УЗБЕКСКОЕ АГЕНТСТВО СВЯЗИ И ИНФОРМАТИЗАЦИИ

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра Устройства
и системы радиосвязи

КОНСПЕКТ ЛЕКЦИЙ ПО КУРСУ

ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ МОБИЛЬНЫХ СИСТЕМ СВЯЗИ

Составитель: Д.Давронбеков

Ташкент 2011

СОДЕРЖАНИЕ

Лекция 1. Определение ССП, основные характеристики, услуги ССП……... 3

Лекция 2. Архитектура ССП……. 12

Лекция 3. Основные протоколы, используемые в сетях следующего поколения…… 19

Лекция 4. Оборудование ССП ……... 36

Лекция 5. Программный коммутатор Softswitch…… 43

Лекция 6. Реализация Softswitch…… 51

Лекция 7. Качество обслуживания…… 58

Лекция 8. Методы обеспечения качества обслуживания: DiffServ и IntServ…… 67

Лекция 9. Технология MPLS…….. 79

Лекция 10. Метки и механизмы MPLS……. 88

Лекция 11. Протоколы распределения меток……. 100

Лекция 12. Протоколы маршрутизации……... 107

Лекция 13. Инжиниринг трафика. Виртуальные частные сети…….. 117

Лекция 14. IMS (IP Multimedia Subsystem)……... 129

Лекция 15. Техническое описание телекоммуникационного оборудования и комплектующих частей сети сотовой связи стандарта GSM M900/M1800……... 139

Лекция 1. Определение ССП, основные характеристики, услуги ССП

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 наши желания, 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).

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.

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 - Взаимодействия Открытых Систем (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.

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.

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.

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*.

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.

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.

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).

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.

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.

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.

Лекция 2. Архитектура ССП

С развитием инфокоммуникационных услуг стали весьма популярны обсуждения различных вариантов архитектуры *ССП*, которые в рамках единой инфраструктуры объединяют сети ТфОП, мобильную связь, ресурсы сети Интернет, телефонию по IP-протоколу. В настоящее время наибольшее распространение получила четырехуровневая архитектура *ССП*:

Рис. 2.1. 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. 2.2).

Как показано на рисунке, разные сети связи имеют различные сетевые элементы, в частности:

- 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*.

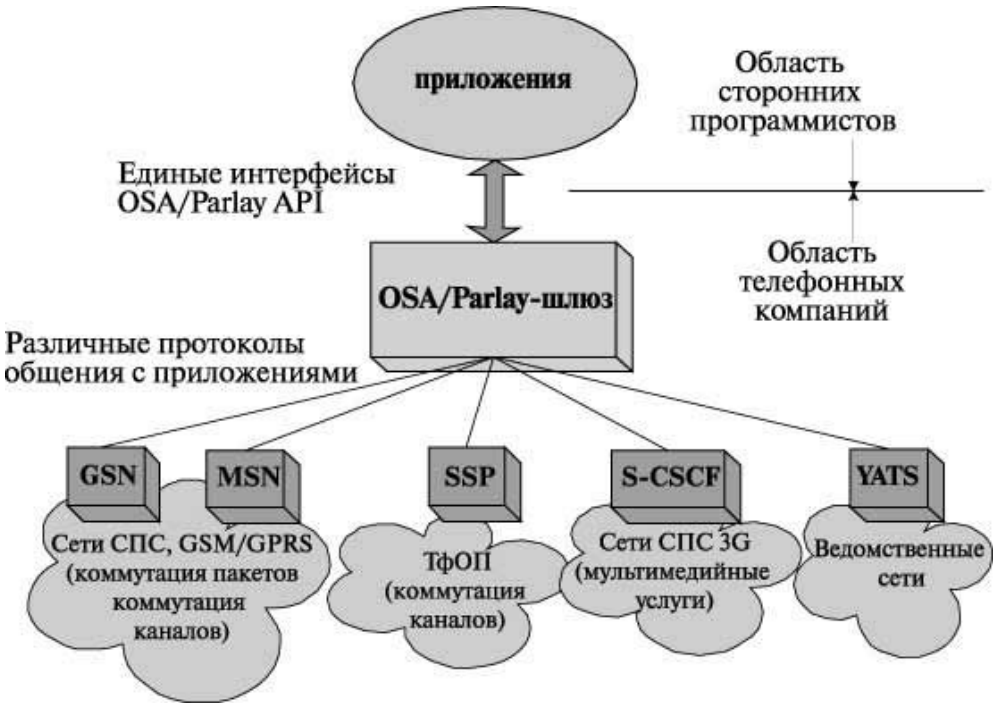


Рис. 2.2. Архитектура Parlay

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. 2.3, где показаны слева четыре набора функций сети:

Рис. 2.3. 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 *API*s).
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. 2.4):

- 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).

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.

В состав базовой сети *ССП* 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 электросвязи (ТфОП, СПД, СПС).

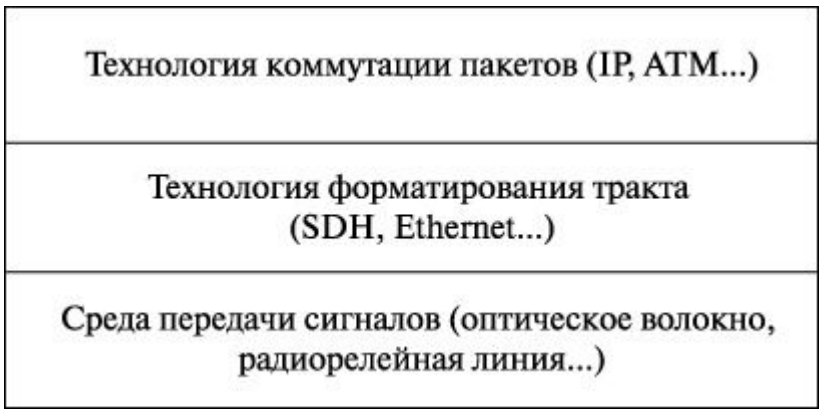


Рис. 2.4. Модель базовой сети

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 электросвязи, так как позволяет заменить дорогостоящие системы коммутации большой емкости небольшими, гибкими и доступными по стоимости даже мелким операторам электросвязи.

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)).

Можно отметить, что 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*.

Архитектура сети электросвязи, построенной в соответствии с концепцией *ССП*, представлена на рис. 2.5 (с некоторыми упрощениями).

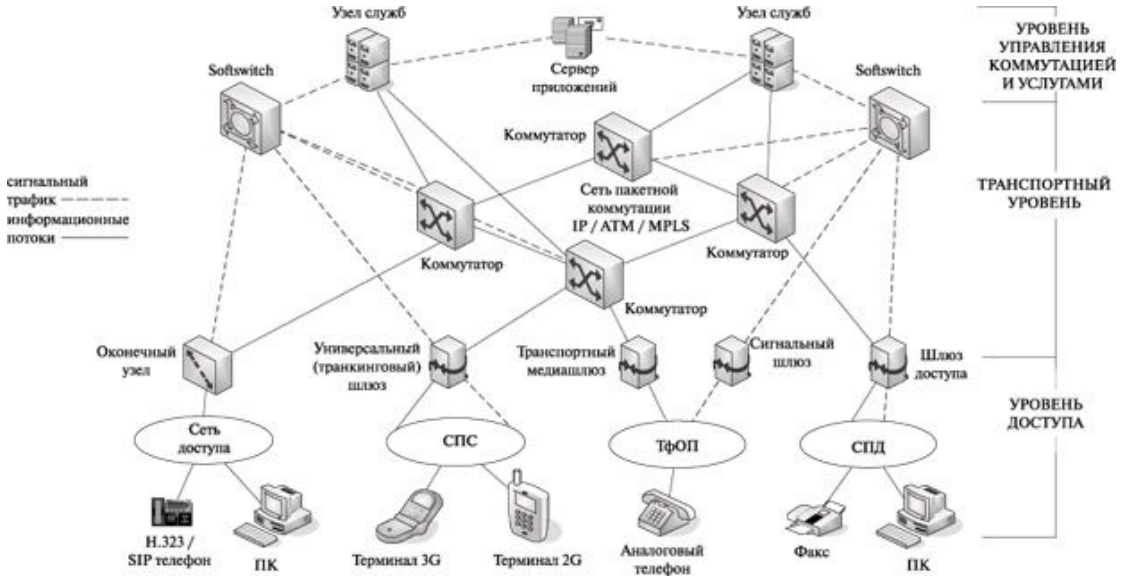


Рис. 2.5.

Инфокоммуникационные услуги предполагают взаимодействие поставщиков услуг и операторов связи, которое может обеспечиваться на основе функциональной модели распределенных (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 взаиморасчетов между операторами связи и поставщиками услуг;
- обеспечение взаимодействия между операторами связи в процессе предоставления услуг интеллектуальной связи;
- обеспечение взаимодействия терминалов с различными функциональными возможностями на разных концах соединения.

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

Концепция *ССП* 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.

В качестве технологической основы построения транспортного *уровня* сетей связи следующего поколения рассматривается технология IP/MPLS с возможным применением в будущем оптической коммутации.

Лекция 3. Основные протоколы, используемые 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.

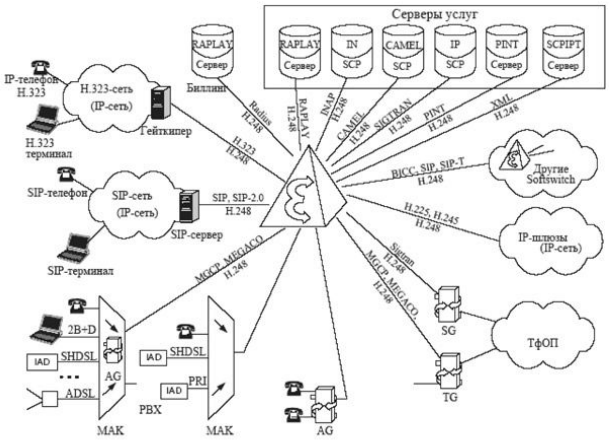
Основными протоколами сигнализации для *управления соединениями* сегодня являются *SIP*, ОКС-7, *H.323*. Также опционально используются:

- 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 — SIPT и BICC (рис. 3.1).

Протоколы RTP, RTCP, UDP

Основным транспортным протоколом для мультимедийных приложений стал *протокол реального* времени RTP (Real Time Protocol), предназначенный для организации передачи пакетов с кодированными речевыми сигналами по пакетной сети. Передача пакетов RTP ведется поверх протокола UDP, работающего, в свою очередь, поверх IP (рис. 3.2).



GK — Gate Keeper (Гейткипер)
SG — Signalling Gateway (Сигнальный шлюз)
TG — Trunking Gateway (Шлюз соединительных линий)
AG — Access Gateway (шлюз доступа)
MAK — Мультисервисные абонентские концентраторы

Рис. 3.1. Взаимодействие Softswitch с остальным оборудованием

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.

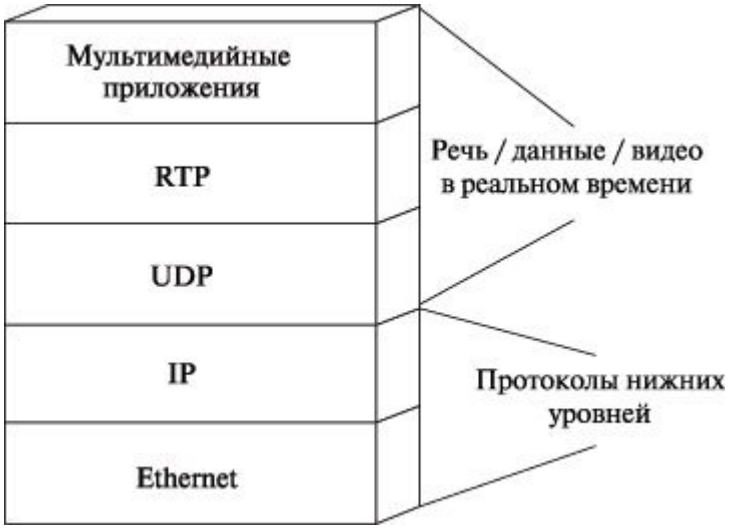


Рис. 3.2. Уровни протоколов RTP/UDP/IP

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 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.

Протокол H.323

Для построения сетей **IP**-телефонии первой стала рекомендация *H.323* МСЭ-Т, которая является также первой зонтичной спецификацией систем мультимедийной связи для работы в сетях с коммутацией пакетов, не обеспечивающих гарантированное качество обслуживания (рис. 3.3).

Сети, построенные на базе протоколов *H.323*, ориентированы на интеграцию с телефонными сетями и могут рассматриваться как сети ЦСИС (цифровая сеть с интеграцией служб), наложенные на сети передачи данных. В частности, процедура установления соединения в таких сетях IP-телефонии базируется на рекомендации МСЭ-Т Q.931 и практически идентична той же процедуре в сетях ЦСИС. При этом рекомендация *H.323* предусматривает применение разнообразных алгоритмов сжатия речевой информации, что позволяет использовать полосу пропускания ресурсов передачи гораздо более эффективно, чем в сетях с коммутацией каналов.

