация IMS

Стандартизация архитектуры IMS является предметом внимания широкого круга международных организаций, благодаря ключевой роли IMS в эволюции сетей в направлении к ССП. Концепция IMS в ее настоящем виде является, главным образом, результатом работ трех международных организаций по стандартизации – 3GPP, 3GPP2 и ETSI.

Партнерство 3GPP было создано в конце 1998 г. по инициативе института ETSI с целью разработки технических спецификаций и стандартов для мобильных сетей связи 3-го поколения (сетей UMTS), базирующихся на развивающихся сетях GSM.

Партнерство 3GPP2 появилось в 1998 г. также по инициативе ETSI и Международного союза электросвязи (МСЭ) для разработки стандартов сетей 3G (сети CDMA-2000) в рамках проекта IMT-2000, созданного под эгидой МСЭ. Оно было образовано практически теми же организациями, что и в случае 3GPP. Основным вкладом организации 3GPP2 в развитие стандартов для мобильных сетей 3G явилось распространение концепции IMS на сети CDMA2000 (IP-транспорт, SIP-сигнализация), описанное в спецификации под общим названием MultiMedia Domain (MMD).

Оба партнерства разрабатывают стандарты сетей 3G, ориентируясь на широкое применение IP-ориентированных протоколов, стандартизованных Комитетом IETF, и используя основные идеи архитектуры ССП.

Впервые концепция IMS была представлена в документе 3GPP Release 5 (март 2002 г.). В нем была сформулирована основная ее цель – поддержка мультимедийных услуг в мобильных сетях на базе протокола IP – и специфицированы механизмы взаимодействия мобильных сетей 3G на базе архитектуры IMS с беспроводными сетями 2G.

Архитектура сетей 3G в соответствии с концепцией IMS имеет несколько уровней (плоскостей) с разделением по уровням транспорта, управления вызовами и приложений. Подсистема IMS должна быть полностью независима от технологий доступа и обеспечивать взаимодействие со всеми существующими сетями – мобильными и стационарными, телефонными, компьютерными и т. д.

В документе 3GPP Release 6 (декабрь 2003 г.) ряд положений концепции IMS был уточнен, добавлены вопросы взаимодействия с беспроводными локальными сетями и защиты информации (использование ключей, абонентских сертификатов).

В релизах 6 и 7 определена идеология осуществления IP-коммуникаций посредством SIP. В соответствии с ней SIP начинается непосредственно с мобильного терминала.

Спецификация Release 7 добавляет две основные функции, которые являются ключевыми в стационарных сетях:

- Network Attachment, которая обеспечивает механизм аутентификации абонентов и необходима в стационарных сетях, поскольку в них отсутствуют SIM-карты идентификации пользователя;
- Resource Admission, резервирующая сетевые ресурсы в стационарных сетях для обеспечения сеансов связи.

Работы, направленные на расширение концепции IMS на стационарные сети, проводятся Комитетом TISPAN. Интерес к архитектуре IMS со стороны ETSI привел к созданию новой рабочей группы (2003 г.), объединившей известную группу TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) и Технический комитет SPAN (Services and Protocols for Advanced Networks), который отвечает за стандартизацию стационарных сетей.

Новая группа, получившая название TISPAN (Telecommunications and

Internet converged Services and Protocols for Advanced Networking), отвечает за стандартизацию современных и перспективных конвергируемых сетей, включая VoIP и ССП, а также все, что связано с архитектурой IMS.

20.2. Архитектура IMS

Принцип, на котором строится концепция IMS, состоит в том, что доставка любой услуги никаким образом не соотносится с коммуникационной инфраструктурой (за исключением ограничений по пропускной способности). Воплощением этого принципа является многоуровневый подход, используемый при построении IMS. Он позволяет реализовать независимый от технологии доступа открытый механизм доставки услуг, который дает возможность задействовать в сети приложения сторонних поставщиков услуг.

В составе IMS выделяются три уровня: транспортный уровень, уровень управления и уровень услуг (рис. 8.1).

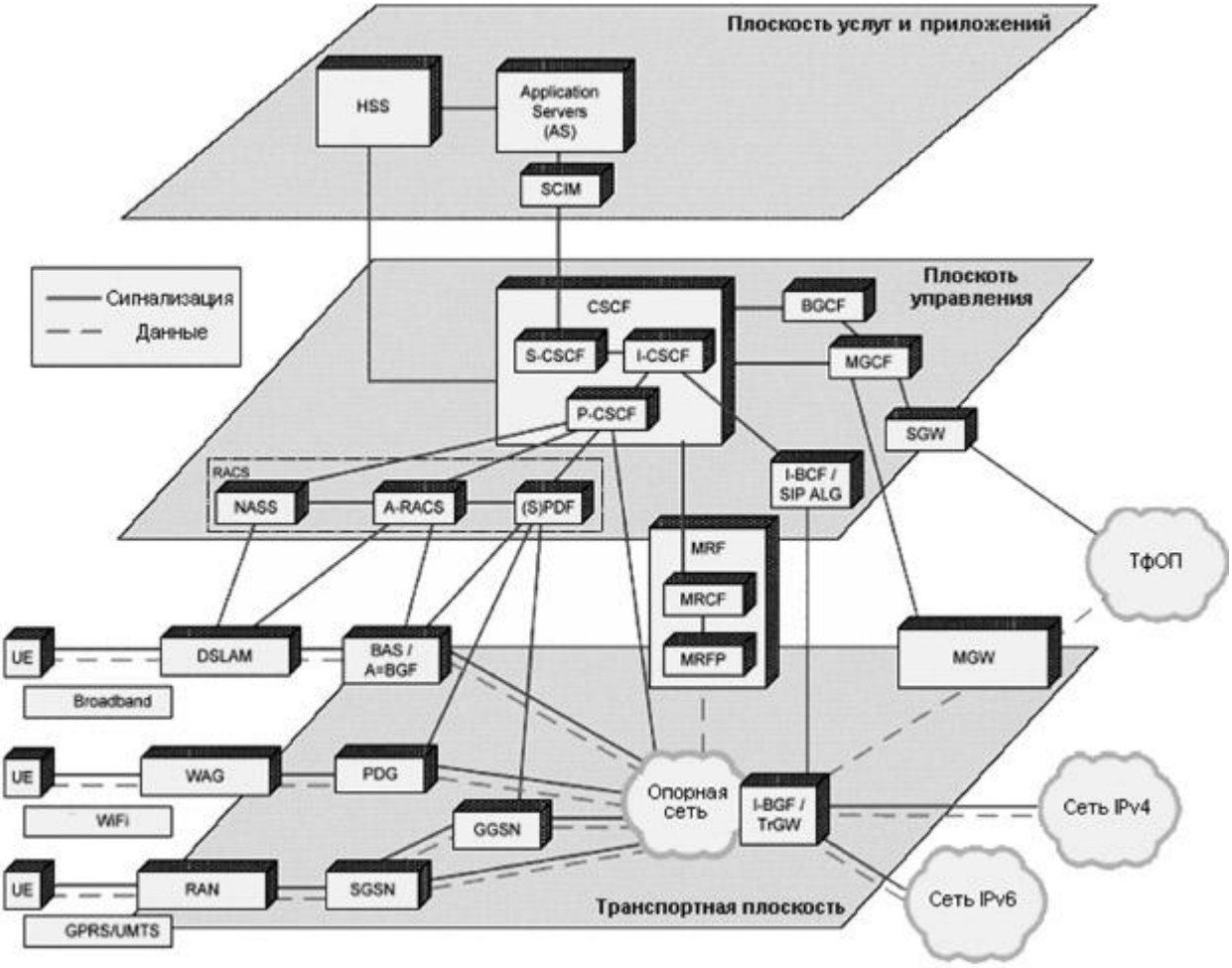


Рис. 8.1. Архитектура IMS

Транспортный уровень

Транспортный уровень отвечает за подключение абонентов к инфраструктуре IMS посредством пользовательского оборудования (User Equipment – UE). В роли данного оборудования могут выступать любой терминал IMS (например телефон (смартфон) 3G, КПК с поддержкой Wi-Fi, или же широкополосный доступ). Также возможно подключение через шлюзы не-IMS терминалов (например терминалы ТфОП).
Основное оборудование транспортной плоскости:

- MRF (Media Resource Function) – медиасервер. Состоит из процессора мультимедийных ресурсов MRFP (Media Resource Function Processor) и контроллера MRFC;
- MRFC обеспечивает реализацию таких услуг, как конференц-связь, оповещения или перекодирование передаваемого сигнала. Предполагалось, что MRFC должен обрабатывать SIP-сообщения, получаемые через узел S-CSCF (Serving Call Session Control Function), и использовать команды протокола управления медиашлюзом (MGCP, H.248 MEGACO) для управления процессором MRFP. Однако сейчас предпринимаются усилия по продвижению протокола на основе SIP/XML для взаимодействия между MRFC и MRFP. К тому же MRFC обеспечивает предоставление необходимой информации системам тарификации и биллинга;
- MRFP – процессор MRFP распределяет медиаресурсы сети согласно командам от MRFC. Его основными функциями являются:
- обслуживание потоков мультимедийных данных для служб оповещения и т. п.;
- объединение входящих мультимедиапотоков;
- обработка потоков мультимедийных данных, например транскодирование;
- MGW (Media GateWay) – транспортный шлюз; обеспечивает прямое и обратное преобразование потоков RTP в потоки сетей с коммутацией каналов (ТфОП);
- BGF (Interconnect Border Gateway Function) – межсетевой пограничный шлюз; обеспечивает взаимодействие между сетями IPv4 и IPv6. Отвечает за обспечение функций безопасности (трансляцию адресов и портов NAPT, функции firewall, инструменты QoS).
- GGSN (Gateway GPRS Support Node) – шлюзовой узел GPRS или узел маршрутизации; представляет собой шлюз между сотовой сетью (ее частью –GPRS) и IMS. GGSN содержит всю необходимую информацию о сетях, куда абоненты GPRS могут получать доступ, а также параметры соединения. Основной функцией GGSN является роутинг (маршрутизация) данных, идущих к абоненту и от него через SGSN;
- SGSN (Serving GPRS Support Node) – узел обслуживания абонентов

GPRS; основной компонент GPRS-системы по реализации всех функций обработки пакетной информации;
- RAN – Radio Access Network – оборудование радиодоступа; обеспечивает взаимодействие IMS и сотовых систем электросвязи;
- PDG (Packet Data Gateway) – пакетный шлюз. Данный сетевой элемент обеспечивает доступ пользовательского оборудования WLAN к IMS. Отвечает за трансляцию удаленного IP-адреса, регистрацию пользовательского оборудования в IMS, обеспечивает выполнение функций безопасности;
- WAG (Wireless Access Gateway) – шлюз беспроводного доступа; обеспечивает соединение сетей WLAN и IMS;
- BGF/BAS (Access Border Gateway Function / Broadband Access Switch) – обеспечивает доступ широкополосного пользовательского оборудования к IMS. Выполняет функции, аналогичные I-BGF;
- DSLAM (Digital Subscriber Line Access Multiplexer) – цифровой абонентский шлюз доступа – обеспечивает соединение абонентов, использующих широкополосный доступ (стационарный, например xDSL, сети КТВ) к IMS.

Плоскость управления

Уровень управления — это совокупность функций IMS, которые осуществляют все действия по управлению сеансами связи.
Основные элементы:
- CSCF(Call Session Control Function)– элемент с функциями управления вызовами и сеансами. Функция CSCF является основной на плоскости управления IMS-платформы. Модуль CSCF, используя протокол SIP, выполняет функции, обеспечивающие доставку множества услуг реального времени посредством транспорта IP. Функция CSCF использует динамическую информацию для эффективного управления сетевыми ресурсами (граничные устройства, шлюзы и серверы приложений) в зависимости от профиля пользователей и приложений. Модуль CSCF включает три основных функции:
  - Serving CSCF (S-CSCF) – обслуживающая CSCF. Обрабатывает все SIP-сообщения, которыми обмениваются оконечные устройства;
  - Proxy CSCF (P-CSCF) – через нее в систему IMS поступает весь пользовательский трафик;
  - Interrogating CSCF (I-CSCF) – запрашивающая CSCF. Представляет собой точку соединения с домашней сетью. I-CSCF обращается к HSS, чтобы найти S-CSCF для конкретного абонента;
- S-CSCF обеспечивает управление сеансами доставки мультимедийных сообщений транспорта IP, включая регистрацию терминалов,