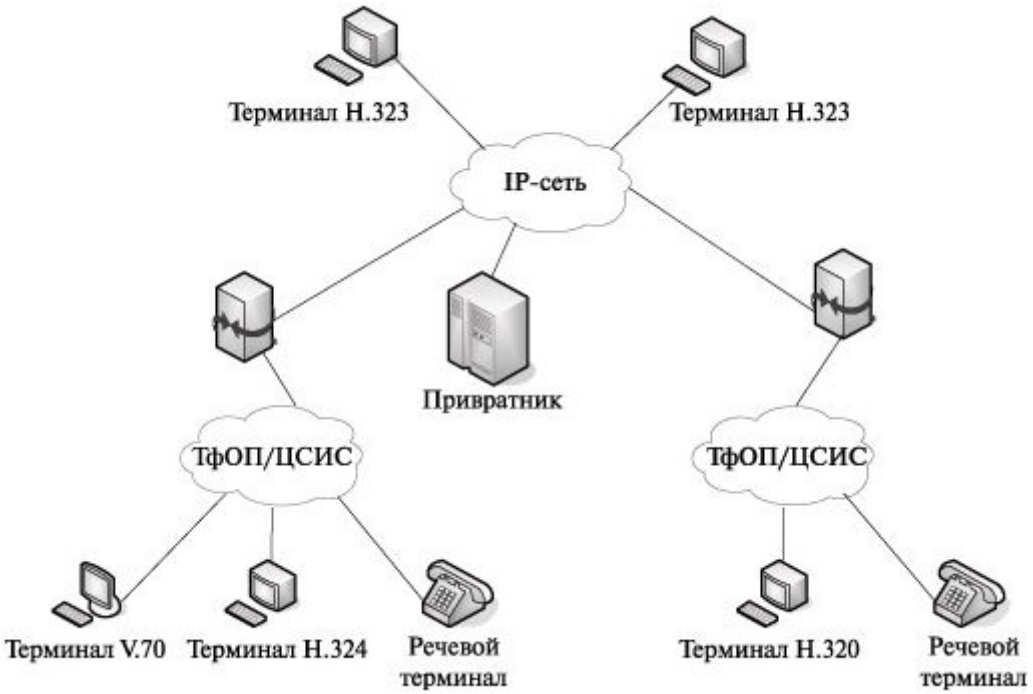


Рис. 3.3. Структура сети H.323

Основными устройствами сети являются: терминал, шлюз, привратник. В отличие от устройств ТфОП, устройства H.323 не имеют жестко закрепленного места в сети, а

подключаются к любой точке IP-сети. Однако при этом сеть H.323 разбивается на зоны, а каждой зоной управляет привратник.

- ***Терминал H.323*** – оконечное устройство сети IP-телефонии, обеспечивающее 2-стороннюю речевую или мультимедийную связь с другим терминалом, шлюзом или устройством управления конференциями.
- **Шлюз** является соединяющим мостом между ТфОП и IP. Основная функция шлюза — преобразование речевой (мультимедийной) информации, поступающей со стороны ТФОП с постоянной скоростью, в вид, пригодный для передачи по IP-сетям, т. е. кодирование информации, подавление пауз в разговоре, упаковка информации в пакеты RTP/UDP/IP, а также обратное преобразование. Кроме того, шлюз должен преобразовывать аналоговую абонентскую сигнализацию, сигнализацию по 2ВСК и сообщения систем сигнализации DSS1 и ОКС7 в сигнальные сообщения H.323. При отсутствии в сети привратника должна быть реализована еще одна функция шлюза: преобразование номера ТфОП в транспортный адрес IP-сети.
- **Привратник** выполняет функции управления зоной сети IP-телефонии, в которую входят терминалы и шлюзы, зарегистрированные у данного привратника. Разные участки зоны сети *H.323* могут быть территориально разнесены, но соединяться друг с другом через маршрутизаторы (рис. 3.4).

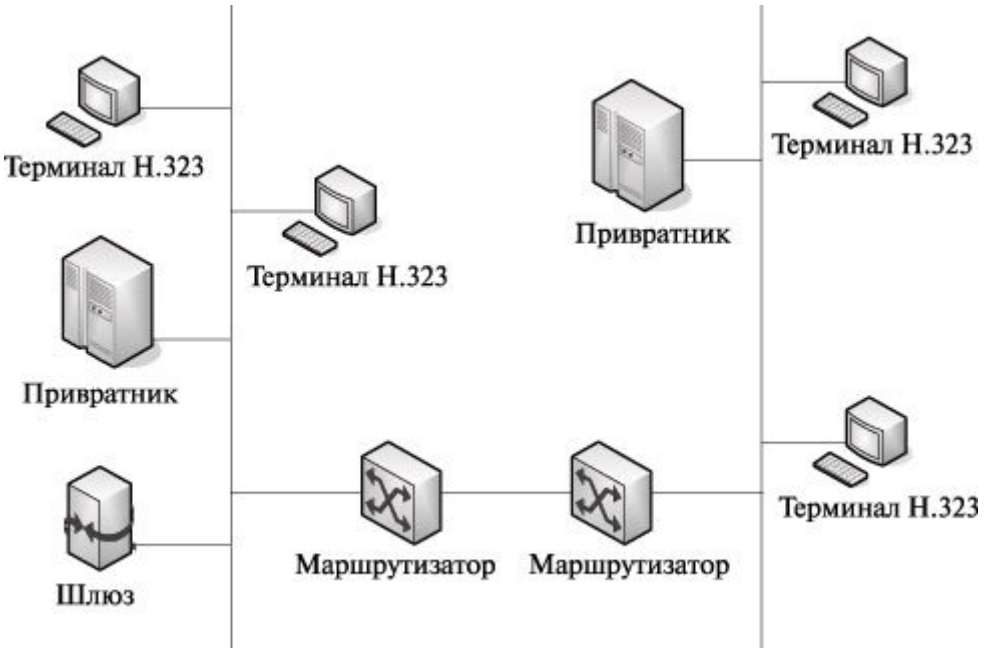


Рис. 3.4. Зоновая архитектура сети H.323

В число наиболее важных функций, выполняемых привратником, входят:

1. преобразование alias-адреса (имени абонента, телефонного номера, адреса электронной почты и др.) в транспортный адрес сетей с маршрутизацией пакетов IP (IP-адрес и номер порта RTP);
2. контроль доступа пользователей системы к услугам IP-телефонии при помощи сигнализации RAS (Registration, Admission and Status);
3. контроль, управление и резервирование пропускной способности сети;
4. маршрутизация сигнальных сообщений между терминалами, расположенными в одной зоне.

Привратник также обеспечивает для пользователя возможность получить доступ к услугам любого терминала в любом месте сети и способность сети идентифицировать пользователей при их перемещении из одного места в другое.

Протокол SIP

Вторым вариантом построения сетей стал протокол *SIP*, разработанный комитетом IETF (Internet Engineering Task Force); 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. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится;
- масштабируемость сети (характеризуется в первую очередь возможностью увеличения количества элементов сети при ее расширении);
- расширяемость протокола характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.

Протокол *SIP* может быть использован совместно с протоколом *H.323*. Возможно также взаимодействие протокола *SIP* с системами сигнализации ТфОП – DSS1 и ОКС7.

Одной из важнейших особенностей протокола *SIP* является его независимость от транспортных технологий. В качестве транспорта могут применяться 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. Пример построения сети *SIP* представлен на рис. 3.5.

Сеть *SIP* содержит следующие основные элементы.

- *Агент пользователя (User Agent или SIP client)* является приложением терминального оборудования и включает в себя две составляющие: клиент агента пользователя (User Agent Client – UAC) и сервер агента пользователя (User Agent Server – UAS), иначе называемые клиент и сервер. Клиент UAC инициирует *SIP*-запросы, т.е. выступает в качестве вызывающей стороны. Сервер UAS принимает запросы и отвечает на них, т.е. выступает в качестве вызываемой стороны.

Запросы могут передаваться не прямо адресату, а на некоторый промежуточный узел (прокси-сервер и сервер переадресации).

- **Прокси-сервер (proxy server)** принимает запросы, обрабатывает их и отправляет дальше на следующий сервер, который может быть как другим прокси-сервером, так и последним UAS. Таким образом, прокси-сервер принимает и отправляет запросы и клиента, и сервера. Приняв запрос от UAC, прокси-сервер действует от имени этого UAC;

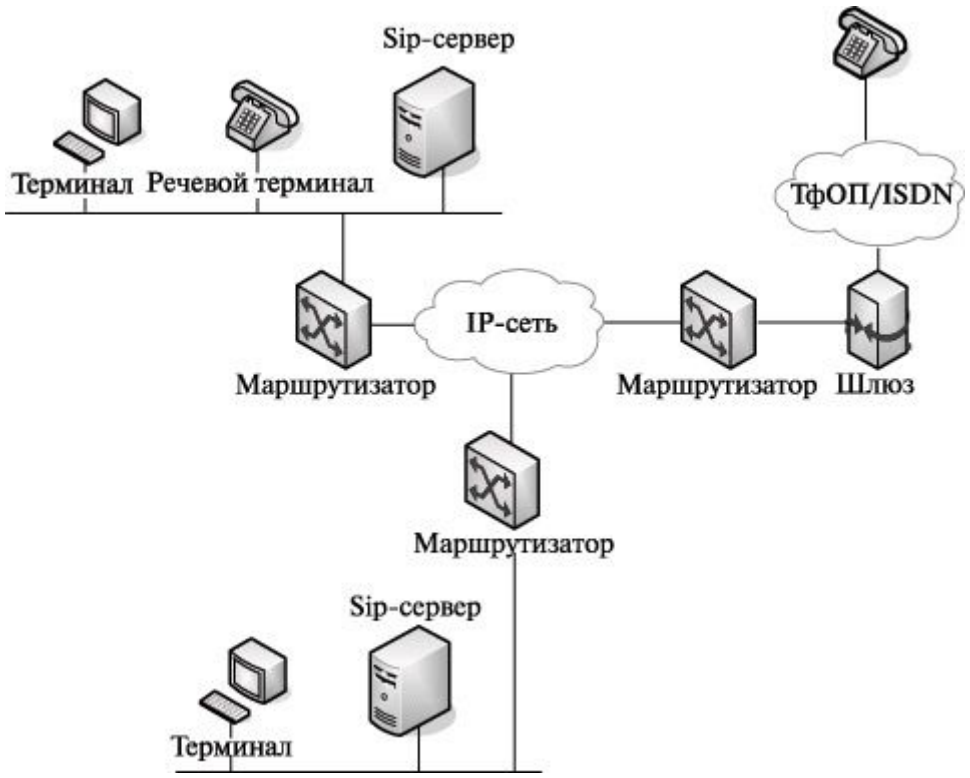


Рис. 3.5. Пример построения SIP-сети

- **Сервер переадресации (redirect server)** передает клиенту в ответе на запрос адрес следующего сервера или клиента, с которым первый клиент связывается затем непосредственно. Он не может инициировать собственные запросы. Адрес сообщается первому клиенту в поле Contact сообщений *SIP*. Таким образом, этот сервер просто выполняет функции поиска текущего адреса пользователя.
- **Сервер местоположения (location server)** – база адресов, доступ к которой имеют *SIP*-серверы, пользующиеся ее услугами для получения информации о возможном местоположении вызываемого пользователя. Приняв запрос, сервер *SIP* обращается к серверу местоположения, чтобы узнать адрес, по которому можно найти пользователя. В ответ тот сообщает либо список возможных адресов, либо информирует о невозможности найти их.

Протокол MGCP

Рабочая группа MEGACO комитета IETF разработала протокол управления шлюзами – ***Media Gateway Control Protocol (MGCP)***.