двустороннее взаимодействие с сервером HSS (получение от него пользовательских данных), анализ сообщения, маршрутизацию, управление сетевыми ресурсами (шлюзами, серверами, пограничными устройствами) в зависимости от приложений и профиля пользователя;

- P-CSCF создает первую контактную точку на сигнальном уровне внутри ядра IMS для терминалов IMS данной сети. Функция P-CSCF принимает запрос от или к терминалу и маршрутизирует его к элементам ядра IMS. Обслуживаемый терминал пользователя закрепляется за функцией P-CSCF при регистрации в сети на все время регистрации. Модуль P-CSCF реализует функции, связанные с аутентификацией пользователя, формирует учетные записи и передает их в сервер начисления платы. Одним из элементов модуля P-CSCF является Policy Decision Function (PDF) – функция выбора политики, оперирующая с характеристиками информационного трафика (например, требуемая пропускная способность) и определяющая возможность организации сеанса или его запрета, необходимость изменения параметров сеанса и т. д.;
- CSCF создает первую контактную точку на сигнальном уровне внутри ядра IMS для всех внешних соединений с абонентами данной сети или визитными абонентами, временно находящимися в сети. Основная задача модуля I-CSCF – идентификация привилегий внешнего абонента по доступу к услугам, выбор соответствующего сервера приложений и обеспечение доступа к нему;
- BGCF (Breakout Gateway Control Function) – функция управления шлюзами, управляет пересылкой вызовов между доменом коммутации каналов (ТфОП или GSM) и сетью IMS. Данный модуль осуществляет маршрутизацию на основе телефонных номеров и выбирает шлюз в домене коммутации каналов (КК), через который сеть IMS (где расположен сервер BGCF) будет взаимодействовать с ТфОП или GSM. Здесь также производится генерация соответствующих учетных записей для начисления платы абонентам сетей КК;
- MGCF (Media GatewaysControl Function) – функция управления шлюзами (Media Gateways) – управляет соединениями в транспортных шлюзах IMS, используя H.248/MEGACO;
- SGW (Signaling Gateway) – сигнальный шлюз – обеспечивает преобразование сигнализации ТфОП в вид, понятный MGCF. Связан с ядром IMS через интерфейсы группы протоколов SIGTRAN;
- RACS (The Resource and Access Control) – подсистема управления ресурсами и доступом – обеспечивает функции управления доступом (на основании имеющихся в распоряжении ресурсов, местной политики и авторизации на основании профилей пользователей) и входа в сеть с помощью управления шлюзом (gate control), включая управление преобразованием сетевых адресов и портов, и присвоение приоритета;

- PDF (Policy Decision Function) – функция выбора политики, оперирующая с характеристиками информационного трафика (например требуемая пропускная способность) и определяющая возможность организации сеанса или его запрета, необходимость изменения параметров сеанса и т. д.;
- NASS (Network Attachment Subsystem) – подсистема подключения сети – в ее основные задачи входит динамическое назначение IP-адресов (используя DHCP – Dynamic Host Configuration Protocol), аутентификация на уровне IP, авторизация доступа к сети, управление местонахождением на уровне IP.

Уровень приложений

Верхний уровень эталонной архитектуры IMS содержит набор серверов приложений, которые, в принципе, не являются элементами IMS. Эти элементы верхней плоскости включают в свой состав как мультимедийные IP-приложения, базирующиеся на протоколе SIP, так и приложения, реализуемые в мобильных сетях на базе виртуальной домашней среды.

Архитектура приложений IMS достаточно сложна, но ключевым моментом здесь является высокая гибкость при создании новых и интеграции с традиционными приложениями. Например, среда пересылки сообщений может интегрировать традиционные свойства телефонного вызова, например обратный вызов и ожидание вызова, с вызовом Интернет. Чтобы сделать это, архитектура IMS позволяет запустить множество услуг и управлять транзакциями между ними.

- SCIM (Service Capability Interaction Manager) – обеспечивает управление взаимодействием плоскости приложений и ядра IMS;
- SIP AS (SIP Application Server) – сервер приложений, служащий для выполнения услуг, базирующихся на протоколе SIP. Ожидается, что все новые услуги в IMS будут находиться именно в сервере SIP AS;
- OSA-SCS (Open Service Access – Service Capability Server) – сервер возможных услуг, который обеспечивает интерфейс к услугам, базирующимся на открытом доступе услугам (OSA – Open Service Access). Целью является обеспечение услугам возможности доступа к сетевым функциям посредством стандартного программного интерфейса приложений;
- IM-SSF (IP Multimedia – Service Switching Function) – сервер коммутации услуги, служит для соединения подсистемы IMS с услугами в системе приспособленных к пользователю приложений для улучшения логики мобильной сети (CAMEL – Customized Applications for Mobile network Enhanced Logic). Речь идет об услугах, разработанных для глобальной системы мобильной связи GSM, а с помощью функции IM-SSF (функция коммутации услуг) использование данных услуг возможно и в IMS;

- TAS (Telephony Application Server) – сервер телефонных приложений принимает и обрабатывает сообщения протокола SIP, а также определяет, каким образом должен быть инициирован исходящий вызов. Сервисная логика TAS обеспечивает базовые сервисы обработки вызовов, включая анализ цифр, маршрутизацию, установление, ожидание и перенаправление вызовов, конференц-связь и т. д. TAS также обеспечивает сервисную логику для обращения к медиасерверам при необходимости воспроизведения оповещений и сигналов прохождения вызова. Если вызов инициирован или терминирован в ТфОП, сервер TAS отвечает за сигнализацию SIP к функции MGCF для выдачи команды медиашлюзам на преобразование битов речевого потока TDM (ТфОП) в поток IP RTP и направление его на IP-адрес соответствующего IP-телефона. В одном сообщении IMS могут содержаться данные о нескольких TAS, предоставляющих определенные услуги различным типам абонентских устройств. Например, один сервер TAS оказывает услуги IP Centrex (частные планы нумерации, общие справочники, автоматическое распределение вызовов и т. д.), другой сервер поддерживает УАТС и предоставляет услуги VPN. Взаимодействие нескольких серверов приложений осуществляется посредством сигнализации SIP-I для завершения вызовов между абонентскими устройствами различных классов;
- HSS (Home Subscriber Server) – сервер домашних абонентов – аналогичен элементу сетей GSM – серверу HLR (Home Location Register) – является базой пользовательских данных. Сервер HSS обеспечивает открытый доступ в режиме чтения/записи к индивидуальным данным пользователя, связанным с услугами. Доступ осуществляется из различных точек окончания – таких как телефон, приложения Web и SMS, телевизионные приставки типа set-top box и т. д. В HSS реализуется также функции SLF (Subscription Locator Function), которая определяет положение базы данных, содержащей данные конкретного абонента, в ответ на запрос от модуля I-CSCF или от сервера приложений.

Наконец, в состав сервера HSS входят модули HLR и AuC (Authentication Center) для работы с сетями 2G.

В среде IMS сервер HSS действует как открытая база данных о каждом пользователе и об услугах, задействованных абонентом: на какие услуги подписан пользователь, активизированы ли эти услуги, какие параметры управления были установлены пользователем.

8.3. Сравнение Softswitch и IMS

Архитектуры Softswitch и IMS имеют уровневое деление, причем границы уровней проходят на одних и тех же местах. Для архитектуры

Softswitch изображены в первую очередь устройства сети, а архитектура IMS определена на уровне функций. Идентичны также идея предоставления всех услуг на базе IP-сети и разделение функций управления вызовом и коммутации. По сути, к уже известным функциям Softswitch добавляются функции шлюза OSA и сервер абонентских данных.