При разработке протокола управления шлюзами рабочая группа MEGACO опиралась на принцип декомпозиции, согласно которому шлюз разбивается на отдельные функциональные блоки (рис. 3.6):

- **транспортный шлюз** – Media Gateway, который выполняет функции преобразования речевой информации, поступающей со стороны ТфОП с постоянной скоростью, 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;

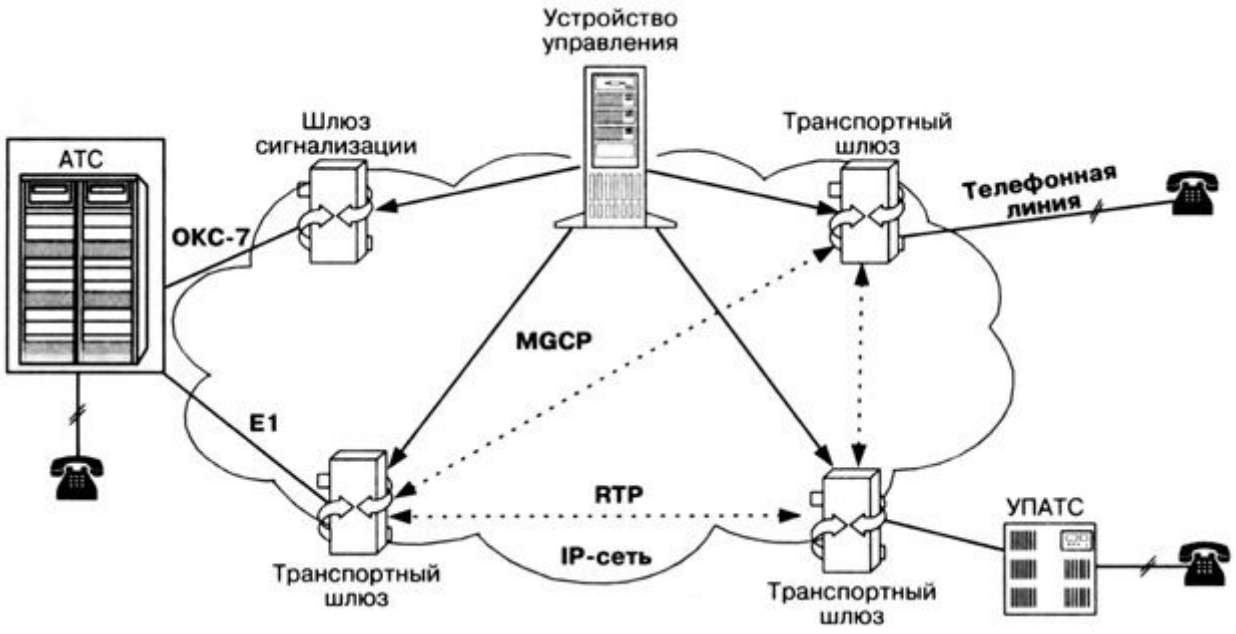


Рис. 3.6. Архитектура сети, базирующейся на протоколе MGCP

- **устройство управления** – Call Agent, выполняющее функции управления шлюзом;
- **шлюз сигнализации** – Signaling Gateway, который обеспечивает доставку сигнальной информации, поступающей со стороны ТфОП, к устройству управления шлюзом и перенос сигнальной информации в обратном направлении.

Таким образом, весь интеллект функционально распределенного шлюза размещается в устройстве управления, функции которого в свою очередь могут быть распределены между несколькими компьютерными платформами. Шлюз сигнализации выполняет функции STP – транзитного пункта системы сигнализации по общему каналу – ОКС7. Транспортные шлюзы выполняют только функции преобразования речевой информации. Одно устройство управления обслуживает одновременно несколько шлюзов. В сети может присутствовать несколько устройств управления. Предполагается, что эти устройства синхронизованы между собой и согласованно управляют шлюзами, участвующими в соединении. Рабочая группа MEGACO не определяет протокол синхронизации работы устройств управления, однако в ряде работ, посвященных исследованию возможностей протокола *MGCP*, для этой цели предлагается использовать протоколы *H.323*, *SIP* или ISUP/IP.

Перенос сообщений протокола *MGCP* обеспечивает протокол UDP.

Одно из основных требований, предъявляемых к протоколу *MGCP*, состоит в том, что устройства, реализующие этот протокол, должны работать в режиме без сохранения информации о последовательности транзакций между устройством управления и транспортным шлюзом, т.е. в устройствах не требуется реализации конечного автомата для описания этой последовательности.

Протокол *MGCP* является внутренним протоколом, поддерживающим обмен информацией между функциональными блоками распределенного шлюза. Протокол *MGCP* использует принцип master/slave (ведущий/ведомый), причем устройство

управления шлюзами является ведущим, а транспортный шлюз – ведомым устройством, которое выполняет команды, поступающие от устройства управления.

Такое решение обеспечивает масштабируемость сети и простоту эксплуатационного управления ею через устройство управления шлюзами. К тому же неинтеллектуальные шлюзы требуют меньшей производительности процессоров и, как следствие, оказываются менее дорогими. Кроме того, обеспечивается возможность быстро добавлять новые протоколы сигнализации и новые дополнительные услуги, так как нужные для этого изменения затрагивают только устройство управления шлюзами, а не сами шлюзы.

Рабочей группой MEGACO предложена следующая классификация транспортных шлюзов (Media Gateways):

- **Trunking Gateway** – шлюз между ТфОП и сетью с маршрутизацией пакетов IP, ориентированный на подключение к телефонной сети посредством большого количества цифровых трактов (от 10 до нескольких тысяч) с использованием системы сигнализации ОКС 7;
- **Voice over ATM Gateway** – шлюз между ТфОП и АТМ-сетью, который также подключается к телефонной сети посредством большого количества цифровых трактов (от 10 до нескольких тысяч);
- **Residential Gateway** – шлюз, подключающий к IP-сети аналоговые, кабельные модемы, линии xDSL и широкополосные устройства беспроводного доступа;
- **Access Gateway** – шлюз для подключения к сети IP-телефонии небольшой учрежденческой АТС через аналоговый или цифровой интерфейс;
- **Business Gateway** – шлюз с цифровым интерфейсом для подключения к сети с маршрутизацией IP-пакетов учрежденческой АТС при использовании, например, системы сигнализации DSS1;
- **Network Access Server** – сервер доступа к IP-сети для передачи данных;
- **Circuit switch или packet switch** – коммутационные устройства с интерфейсом для управления от внешнего устройства.

Протокол MEGACO/H.248

Рабочая группа MEGACO комитета IETF, продолжая исследования, направленные на усовершенствование протокола управления шлюзами, создала более функциональный (по сравнению с рассмотренным в предыдущей главе протоколом *MGCP*) протокол MEGACO. Но разработкой протоколов управления транспортными шлюзами, кроме комитета IETF, занималась еще и исследовательская группа SG 16 Международного союза электросвязи. Спецификации адаптированного протокола приведены в рекомендации ITU-T H.248.

Рассмотрим кратко основные особенности протокола *MEGACO/ H.248*. Для переноса сигнальных сообщений *MEGACO/ H.248* могут использоваться протоколы UDP, TCP, SCTP или транспортная технология ATM. Поддержка для этих целей протокола UDP – одно из обязательных требований к контроллеру шлюзов. Протокол TCP должен поддерживаться и контроллером, и транспортным шлюзом, а поддержка протокола SCTP, так же как и технологии ATM, является необязательной.

При описании алгоритма установления соединения с использованием протокола MEGACO комитет IETF опирается на специальную модель процесса обслуживания вызова, отличную от модели *MGCP*. Протокол MEGACO оперирует с двумя логическими объектами внутри транспортного шлюза: **порт (termination)** и **контекст (context)**, которыми может управлять контроллер шлюза (рис. 3.7).

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.

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.

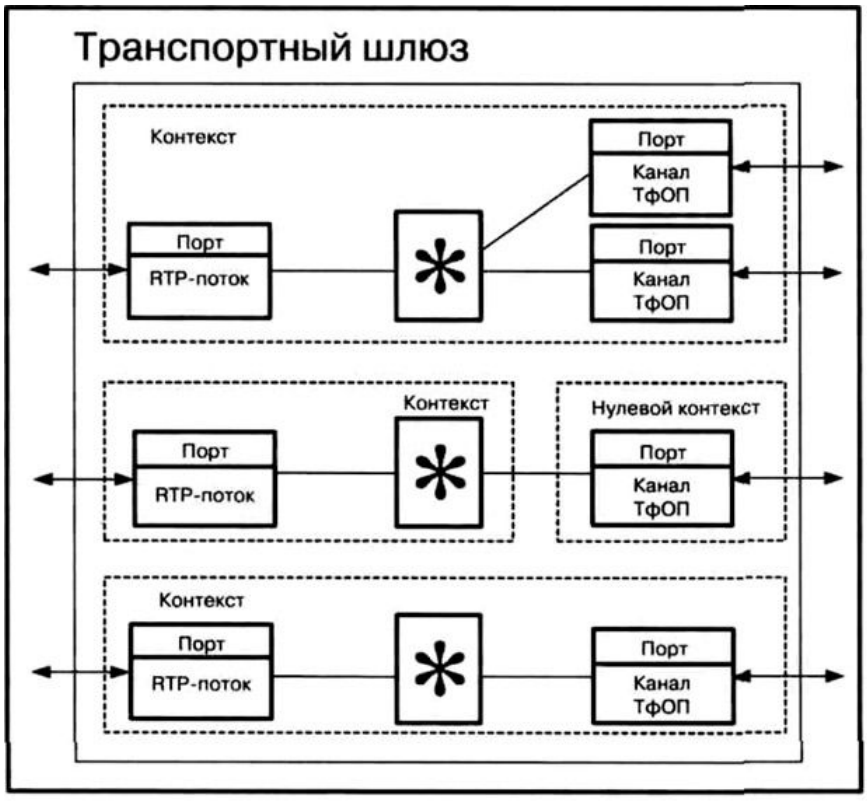


Рис. 3.7. Примеры модели процесса обслуживания вызова

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.

При помощи протокола MEGACO контроллер может изменять свойства портов шлюза. Свойства портов группируются в дескрипторы, которые включаются в команды управления портами.

Сведем основные характеристики протоколов IP-телефонии в одну таблицу (таблица 3.1).

Таблица 3.1. Основные протоколы IP-телефонии

Характеристики	***SIP***	***H.323***	***MGCP*** **MEGACO**	**ISUP**
Назначение	Для IP-коммуникаций	Для IP-телефонии	Для управления транспортными шлюзами	Для сетей с ВРК
Архитектура	Peer-to-Peer	Peer-to-Peer	Master-Slave	Peer-to-Peer
Интеллект	Рассредоточен по элементам сети	В ядре сети	В ядре сети	В ядре сети
Сложность	Простой	Сложный	Простой	Сложный
Масштабируемость	Высокая	Средняя	-	Средняя
Тип данных	Речь, данные, видео	Речь, данные, видео	Управление передачей речи, данных	Речь и данные
QoS	Поддерживается	Поддержка диффиринцированного обслуживания	Контроль QoS на уровне IP	Не требуется
Адресация	Поддержка IP-адресов и имен доменов, через DNS	Поддержка IP-адресов, мультизонная, многодоменовая поддержка через привратник	Цифровая адресация терминалов пользователей, поддержка IP-адресов и имен доменов для транспортных шлюзов	Статические

Сравнение протоколов (с позиции применения в ССП)

MEGACO/H.248 и MGCP

Прежде всего, MEGACO имеет более общую модель обслуживания вызовов, что позволяет ему лучше работать с такими соединениями как TDM-TDM, TDM-ATM, и TDM-IP, а также более гибко управлять конференциями. Еще одно различие касается транзакций. MEGACO в транзакциях содержит команды раздельно друг от друга, в то время как MGCP позволяет использовать вложенные команды, что усложняет процесс поиска команды. MEGACO может применять в целях обеспечения безопасности заголовки аутентификации, которых нет у *MGCP*. Что касается мультимедиа, MEGACO

позволяет микшировать аудио/видеоданные и таким образом поддерживает мультимедийный трафик, а *MGCP* ориентирован только на поддержку аудиоинформации. Если шлюз обнаруживает аварию на управляющем им Softswitch при помощи команд, протокол MEGACO позволяет назначить новый управляющий Softswitch. В *MGCP* это делается гораздо более сложным способом.

MEGACO/H.248 и SIP

MEGACO/ H.248 и *SIP* не соперничают друг с другом, т.к. MEGACO – это протокол, предназначенный для взаимодействия Softswitch и медиашлюзов, а *SIP* – это протокол взаимодействия одноранговых устройств (Softswitch или *SIP*-телефон). Взаимодействие транспортных шлюзов ограничено областью одного домена, т.к. они контролируются одним Softswitch. Таким образом, можно сказать, что MEGACO не определяет систему связи в целом, ему нужен протокол для взаимодействия Softswitch, которым может быть *SIP*.

MEGACO/H.248 и H.323

Как и *SIP*, протокол *H.323* может дополнять *MEGACO/ H.248*, поскольку тоже является протоколом, обеспечивающим взаимодействие одноранговых устройств. В таком случае *MEGACO/H.248* позволит H.323 избавиться от присущих ему проблем с масштабируемостью, доступностью и возможностью взаимодействовать с ОКС7. В этих условиях H.323 будет протоколом терминалов для взаимодействия друг с другом и с сетью, а MEGACO будет использоваться привратниками для управления большими шлюзами, обеспечивающими взаимодействие IP-сети, построенной согласно H.323 с сетью ТфОП.

Протокол BICC

Для взаимодействия Softswitch между собой теоретически должен применяться протокол BICC (Bearer Independent Call Control), разработанный МСЭ. И хотя на практике более популярным становится второй протокол – *SIP* (SIP-T), разработанный IETF, протокол BICC успешно используется до сих пор, например в решениях Ericsson.

При разработке данного протокола обязательным требованием являлась поддержка сигнальных сообщений ISUP, поскольку протокол должен был облегчить операторам переход к ССП и обеспечить взаимодействие новой мультисервисной сети с существующими сетями ISDN. Фактически протокол BICC рассматривался как еще одна прикладная подсистема сигнализации ОКС7, обеспечивающая экономичный переход к мультисервисной сети с сохранением большей части сигнального оборудования ISUP сетей с временным разделением каналов TDM. В свое время данный протокол позволил операторам, не желавшим вкладывать инвестиции в дальнейшее развитие TDM-сетей, предоставлять уже существующие услуги ТфОП/ISDN в пакетных сетях, а также поддерживать взаимодействие имеющихся узлов коммутации TDM узлами пакетной сети и взаимодействие узлов коммутации TDM через пакетную сеть.