Оценив списки функций в обеих архитектурах, можно заметить, что состав функций практически не отличается. Можно было бы заключить, что обе архитектуры почти тождественны. Это верно, но только отчасти: они идентичны в архитектурном смысле. Если же разобрать содержание каждой из функций, то обнаружатся значительные различия в системах Softswitch и IMS. Например, функция CSCF: из ее описания уже видно отличие от аналогичных функций в Softswitch. К тому же если в архитектуре Softswitch функции имеют довольно условное деление и описание, то в документах IMS дается жесткое описание функций и процедур их взаимодействия, а также определены и стандартизированы интерфейсы между функциями системы.

Различие начинается с основной концепции систем.

Softswitch – это в первую очередь оборудование конвергентных сетей. Функция управления шлюзами (и соответственно протоколы MGCP/MEGACO) является в нем доминирующей (протокол SIP для взаимодействия двух Softswitch/ MGC).

IMS проектировалась в рамках сети 3G, полностью базирующейся на IP. Основным ее протоколом является SIP, позволяющий устанавливать одноранговые сессии между абонентами и использовать IMS лишь как систему, предоставляющую сервисные функции по безопасности, авторизации, доступу к услугам и т.д. Функция управления шлюзами и сам медиашлюз здесь лишь средство для связи абонентов 3G с абонентами фиксированных сетей. Причем имеются в виду лишь ТФОП.

Также к особенностям IMS относится ориентированность на протокол IPv6: многие специалисты считают, что популярность IMS послужит толчком к затянувшемуся внедрению шестой версии протокола IP. Но пока это представляет некоторую проблему: сети UMTS поддерживают и IPv4 и IPv6, в то время как IMS – как правило, только IPv6. Поэтому на входе в IMS-сеть необходимо наличие шлюзов, преобразующих формат заголовков и адресную информацию. Эта проблема присуща не только IMS, но и всем сетям IPv6.

Продолжая тему проблем IMS, следует сказать о протоколе SIP. Дело в том, что SIP разработан и специфицирован комитетом IETF, но для использования в IMS он был частично доработан и изменен. В результате может возникнуть ситуация, когда при получении запросов SIP или отправке их во внешние сети подфункция S-CSCF может обнаружить отсутствие поддержки соответствующих расширений протокола SIP и/или отказать в установлении соединения, а также обработать его некорректно.

Одной из сильных сторон подхода IPCC в настоящее время является его распространенность: в мире существует множество сетей, пошедших по

этому пути развития, и уже накоплен обширный опытный материал по внедрению SoftSwitch-архитектур. Большое количество поддерживаемых технологий дает возможность оператору подобрать оборудование, наиболее отвечающее его требованиям и позволяющее оптимальным образом взаимодействовать с уже имеющимися сетевыми ресурсами. SoftSwitch-решения относительно легко масштабировать, начиная с простейшей архитектуры, обслуживающей корпоративный сектор, и заканчивая крупномасштабными проектами межрегионального оператора. Таким образом, оператор может минимизировать первоначальные вложения в сеть ССП. Эта же особенность позволяет оператору, создающему крупномасштабный проект, использовать новые сетевые ресурсы (и, следовательно, получать прибыль) сразу после их установки. Если обобщать перечисленные преимущества, то их можно охарактеризовать одним словом – "гибкость", подразумевая под ним адаптацию к любым запросам оператора.

Однако у решения IPCC есть и другая сторона. Многообразие оборудования, представленного в данном сегменте рынка, порождает проблему его совместимости. Многочисленные центры по обеспечению системного взаимодействия помогают решить ее лишь отчасти, так как зачастую тесты не успевают за обновлением версий программного обеспечения и не могут охватить все возможные комбинации устройств, работающих в сетях операторов. Это также порождает более широкую проблему взаимодействия операторов друг с другом и сводит на нет предусмотренные многими технологиями возможности по обеспечению мобильности пользователя и услуг. Некоторые производители оборудования предоставляют фирменные системы управления сетью, которые не всегда корректно и полноценно работают с оборудованием сторонних поставщиков при его интеграции в сеть оператора, поскольку имеются отличия не только в реализации, но и в функциональности многих систем.