Архитектура BICC предусматривает, что вызовы будут входить в сеть и выходить из нее с поддержкой BICC через интерфейсы узлов обслуживания – Interface Serving Nodes (ISN), – предоставляющие сигнальные интерфейсы между узкополосной ISUP (сетью ТфОП/ISDN с коммутацией каналов) и одноранговым узлом ISN (находящимся в пакетной сети). Также определены:

- транзитный узел обслуживания (Transit Serving Node (TSN)) – этот тип узла обеспечивает транзитные возможности в пределах одной сети. Служит для обеспечения возможности предоставления услуги ТфОП/ISDN внутри своей сети;
- пограничный узел обслуживания (Gateway Serving Node (GSN)) – этот тип узла обеспечивает выполнение функций межсетевого шлюза для информации вызова и транспортировки, используя BICC-протокол. Обеспечивает соединение двух областей BICC, принадлежащих двум разным операторам, и это соединение состоит из двух узлов GSN, непосредственно связанных друг с другом.

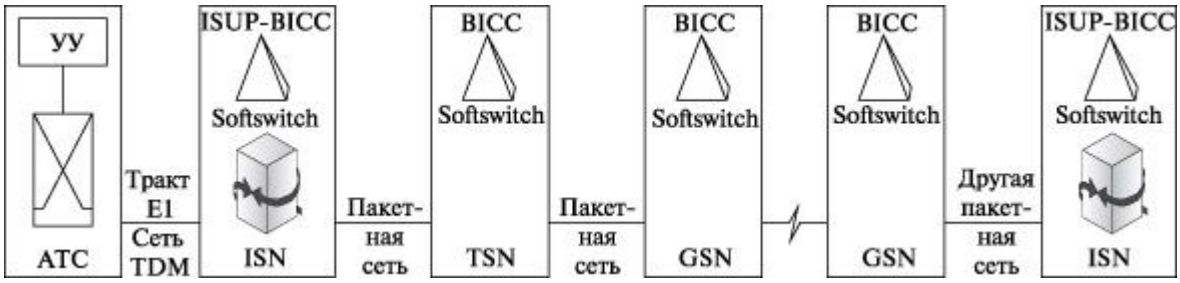


Рис. 3.8. Протокол BICC

На рис. 3.8 представлены узлы всех рассмотренных типов. Имеются также промежуточные коммутаторы, через которые тракт проключается при помощи сетевой сигнализации. Эти коммутаторы характерны для сетей ATM и в терминах BICC называются узлами ретрансляции носителя – Bearer Relay Nodes (BRN) или коммутирующими узлами – Switching Nodes (SWN), но не все сетевые технологии требуют их наличия.

Транспортировка информации сигнализации(SIGTRAN)

Транспортировка информации сигнализации по технологии *SIGTRAN* (рис. 3.9) предназначена для передачи сообщений протокола сигнализации сети с коммутацией каналов через сеть с коммутацией пакетов и должна обеспечивать:

1. передачу сообщений разнообразных протоколов сигнализации, обслуживающих соединения сетей с коммутацией каналов (CSN), например протоколов прикладных и пользовательских подсистем ОКС7 (включая уровень 3 MTP, ISUP, SCCP, TCAP, MAP, INAP и т. д.), а также сообщений уровня 3 протоколов DSS1/PSS1 (т. е. Q.931 и QSIG);
2. средства идентификации конкретного транспортируемого протокола сигнализации сети с коммутацией каналов;
3. общий базовый протокол, определяющий форматы заголовков, расширения в целях информационной безопасности и процедуры для транспортировки сигнальной информации, а также (при необходимости) расширения для введения конкретных индивидуальных протоколов сигнализации сети с коммутацией каналов;
4. функциональные возможности (с участием нижележащего сетевого протокола, например IP), соответствующие нижнему уровню конкретной сети с коммутацией каналов.

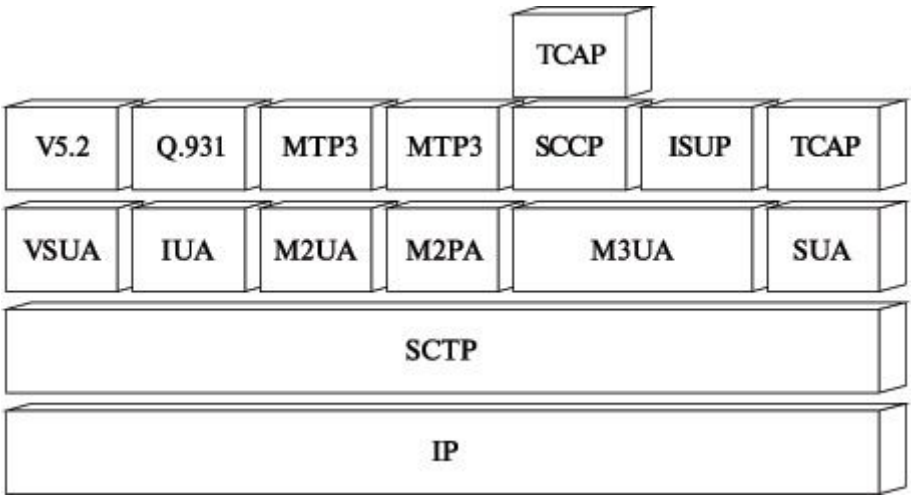


Рис. 3.9. Архитектура протоколов SIGTRAN

При транспортировке сигнальной информации через инфраструктуру сети Интернет используемым промежуточным средством считается протокол передачи информации управления потоком (Stream Control Transmission Protocol – SCTP).

Протокол передачи информации управления потоком (SCTP)

Протокол передачи информации управления потоком (SCTP) обеспечивает транспортировку сообщений сигнализации через сеть IP между двумя оконечными пунктами, с избыточностью доставки информации и повышенной степенью надежности. Для этого применяется стандартизованный метод, отличающийся встраиванием в протокол повышенной надежности доставки в реальном времени информации от нескольких источников по нескольким информационным потокам.

Также обеспечивается самоотключение в случае перегрузки соединения Интернет, по которому функционирует этот протокол. Интерфейс между SCTP и его сигнальными приложениями управляется через адаптационные уровни, которые образуют промежуточный уровень таким образом, чтобы сигнальные протоколы высших уровней конкретной архитектуры стека протоколов не меняли свой интерфейс с транспортной средой и внутренние функциональные возможности, когда начинают использовать SCTP вместо другого транспортного протокола. Другой аспект состоит в том, что поддерживаемая архитектура стека протоколов согласована с архитектурой Интернет без нарушения собственных правил.

Пользовательский уровень адаптации ISDN (IUA)

Существует необходимость доставки сообщений сигнальных протоколов сети с коммутацией каналов от сигнального шлюза (SG) ISDN к контроллеру шлюза среды передачи (MGC). Механизм доставки должен поддерживать:

- транспортировку пограничных примитивов Q.921/Q.931;
- связь между модулями управления уровнями SG и MGC;
- управление активными связями между SG и MGC.

Данным уровнем предусматривается поддержка первичного и базового доступов ISDN (PRI и BRI) как для режима "точка-точка", так и для разветвленного режима "точка

– несколько точек". Процедуры уровня адаптации QSIG не отличаются от аналогичных процедур Q.931.

Пользовательский уровень адаптации MTP уровня 2 (M2UA – MTP2 –User Adaptation Layer)

Пользовательский уровень адаптации MTP уровня 2 обеспечивает эмуляцию одного звена MTP между двумя узлами ОКС7.

Избыточность звеньев достигается посредством многоточечного подключения собственно в пределах SCTP. В направлении к DPC (Destination Point Code – Код пункта назначения ОКС7) может иметься несколько звеньев. Избыточность приложений поддерживается на пользовательских уровнях адаптации посредством переключения с одного соединения на другое при необходимости.

При необходимости доставки сообщений сигнальных протоколов сети КК от сигнального шлюза (SG) к контроллеру шлюза среды передачи (MGC) или пункту сигнализации IP (IPSP) механизм доставки должен поддерживать:

- интерфейс на границе MTP уровня 2 и MTP уровня 3;
- связь между модулями управления уровнями SG и MGC;
- управление активными связями между SG и MGC.

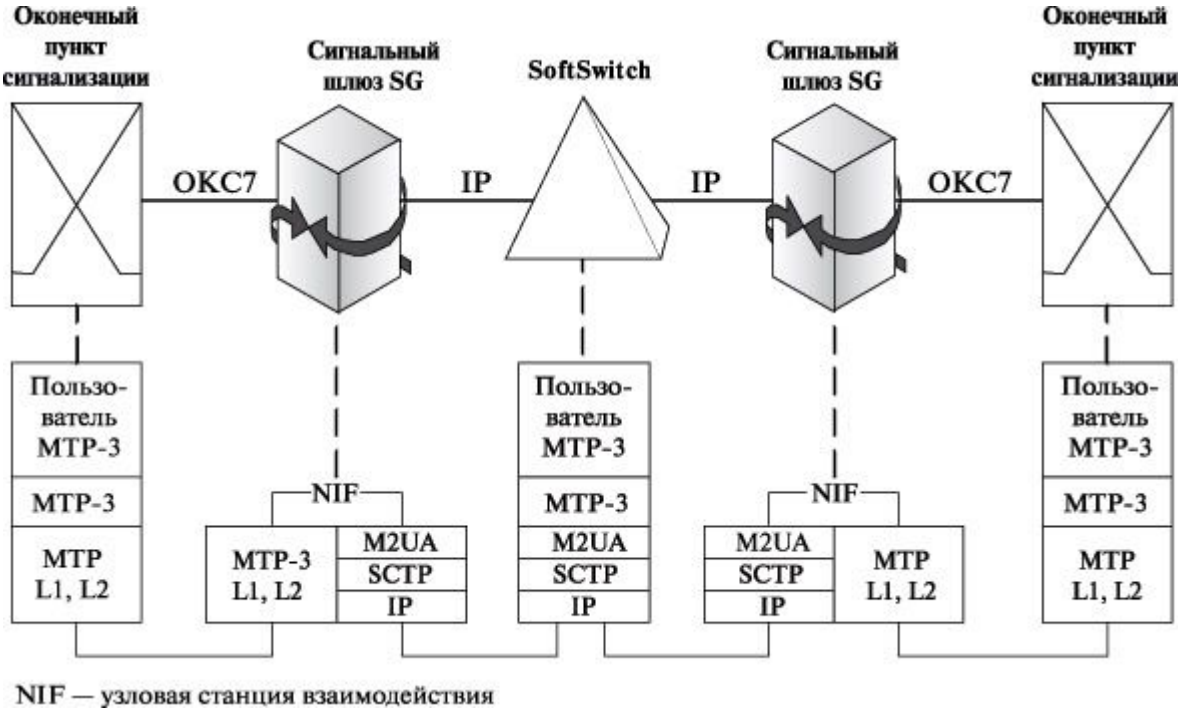


Рис. 3.10. Функции M2UA в Softswitch

Другими словами, SG будет иметь возможность транспортировать сообщения MTP уровня 3 к MGC или IPSP. В случае доставки от SG к IPSP, SG и IPSP функционируют как традиционные узлы ОКС7, используя сеть IP в качестве нового типа звена ОКС7. Этим обеспечивается полномасштабная обработка сообщений MTP уровня 3 и соответствующие возможности управления сетью (рис. 3.10).

Пользовательский уровень адаптации M2PA

Пользовательский уровень адаптации M2PA (MTP2 Peer-to-Peer Adaptation Layer) также обеспечивает адаптацию SCTP к MTP3, но уже в другой области. Аналогично случаю с M2UA, уровень MTP3 в узле сети IP (Softswitch, в частности) обменивается информацией с M2PA, как если бы он был обычным MTP2. Различия между M2UA и M2PA определяются их ролями в сетевой архитектуре: если Softswitch соединяется с сетью ОКС7 просто на правах терминала сигнализации ОКС7, то достаточно применения M2UA. Шлюз SG, который использует M2PA, сам фактически является транзитным пунктом сигнализации STP на базе IP, у него есть собственный код пункта сигнализации (DCP), он может также выполнять функции сигнализации верхнего уровня, такие как функции SCCP.

Пользовательский уровень адаптации MTP уровня 3 (M3UA)

Обеспечивает интерфейс между SCTP и теми протоколами ОКС7, которые используют услуги MTP3, например ISUP и SCCP. Благодаря M3UA эти протоколы не ощущают, что вместо типичной транспортировки MTP3 применяется транспортировка SCTP поверх IP. Однако M3UA – просто адаптационный уровень между протоколами верхнего уровня и SCTP, он не является полной копией MTP3 в IP-сети и не реализует некоторые стандартные управляющие сообщения сетевой сигнализации MTP3 (рис. 3.11).

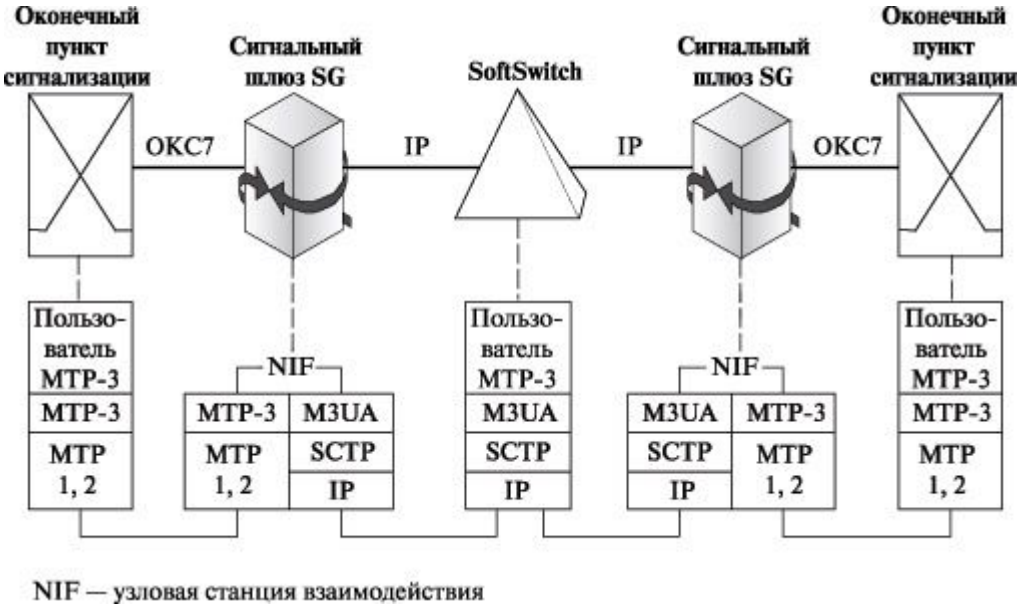


Рис. 3.11. Протокол M3UA

Для выхода на нужный сервер приложений (Application Server – AS) в SG должна осуществляться строгая процедура присвоения.

Уровень M3UA должен обслуживать несколько соединений SCTP (или по крайней мере одно). Выбор соединения SCTP может производиться по одной или нескольким частям полей DPC (код пункта назначения ОКС7).

Пользовательский уровень адаптации SCCP (SUA)

Пользовательский уровень адаптации SCCP (SUA)

Средствами сети IP возможна доставка сообщений подсистем пользователей SCCP. Архитектура такой доставки может представлять собой связь от SG ОКС7 к сигнальному узлу IP (например резидентной базе данных IP) или связь между двумя оконечными точками, расположенными в пределах сети IP. (рис. 3.12). Механизм доставки должен поддерживать:

- передачу сообщений пользователей SCCP;
- услугу SCCP, не ориентированную на соединение;
- услугу SCCP. ориентированную на соединение;
- взаимодействие равноуровневых объектов пользователей SCCP в полном объеме;
- управление транспортными связями SCTP между SG и одним или несколькими сигнальными узлами IP;
- функционирование сигнальных узлов IP с распределенной структурой;

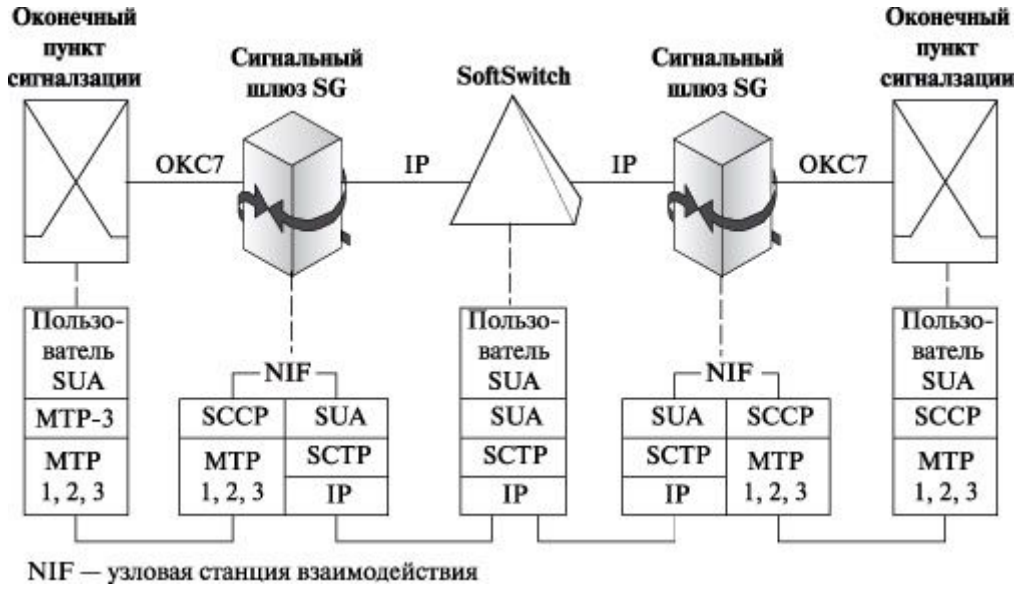


Рис. 3.12. Протокол SUA

- в целях управления – выдачу отчетов об изменении состояний конфигурации в асинхронном режиме.

SCTP для MEGACO

Направленные на достижение высокой пропускной способности и доступности, реализации протокола MEGACO могут особенно эффективно использоваться в сочетании с теми возможностями образования информационных потоков, избыточности сетевой поддержки, исключения перегрузок и обеспечения высоких характеристик информационной безопасности, которые предоставляются протоколом SCTP.

Реализациями MEGACO могут применяться следующие предоставляемые SCTP возможности:

- транспортировка, основанная на передаче дейтаграмм;
- надежность доставки информации: как транспортный протокол повышенной надежности, SCTP обеспечивает механизмы восстановления пакетов

информации при ее потере или дублировании. Указанное свойство позволяет упростить разработку уровня приложений;

- надежность доставки сообщений при обеспечении очередности и без таковой: при необходимости ускоренного обслуживания приложения для каждого сообщения может устанавливаться высший по сравнению с не нуждающимися в обеспечении очередности приоритет транзакций:
- передача потоков информации: SCTP в состоянии обеспечить до 65536 однонаправленных потоков в каждом направлении связи MGC-MG. SCTP передает сообщения и обрабатывает принимаемые сообщения одного потока независимо от порядка или статуса сообщений других потоков. Приложение имеет возможность эффективно избегать возникновения блокировок линии посредством передачи информации независимых друг от друга транзакций по разным потокам;
- защита против столкновений сообщений: встроенный в SCTP механизм шифрования обеспечивает защиту на узле MGC или MG;
- управление сетевыми перегрузками: средствами SCTP для обнаружения и обработки случаев перегрузки сети обеспечены эффективные средства;
- управление резервным маршрутом: для крупного MG на сетевом уровне может требоваться наличие с MGC связи, имеющей повышенную устойчивость к отказам.

В целях предоставления резервных маршрутов SCTP поддерживает функционирование нескольких находящихся в разных местах (multi-homed) узлов IP.

SCTP обеспечивает проверку доступности, функции ускоренного переключения в аварийных ситуациях (switch-over/fail-over) и (потенциально) балансирование нагрузки между резервными маршрутами

Лекция 4. Оборудование ССП

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.

Шлюзы (Gateways) – устройства доступа к сети и сопряжения с существующими сетями. Оборудование *шлюзов* реализует функции по по преобразованию сигнальной информации сетей с коммутацией каналов 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.

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.

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.

Лекция 5. Программный коммутатор 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.

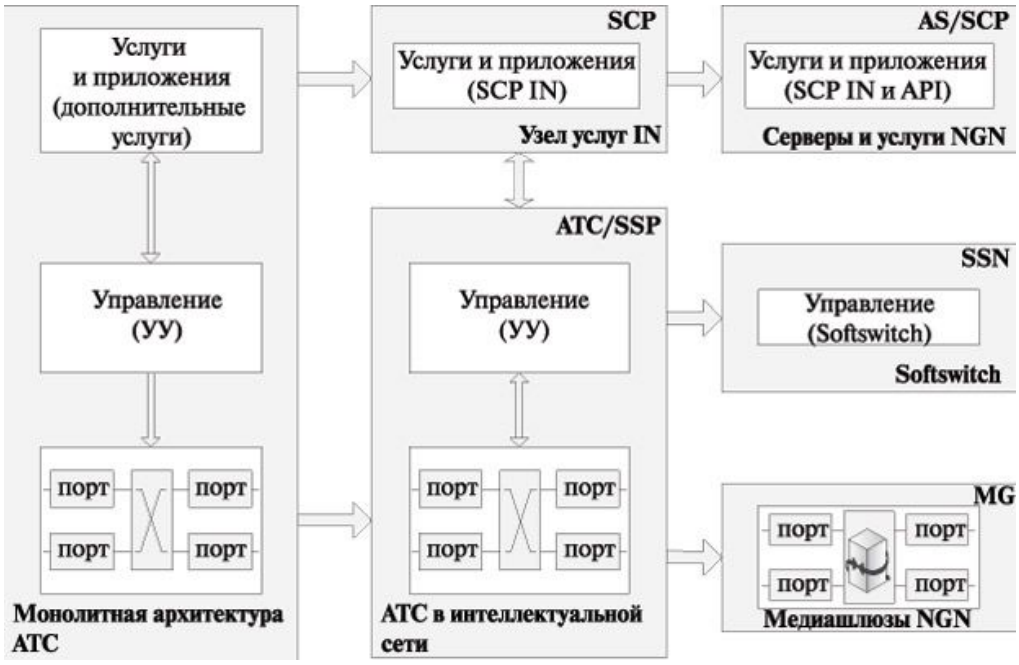


Рис. 5.1. Декомпозиция АТС и Softswitch

Рис. 5.2. Эталонная архитектура Softswitch

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. 5.1).

Согласно эталонной архитектуре *Softswitch*, разработанной консорциумом IPCC (International Packet Communication Consortium), в ней предусматривается четыре представленные на рис. 5.2 функциональные плоскости:

- транспортная;
- управления обслуживанием вызова и сигнализации;
- услуг и приложений;
- эксплуатационного управления.

Транспортная плоскость

Транспортная плоскость (Transport Plane) отвечает за транспортировку 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 стороны других 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

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

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.

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. 5.2 таким образом, чтобы разместить эти 12 автономных функциональных объектов (ФО) на плоскостях эталонной архитектуры *Softswitch* (рис. 5.3).

Рис. 5.3. Функциональные объекты эталонной архитектуры Softswitch AS-F — ФО сервера приложений; SC-F — ФО управления услуга- ми; CA-F —ФО устройства управления шлюзом; MGC-F — ФО контроллера медиашлюзов; SPS-F— ФО прокси-сервера SIP; R-F — ФО маршрутизатора вызова; A-F — ФО учета, авторизации, аутентентификации; MS-F —ФО транспортного сервера; SG-F — ФО шлюза

сигнализации; MG-F —ФО медиашлюза; IW-F — ФО взаимодействия; AGS-F — ФО сигнализации шлюза доступа.

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 прозрачно 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.

Лекция 6. Реализация Softswitch

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. 6.1. 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).

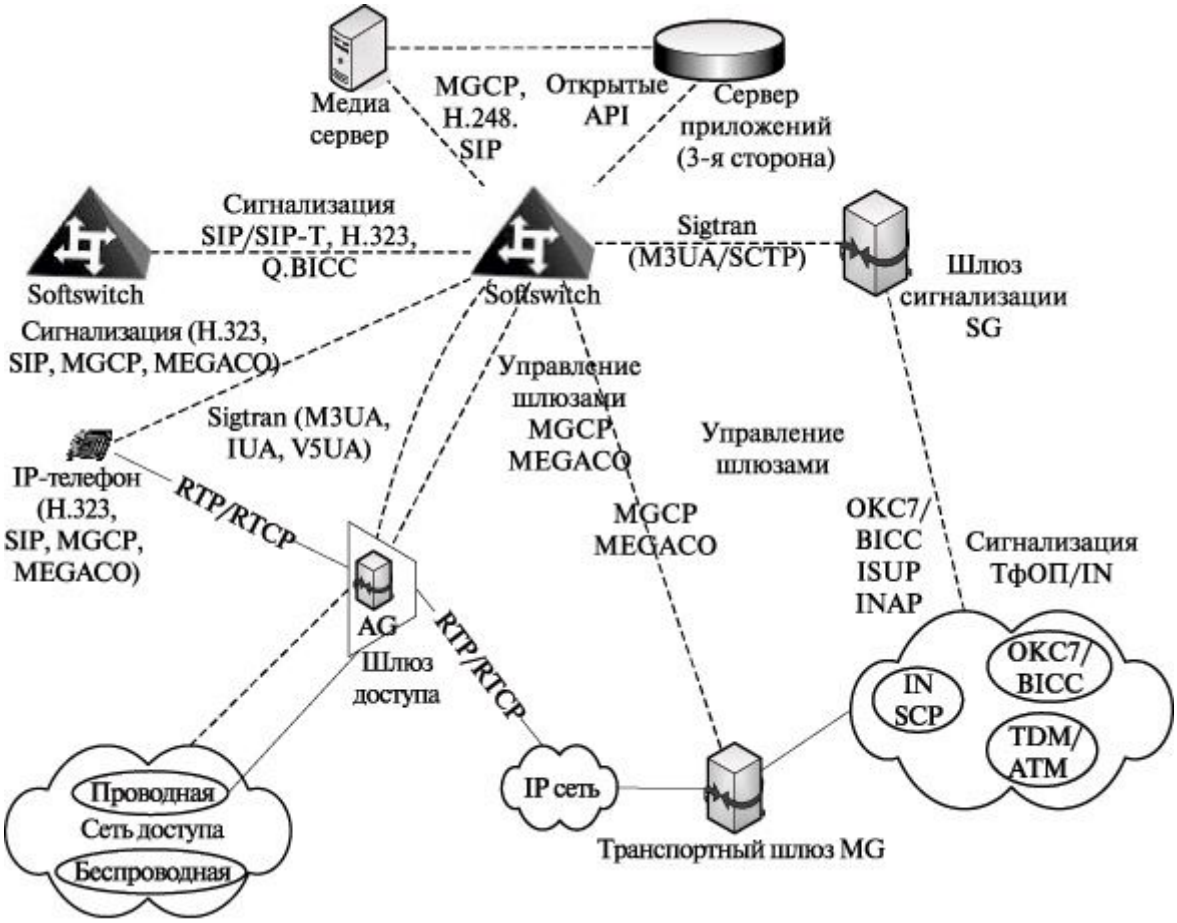


Рис. 6.1. Пример архитектуры ССП

Softswitch в данном примере выполняет функции MGC-F, R-F и A-F, обрабатывает всю сигнализацию, управляет TG, AG и соответствующим выделением медиаресурсов, а также обеспечивает 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.