В IMS частично сглаживаются проблемы совместимости оборудования, поскольку взаимодействие функциональных модулей регулируется стандартами. Новый подход к предоставлению услуг оказался чрезвычайно удачным и обеспечил роуминг услуг, что должно принести дополнительную прибыль оператору. Использование в проводных сетях ССП и мобильных сетях 3G единообразной системы IMS позволяет видеть в перспективе возможность конвергенции фиксированных и мобильных сетей — идеи, набирающей популярность по всему миру, подтверждением чему является постоянное увеличение участников FMCA (Fixed-Mobile Convergence Alliance) – международного объединения крупнейших операторов связи.

Контрольные вопросы

1. Как расшифровывается IMS?
2. Что описывает концепция IMS?
3. Укажите основные свойства архитектуры IMS

4. Назначение и состав уровня приложений
5. Назначение и состав транспортного уровня
6. Назначение и состав плоскости управления

ЛИТЕРАТУРА

1. Гулевич Д. С. Сети связи следующего поколения. БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий - ИНТУИТ.ру, 2007.
2. Росляков А.В. Сети следующего поколения NGN. - Эко-Трендз, 2008. - 424с.
3. Кучерявый А.Е., Гильченок Л.З., Иванов А.Ю. Пакетная сеть связи общего пользования. СПб:. Наука и техника, 2004.
4. Семенов А.В. Сети нового поколения. СПб: Наука и техника, 2005.
5. Материалы курса «Сети связи следующего поколения» сайта Интернет-Университета Информационных Технологий http://www.INTUIT.ru
6. А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева. IP-телефония. ИТЦ Эко-Трендз. 2002.
7. Б.С. Гольштейн, А.В. Пинчук, А.Л. Суховицкий. IP-телефония. Москва. Радио и связь. 2003.
8. Гольдштейн Б.С., Гольдштейн А.Б. SoftSwitch. СПб.: БХВ - Санкт-Петербург, 2006.
9. Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы MPLS. СПб.: БХВ - Санкт-Петербург, 2005.
10. Крук Б.И. Папантанопуло В.Н. Шувалов В.П Телекоммуникационные сети и системы: Современные технологии. М.: Горячая линия - Телеком, 2003.
11. Современные телекоммуникации. Технологии и экономика. Под ред. Довгого С.А. –М.: Эко-Трендз, 2003.
12. Садчикова С.А. IP-телефония. Учебное пособие для студентов специальностей 5А522202, 5А522203, 5А522205, 5А522216. Ташкент. ТУИТ.2008
13. С. Илич. FTTC: решение для широкополосных сетей доступа с оптимальной стоимостью. Вестник связи, №10, 2010
14. Доступ следующего поколения – Комбинирование широкополосного доступа FTTC и FTTB. Описание технического решения Iskratel FTTx
15. Мультисервисные сети Ethernet масштаба города (Metro Ethernet) http://www.polytron-tv.ru/design/metroethernet.html
16. .Мультиплексор цифровых соединительных линий DSLAM MA5100 компании HUAWEI. Huawei Technologies Co., Ltd, 2004.
17. http://nag.ru/articles/reviews/15443/metro-ethernet-arhitektura-i-tehnologii.html
18. http://nag.ru/articles/reviews /bras-ologiya.html
19. http://www.trcs.ru/catalog/huawei/seti-fiksirovannoj-svjazi/oborudovanie-bras

ТЕХНОЛОГИИ СЕТЕЙ СВЯЗИ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

Методическое пособие

для студентов специальностей

5522200 – телекоммуникация

Рассмотрено и одобрено на заседании каф. ТИ. Протокол заседания кафедры ТИ №_____ от _____г.

Рекомендовано к тиражированию НМС в типографии ТУИТ. Протокол заседания НМС №_____ от _____г.

Авторы издания: Эшмурадов А.М.

Садчикова С.А.

Норматова Д.Т.

Рецензенты: Парсиев С.С.

Ответственный редактор Гультураев Н.Х.

Корректор Абдуллаева С.Х.