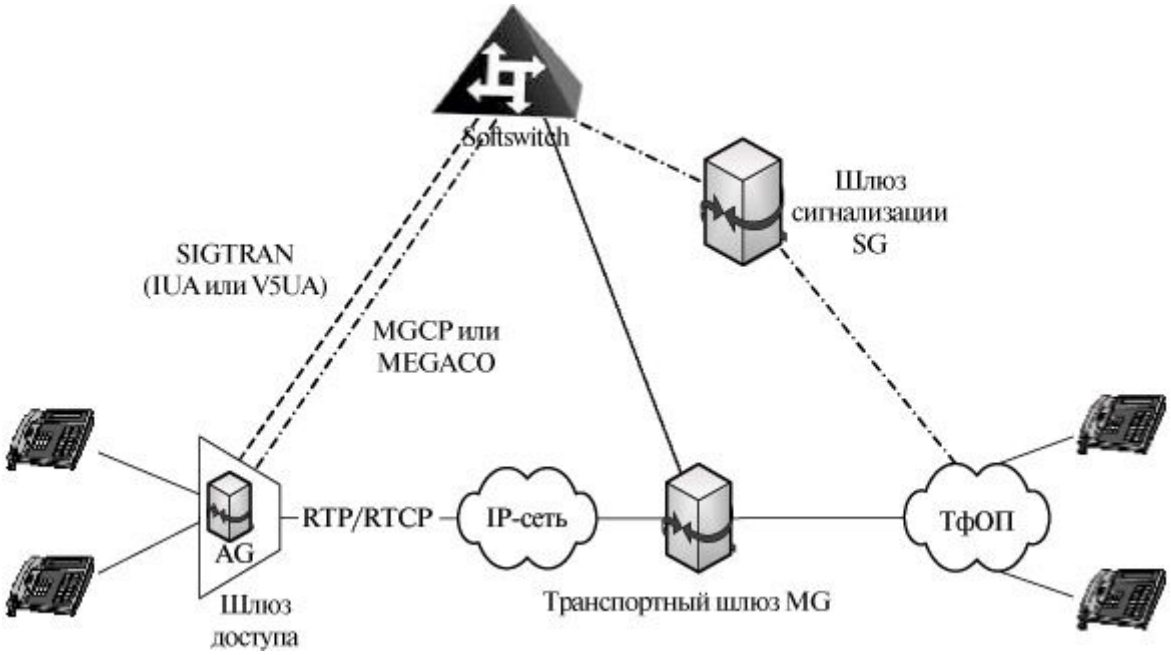


Рис. 6.2. Пример с ISDN и V5

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. 6.2 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. 6.3 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 RTP 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).

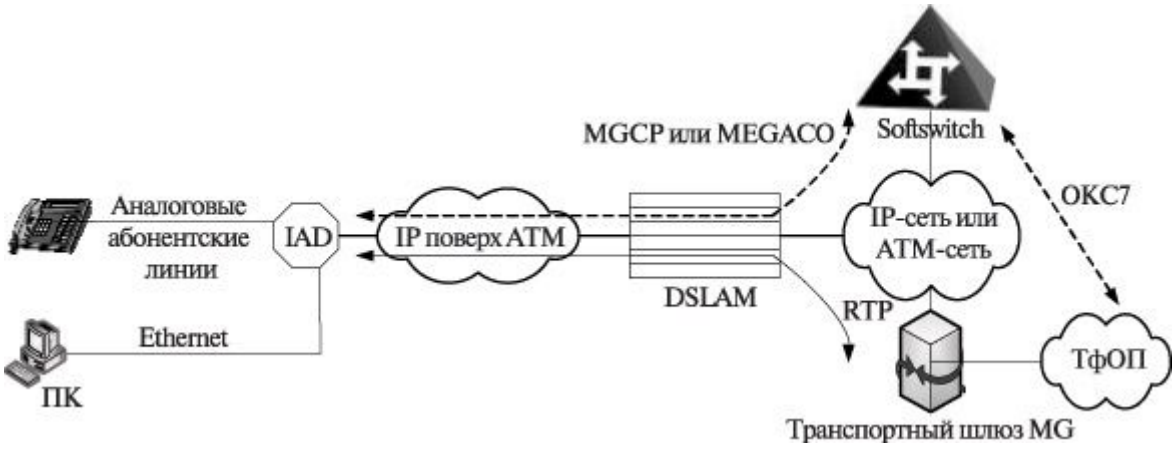


Рис. 6.3. Архитектура ССП с IAD и DSLAM

Взаимодействие Softswitch и ОКС7

Рассмотренная ранее 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. 6.4, причем в число используемых протоколов входят SCTP, M3UA или M2UA.

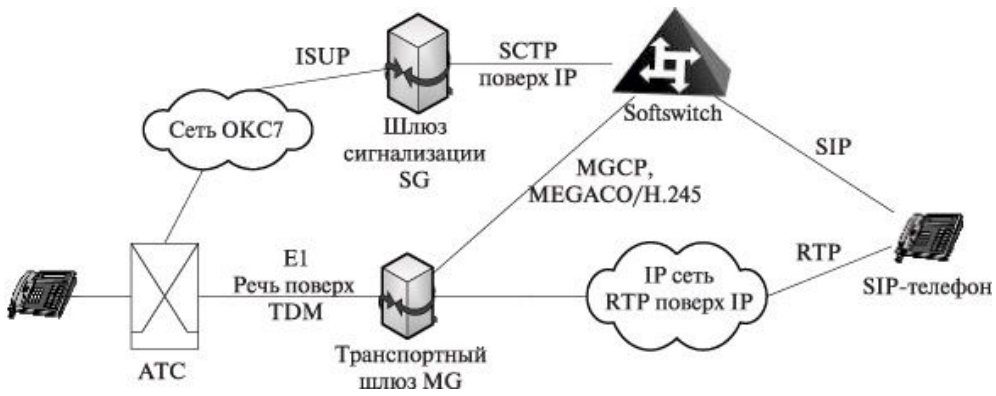


Рис. 6.4. Взаимодействие ОКС7 и архитектуры Softswitch

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.

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.

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.

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.

Лекция 7. Качество обслуживания

Одним из основных аспектов, который должен приниматься во внимание при проектировании сетей ССП, является обеспечение *качества обслуживания*. Специфика пакетных сетей состоит в том, что, в отличие от сетей с коммутацией каналов, в одном и том же информационном потоке может передаваться разнородный трафик. При этом каждый из типов трафика характеризуется рядом критичных и некритичных параметров. Для передачи голосового трафика через пакетные сети вводится понятие классов обслуживания, позволяющих оценить качество предоставления услуги в пакетной сети. Определение качества обслуживания в настоящий момент является субъективным и базируется на методе экспертных оценок, т.е. априори невозможно абсолютно гарантировать, что при проектировании сети будут заложены сетевые характеристики, позволяющие однозначно обеспечить требуемое качество. С другой стороны, пакетные сети имеют развитые механизмы обеспечения качества обслуживания, использование которых позволяет влиять на предоставление услуг связи в процессе эксплуатации.

Функции качества обслуживания (QoS) заключаются в обеспечении гарантированного и дифференцированного обслуживания сетевого трафика путем передачи контроля за использованием ресурсов и загруженностью сети ее оператору. *QoS* представляет собой набор требований, предъявляемых к ресурсам сети при транспортировке потока данных. *QoS* обеспечивает сквозную гарантию передачи данных и основанный на системе правил контроль за средствами повышения производительности IP-сети, такими как механизм распределения ресурсов, коммутация, маршрутизация, механизмы обслуживания очередей и механизмы отбрасывания пакетов.

Ниже перечислены некоторые из основных преимуществ *качества обслуживания*.

- Обеспечение поддержки существующих и появляющихся мультимедийных служб и приложений.
- Передача контроля за ресурсами сети и их использованием сетевому оператору. Обеспечение гарантии обслуживания и дифференцирование сетевого трафика. Это условие является необходимым для объединения аудио/видеотрафика и трафика приложений в пределах одной IP-сети.
- Возможность поставщикам услуг Internet предлагать клиентам дополнительные услуги наряду со стандартной услугой негарантированной доставки данных (другими словами, предоставлять услуги в соответствии с так называемым классом обслуживания – Class of Service (***CoS***)).
- Играет значительную роль в развитии новых сетевых технологий, таких как виртуальные частные сети (Virtual Private Networks – VPNs).

Способность сети обеспечивать различные уровни обслуживания, запрашиваемые теми или иными сетевыми приложениями, наряду с проведением контроля за характеристиками производительности – полосой пропускания, задержкой/дрожанием и потерей пакетов – может быть классифицирована по трем перечисленным ниже категориям.

Негарантированная доставка данных (best-effort service). Обеспечение связности узлов сети без гарантии времени и самого факта доставки пакета в пункт назначения. Отбрасывание пакета может произойти только в случае переполнения буфера входной или выходной очереди маршрутизатора.

На самом деле негарантированная доставка пакетов не является частью *QoS* вследствие отсутствия гарантии *качества обслуживания* и гарантии обеспечения доставки пакетов. Негарантированная доставка пакетов является на сегодняшний день единственной услугой, поддерживаемой в Internet.

Дифференцированное обслуживание (differentiated service). Дифференцирование обслуживание предполагает разделение трафика на классы на основе требований к *качеству обслуживания*. Каждый класс трафика дифференцируется и обрабатывается сетью в соответствии с заданными для этого класса механизмами *QoS*. Подобная схема обеспечения *качества обслуживания* (*QoS*) довольно часто называется схемой *CoS*.

Следует отметить, что дифференцированное обслуживание само по себе не предполагает обеспечения гарантий предоставляемых услуг. В соответствии с данной схемой трафик распределяется по классам, каждый из которых имеет свой собственный приоритет. По этой причине дифференцированное обслуживание довольно часто называют мягким *QoS (soft QoS)*.

Дифференцированное обслуживание удобно применять в сетях с интенсивным трафиком приложений.

Гарантированное обслуживание (guaranteed service). Гарантированное обслуживание предполагает резервирование сетевых ресурсов с целью удовлетворения специфических требований к обслуживанию со стороны потоков трафика.

В соответствии с гарантированным обслуживанием выполняется предварительное резервирование сетевых ресурсов по всей траектории движения трафика.

Гарантированное обслуживание довольно часто называют еще жестким *QoS (hard QoS)* в связи с предъявлением строгих требований к ресурсам сети.

К сожалению, резервирование ресурсов на всем пути следования отдельных потоков трафика невозможно реализовать в масштабах магистрали Internet, обслуживающей в отдельный момент времени тысячи потоков данных.

Характеристики производительности сетевого соединения

Внедрение механизмов *QoS* предполагает обеспечение со стороны сети соединения с определенными ограничениями по производительности. Основными характеристиками производительности сетевого соединения являются полоса пропускания, задержка, дрожание и уровень потери пакетов.

Полоса пропускания

Термин **полоса пропускания (bandwidth)** используется для описания номинальной пропускной способности среды передачи информации, протокола или соединения.

Как правило, каждое соединение, нуждающееся в гарантированном *качестве обслуживания*, требует от сети резервирования минимальной полосы пропускания. К примеру, приложения, ориентированные на передачу оцифрованной речи, создают поток информации интенсивностью 64 Кбит/с. Эффективное использование таких приложений

становится практически невозможным вследствие снижения полосы пропускания ниже 64 Кбит/с на каком-либо из участков соединения.

Задержка при передаче пакета (packet delay), или **латентность (latency)**, на каждом переходе состоит из задержки сериализации, задержки распространения и задержки коммутации. Ниже приведены определения каждого из названных выше типов задержки.

Задержка сериализации (serialization delay). Время, которое требуется устройству на передачу пакета при заданной ширине полосы пропускания. Задержка сериализации зависит как от ширины полосы пропускания канала передачи информации, так и от размера передаваемого пакета. Например, передача пакета размером 64 байт при заданной полосе пропускания 3 Мбит/с занимает всего лишь 171 нс. Обратите внимание, что задержка сериализации очень сильно зависит от полосы пропускания: передача того же самого пакета размером 64 байт при заданной полосе пропускания 19,2 Кбит/с занимает уже 26 мс. Довольно часто задержку сериализации называют еще задержкой передачи (transmission delay).

Задержка распространения (propagation delay). Время, которое требуется переданному биту информации для достижения принимающего устройства на другом конце канала. Эта величина довольно существенна, поскольку в наилучшем случае скорость передачи информации соизмерима со скоростью света. Задержка распространения зависит от расстояния и используемой среды передачи информации, а не от полосы пропускания. Для линий связи глобальных сетей задержка распространения измеряется в миллисекундах. Для трансконтинентальных сетей Соединенных Штатов характерна задержка распространения порядка 30 мс.

Задержка коммутации (switching delay). Время, которое требуется устройству, получившему пакет, для начала его передачи следующему устройству. Как правило, это значение меньше 10 нс.

Обычно каждый из пакетов, принадлежащий одному и тому же потоку трафика, передается с различным значением задержки. Задержка при передаче пакетов меняется в зависимости от состояния промежуточных сетей.

Если сеть не испытывает перегрузки, то пакеты не ставятся в очередь в маршрутизаторах, а общее время задержки при передаче пакета состоит из суммы задержки сериализации и задержки распространения на каждом промежуточном переходе. В этом случае можно говорить о минимально возможной задержке при передаче пакетов через заданную сеть. Следует отметить, что задержка сериализации становится незначительной по сравнению с задержкой распространения при передаче пакета по каналу с большой пропускной способностью.

Если же сеть перегружена, задержки при организации очередей в маршрутизаторах начинают влиять на общую задержку при передаче пакетов, и приводят к возникновению разницы в задержке при передаче различных пакетов одного и того же потока. Колебание задержки при передаче пакетов получило название **джиттер-пакетов (packet jitter)**.

Данный параметр имеет большую важность, поскольку именно он определяет максимальную задержку при приеме пакетов в конечном пункте назначения. Принимающая сторона, в зависимости от типа используемого приложения, может попытаться компенсировать дрожание пакетов за счет организации приемного буфера для

хранения принятых пакетов на время, меньшее или равное верхней границе дрожания. К этой категории относятся приложения, ориентированные на передачу/прием непрерывных потоков данных, например IP-телефония или приложения, обеспечивающие проведение видеоконференций.

Потеря пакетов

Уровень потери пакетов (packet loss) определяет количество пакетов, отбрасываемых сетью во время передачи. Основными причинами потери пакетов являются перегрузка сети и повреждение пакетов во время передачи по линии связи. Чаще всего отбрасывание происходит в местах перегрузки, где число поступающих пакетов намного превышает верхнюю границу размера выходной очереди. Кроме того, отбрасывание пакетов может быть вызвано недостаточным размером входного буфера. Как правило, уровень потери выражается как доля отброшенных пакетов за определенный интервал времени.

Некоторые приложения неспособны нормально функционировать или же функционируют крайне неэффективно в случае потери пакетов. Подобные приложения требуют от сети гарантии надежной доставки всех пакетов.

Как правило, хорошо спроектированные сети характеризуются очень низким значением потери пакетов. Потеря пакетов также несвойственна приложениям, для которых были заранее зарезервированы требуемые этими приложениями ресурсы. Что касается волоконно-оптических линий связи со значением частоты появления ошибочных битов (Bit Error Rate – BER) 10e-9, то здесь потеря пакетов возможна только в случае их отбрасывания в местах перегрузки сети. Отбрасывание пакетов, к сожалению, является неизбежным явлением при негарантированной доставке трафика, хотя и в этом случае оно обусловливается крайней необходимостью.

Технология ATM с самого начала разрабатывалась для транспорта различных видов нагрузки, в том числе телефонной, и в нее были заложены средства обеспечения *QoS*. Технология же IP была создана для негарантированной доставки данных, поэтому требует для обеспечения *QoS* некоторых дополнительных механизмов, особенно для транспорта трафика реального времени, в том числе телефонного. Однако на сегодняшний день, как показывает анализ общемировых тенденций в развитии телекоммуникаций, технология IP является более перспективной. Это подтверждается и результатами испытаний оборудования Softswitch различных производителей в Технопарке ЦНИИС, которые показали, что оборудование Softswitch большинства производителей ориентировано на применение в среде IP. Исходя из указанных обстоятельств, ниже более подробно будет рассмотрено обеспечение *QoS* в транспортных сетях IP.

В соответствии с Рекомендацией МСЭ-Т I.380/Y.1540 основными параметрами, характеризующими *QoS* в сетях IP, являются:

- задержка переноса пакетов;
- вариация задержки пакетов (джиттер);
- коэффициент потери пакетов;
- коэффициент ошибок по пакетам.

Последний параметр зависит в основном от используемых на физическом уровне сети систем передачи, и проблем с ним, как правило, не возникает. Механизмы обеспечения *QoS* в сетях IP направлены на улучшение первых трех из указанных параметров. Именно они и являются основными характеристиками транспортной сети, определяющими качество передачи речи (рис. 7.1). Эти же параметры, как правило, используются и в соглашениях об уровне обслуживания (Service Level Agreement — ***SLA***), предлагаемых ведущими операторами своим клиентам.

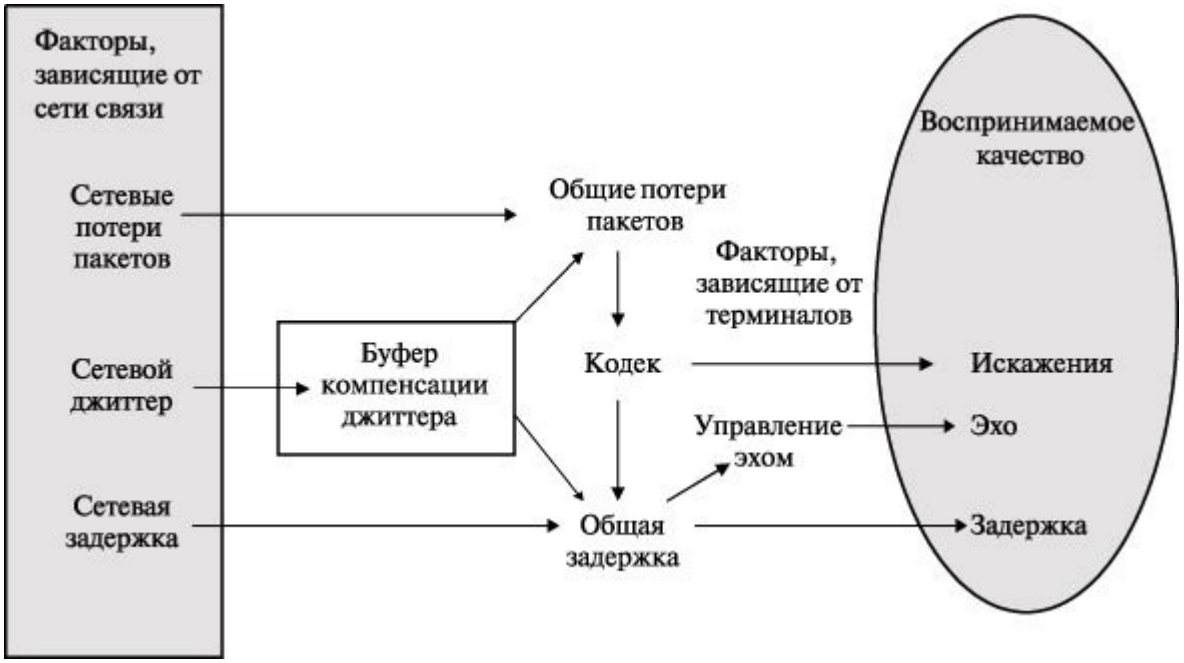


Рис. 7.1. Взаимовлияние факторов, определяющих качество передачи речи

Категории и классы качества передачи речи

Документ ETSI TS 102 024 – 2, разработанный в рамках проекта TIHPON (Release 5, сентябрь 2003 г.), определяет три класса качества:

- *широкополосный (wideband)*, обеспечивающий пользователям качество лучшее, чем в ТфОП. Он требует использования широкополосных кодеков (обрабатывающих аналоговые сигналы с полосой более 3,1 кГц) и сетей IP, спроектированных в соответствии с требованиями *QoS*;
- *узкополосный (narrowband)*, обеспечивающий пользователям качество, подобное ТфОП. Он требует использования спроектированных в соответствии с требованиями *QoS* сетей IP;
- *негарантированный (best effort)*, предоставляющий пригодные для использования услуги, но без гарантий на характеристики соединения. Могут быть периоды значительного ухудшения качества речи и большие задержки из конца в конец, которые отрицательно влияют на общую диалоговую интерактивность. Этот класс качества обеспечивается в сетях IP, разработанных без учёта требований *QoS*, например, общедоступного Интернета.

Широкополосный и узкополосный классы обеспечивают гарантии характеристик для 95% всех соединений.

Узкополосный класс делится на три подкласса:

- *высокий (high)*, обеспечивающий качество, эквивалентное тому, которое предоставляется услугами ЦСИС;
- *средний (medium)*, обеспечивающий качество, эквивалентное тому, которое предоставляется услугами беспроводной мобильной телефонии в условиях хорошей радиосвязи, например в сетях GSM, использующих кодеки EFR, или системами, использующими кодеки по Рекомендации МСЭ-Т G.726 на скорости 32 Кбит/с;
- *приемлемый (acceptable)*, обеспечивающий качество, эквивалентное тому, которое предоставляется обычными услугами беспроводной мобильной телефонии, например в сетях GSM, использующих кодеки FR, или системами, включающими геостационарные спутники.

Каждый из вышеуказанных классов определяется тремя характеристиками:

- общим рейтингом качества передачи (R);
- качеством речи, воспринимаемым слушателем (качество односторонней неинтерактивной передачи речи из конца в конец);
- задержкой из конца в конец (средней односторонней).

Значения этих характеристик для каждого из классов качества приведены в следующей таблице.

Таблица 7.1. Классы качества передачи речи в соответствии с подходом ETSI

Характеристика	**3 (широкополосный)**	**2 (узкополосный)**			**1(best effort)негарантированный**
		2-H (высокий)	**2-M (средний)**	**2-A (приемлемый)**	
Общий рейтинг качества передачи (R)	(В настоящее время находится на этапе изучения в международных организациях стандартизации)	> 80	> 70	> 50	> 50 (ориентир)
Относительное качество речи (одностороннее, неинтерактивное)	Лучше, чем G.711	Равно или лучше, чем G.726 при 32 Кбит/с	Равно или лучше, чем GSM-FR	Не определено	Не определено
Результирующий общий рейтинг качества передачи (R)	Не применяется	> 86	> 73	> 50	> 50
Задержка из конца в конец, мс	< 100	< 100	< 150	< 400	< 400(ориентир)

Услуга телефонной связи сети общего пользования должна обеспечивать пользователям качество передачи речи, соответствующее наилучшей и высокой категориям по Рекомендации МСЭ-Т G.109 или широкополосному и узкополосному высокому классам по ETSI TS 102 024 – 2.

Качество из конца в конец, соответствующее средней категории или узкополосному среднему классу, может предоставляться при соединениях с абонентами сетей подвижной связи или корпоративным клиентам при наличии с ними

соответствующих договоров. Более низкое качество в телефонных сетях общего пользования допускаться не должно.

Влияние оконечного оборудования и сети на показатели качества речи

Общее качество передачи речи определяется факторами, зависящими как от сети, так и от оконечного оборудования.

Основные параметры, влияющие на качество передачи речи из конца в конец, и их отношение к терминальному оборудованию и/или сети приведены в следующей таблице.

Таблица 7.2. Основные параметры качества передачи речи и их связь с терминальным оборудованием и/или сетью

Параметр	**Связан с**	
	терминальным оборудованием	**сетью**
Тип кодека	Да	Нет
Потери пакетов	Нет [1]	Да
Задержка	Да [2]	Да [3]
Вариации задержки	Нет [4]	Да [5]

Примечания.

1. Предполагается достаточно большая емкость буфера компенсации джиттера, позволяющая избежать потерь пакетов.
2. Обусловлена кодированием/пакетизацией речи и компенсацией джиттера.
3. Обусловлена маршрутизацией/распространением в сети.
4. Предполагается, что вся вариация задержки включена в задержку в терминале.
5. Вариация задержки вносится сетью, но компенсируются терминалом.

Функции качества обслуживания

Классификация и маркировка пакетов

Маршрутизаторы, расположенные на границе сети, используют функцию классификации для распознавания пакетов, принадлежащих различным классам трафика, в зависимости от значения одного или нескольких полей в заголовке TCP/IP. Функция маркировки пакетов используется для разметки классифицированного трафика путем установки значения поля IP-приоритета или поля кода дифференцированного обслуживания (Differentiated Services Code Point – DSCP). Более подробно функции классификации и маркировки пакетов рассматриваются в следующей лекции.

Управление интенсивностью трафика

Поставщики услуг используют ограничивающую функцию для приведения параметров поступающего в сеть клиентского трафика в соответствии с его профилем. В то же время корпорации используют выравнивающую функцию для дозирования поступающего в сеть поставщика услуг трафика и выравнивания его интенсивности в соответствии с заданным профилем.

Распределение ресурсов

Наиболее распространенным механизмом обслуживания очередей в маршрутизаторах и коммутаторах современной Internet является ставший уже традиционным механизм "первым пришел, первым вышел" (first-in, first-out – FIFO). Несмотря на простоту реализации, для механизма FIFO характерно несколько фундаментальных проблем, затрудняющих выполнение функций *качества обслуживания*. Так, механизм FIFO не предусматривает приоритетной обработки чувствительного к задержке трафика путем его перемещения во главу очереди. Весь трафик обрабатывается одинаково, без учета принадлежности потоков к различным классам с разными требованиями к обслуживанию.

Минимальное требование, предъявляемое к поддерживающему функции *QoS* алгоритму обслуживания очередей, – способность дифференцировать и определять требования к обработке различных пакетов. В соответствии с этими параметрами алгоритм обслуживания должен планировать порядок передачи поставленных в очередь пакетов. Частота обслуживания пакетов одного и того же потока трафика определяет выделенную этому потоку полосу пропускания.

Предотвращение перегрузки и политика отбрасывания пакетов

Традиционный механизм обслуживания очередей FIFO предусматривает отбрасывание всех входящих пакетов после достижения максимального значения длины очереди. Подобный способ управления очередью получил название "отбрасывание хвоста" (tail drop) и характеризуется тем, что сигнал о перегрузке поступает лишь в момент фактического переполнения очереди. К сожалению, механизм FIFO не предусматривает проведения каких-либо активных действий по предотвращению перегрузки или по уменьшению размера очереди с целью снижения времени задержки. Активный алгоритм управления очередями позволяет маршрутизатору предвидеть перегрузку еще до переполнения очереди.

Маршрутизация

Традиционная маршрутизация осуществляется на основании адреса назначения пакета и предполагает выбор наименее короткого маршрута, хранящегося в таблице маршрутизации. К сожалению, подобный механизм является недостаточно гибким для некоторых сетевых сценариев. Маршрутизация на основе политики – это функция *качества обслуживания*, позволяющая заменить традиционный механизм маршрутизации пакетов механизмом, учитывающим всевозможные настраиваемые пользователем параметры.

Современные протоколы маршрутизации, работающие по методу выбора наименее короткого пути, позволяют учитывать такие значения метрики, как административное расстояние, вес или число переходов. Маршрутизация пакетов осуществляется на основании хранящейся в таблице маршрутизации информации без учета требований потока трафика к *качеству обслуживания* или доступности сетевых ресурсов на всем протяжении маршрута. *QoS*-маршрутизация представляет собой механизм маршрутизации пакетов, учитывающий требования потоков трафика к *качеству обслуживания* и осуществляющий выбор маршрута в зависимости от наличия сетевых ресурсов.

Более подробно маршрутизация на основе политики рассматривается в приложении в следующих лекциях.

Совокупность контролируемых параметров информационного потока гарантирует соответствие между реальными параметрами качества и заданными. Заданные параметры определяют допустимые алгоритмы его маршрутизации и необходимый объем сетевых ресурсов. Оператор может использовать различные механизмы управления сетевыми ресурсами, обеспечивающие необходимый уровень *QoS*. Эти механизмы зависят от концепции построения системы управления мультисервисной сети и особенностей оборудования, используемого в узлах коммутации магистральной сети.

Механизмы обеспечения качества абонентского обслуживания по транспортировке трафика в мультисервисной сети *QoS* могут реализовываться как на канальном (2-й уровень сетевой модели), так и на сетевом (3-й уровень модели) уровне модели ISO/OSI:

- механизмы *QoS* канального уровня ATM;
- механизмы *QoS* канального уровня коммутируемой сети Ethernet, основанные на классификации и приоритезации информационных потоков;
- технология MPLS (MultiProtocol Label Switching), повышающая эффективность прохождения трафика за счет упрощения процессов маршрутизации. Механизм MPLS может быть применен для обеспечения *QoS* как в среде Ethernet, так и в среде ATM.

Лекция 8. Методы обеспечения качества обслуживания: DiffServ и IntServ

Архитектура интегрированных услуг (IntServ)

Integrated Service (IntServ, RFC 1633) – модель интегрированного обслуживания: может обеспечить сквозное (End-to-End) *качество обслуживания*, гарантируя необходимую пропускную способность. *IntServ* использует для своих целей протокол сигнализации ***RSVP***, позволяет приложениям выражать сквозные требования к ресурсам и содержит механизмы обеспечения данных требований. *IntServ* можно кратко охарактеризовать как резервирование ресурсов (Resource reservation).

Протокол RSVP

Данный протокол позволяет приложениям посылать сигналы в сеть о своих *QoS*-требованиях для каждого потока. Чтобы определить количественные характеристики этих требований с целью управления доступом, используются служебные параметры.

Протокол *RSVP* применяется в приложениях с групповой рассылкой, таких как приложения аудио- и видеоконференций. Несмотря на то, что изначально протокол *RSVP* был ориентирован на мультимедийный трафик, с его помощью легко можно резервировать полосу пропускания для однонаправленного трафика, например для трафика сетевой файловой системы (Network File System – NFS) и управляющего трафика виртуальных частных сетей (Virtual Private Networks – VPN).

Протокол *RSVP* сигнализирует о запросах резервирования ресурсов по доступному маршрутизируемому пути в сети. При этом *RSVP* не производит собственную маршрутизацию; напротив, этот протокол был разработан для использования других, более мощных протоколов маршрутизации. Как и любой другой IP-трафик, при определении пути для данных и управляющего трафика *RSVP* полагается на применяемый в сети протокол маршрутизации.

Работа протокола RSVP

Конечные системы используют протокол *RSVP* для запрашивания у сети определенного уровня *QoS* от имени потока данных приложения. *RSVP*-запросы передаются по сети при прохождении каждого узла, который применяется для передачи потока. Протокол *RSVP* пытается зарезервировать ресурсы для потока данных на каждом из этих узлов.

RSVP-совместимые маршрутизаторы помогают доставить нужные потоки данных в нужную точку назначения. На рис. 8.1 изображены основные модули, информация о потоке данных и информация об управляющих потоках клиента и маршрутизатора, поддерживающих протокол *RSVP*

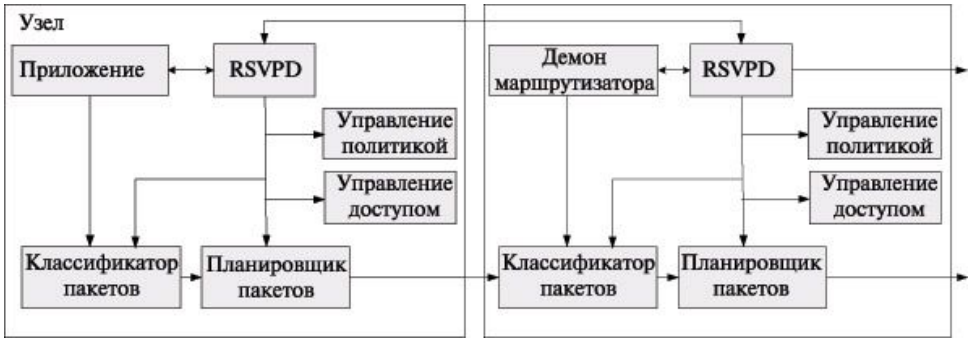


Рис. 8.1. Основные модули RSVP

Перед тем как зарезервировать ресурсы, *RSVP*-демон маршрутизатора соединяется с двумя локальными модулями принятия решения – модулем управления доступом (admission control) и модулем управления политикой (policy control). Модуль управления доступом определяет, имеет ли узел достаточно свободных ресурсов для обеспечения

запрошенного уровня *QoS*. Модуль управления политикой определяет, есть ли у пользователя права для того, чтобы произвести резервирование. Если какая-либо из проверок не прошла, *RSVP*-демон отправляет сообщение об ошибке процессу приложения, которое создало запрос. Если обе проверки прошли нормально, *RSVP*-демон устанавливает параметры классификатора пакетов (packet classifier) и планировщика пакетов (packet scheduler) для получения нужного уровня *QoS*. Классификатор пакетов определяет класс *QoS* для каждого пакета, а планировщик пакетов управляет передачей пакетов, основываясь на их классе *QoS*. Взвешенный алгоритм равномерного обслуживания очередей (Weighted Fair Queuing – WFQ) и взвешенный алгоритм произвольного раннего обнаружения (Weighted Random Early Detection – WRED) обеспечивают поддержку *QoS* на уровне планировщика. Алгоритмы WFQ и WRED рассмотрены ниже.

Во время процесса принятия решения модулем управления доступом резервирование затребованной полосы пропускания производится только в том случае, если для запрашиваемого класса трафика достаточно оставшейся части. В противном случае запрос на доступ отклоняется, но трафик все равно передается с *качеством обслуживания*, определенным по умолчанию для данного класса трафика. Во многих случаях, даже если запрос на доступ отклонен на одном или нескольких маршрутизаторах, модуль все еще может реализовать приемлемое *качество обслуживания*, установив резервирование на перегруженных маршрутизаторах. Это возможно из-за того, что другие потоки данных могут не полностью использовать заказанную ими полосу пропускания.

Резервирование всегда должно следовать по одному и тому же одноадресному пути или по многоадресному дереву. В случае выхода из строя линии связи маршрутизатор должен сообщить об этом *RSVP*-демону, чтобы генерируемые им *RSVP*-сообщения передавались по новому пути.

Процесс установки резервирования можно разбить на пять отдельных шагов.

1. Отправители данных посылают управляющие сообщения *RSVP PATH* по тому же пути, по которому они отправляют обычный трафик с данными. В этих сообщениях описываются данные, которые уже отправляются или только будут отправляться.
2. Каждый *RSVP*-маршрутизатор перехватывает PATH-сообщения, сохраняет IP-адрес предыдущей точки назначения, записывает вместо него свой собственный адрес и отправляет обновленное сообщение дальше по тому же пути, по которому передаются данные приложения.
3. Станции-получатели выбирают подмножество сеансов, для которых они получили PATH-информацию и с помощью *RSVP* RESV-сообщения запрашивают *RSVP*-резервирование ресурсов у предыдущего маршрутизатора. *RSVP RESV* -сообщения идут от получателя к отправителю в противоположном направлении по маршруту, пройденному *RSVP PATH*-сообщениями.
4. *RSVP*-маршрутизаторы определяют, могут ли они удовлетворить эти RESV-запросы. Если нет, они отказывают в резервировании. Если да, то они объединяют полученные запросы на резервирование и отсылают запрос предыдущему маршрутизатору.
5. Отправители, получив запросы на резервирование ресурсов от соответствующих маршрутизаторов, считают резервирование ресурсов состоявшимся. Т.е реальное резервирование ресурсов осуществляется RESV-сообщениями.

Механизм *RSVP*-резервирования схематически показан на рис. 8.2.

Рис. 8.2. Механизм RSVP-резервирования ресурсов

RSVP-компоненты

RSVP-компоненты выполняют следующие функции:

- *RSVP*-отправитель (*RSVP* sender) – это приложение, инициирующее отправку трафика в *RSVP*-сеансе. Ниже перечислены спецификации потока, которые *RSVP*-отправители могут передавать по *RSVP*-сети:
  - средняя скорость передачи данных;
  - максимальный размер всплеска.

По сети, состоящей из *RSVP*-совместимых маршрутизаторов (*RSVP*-enabled router network), прокладывается путь между *RSVP*-отправителями и *RSVP*-получателями.

- *RSVP*-получатель (*RSVP*-receiver) – это приложение, которое получает трафик в *RSVP*-сеансе. Во время конференций или при передаче голоса по протоколу IP (Voice over IP – VoIP) приложение может играть роль и *RSVP*-отправителя, и *RSVP*-получателя. Ниже перечислены спецификации потока, который *RSVP*-получатели могут передавать по *RSVP*-сети:
  - средняя скорость передачи данных;
  - максимальный размер всплеска;
  - *QoS*, включая:
    - гарантированное обслуживание – в PATH-сообщениях также описываются максимально возможные задержки в сети;
    - обслуживание с управляемой нагрузкой – маршрутизаторы гарантируют только то, что сетевые задержки будут минимальными.

Стили резервирования

RSVP-резервирование ресурсов для потока можно разбить на два главных типа: индивидуальное и общее.

Индивидуальное резервирование

Индивидуальное резервирование (distinct reservations) применяется в тех приложениях, в которых несколько источников данных могут отправлять информацию одновременно. В видеоприложениях каждый отправитель генерирует индивидуальный поток данных, для которого необходимо осуществлять отдельное управление доступом и планирование очереди на всем пути к получателю. Следовательно, для такого потока необходимо осуществлять отдельное резервирование ресурсов для каждого отправителя и для каждого канала в пути.

Самый простой случай индивидуального резервирования ресурсов наблюдается на примере приложения с одноадресным трафиком, где есть только один отправитель и один получатель.

Общее резервирование

Общее резервирование (shared reservations) применяется в тех приложениях, в которых несколько источников данных не склонно передавать информацию одновременно, например цифровые аудиоприложения, такие как приложения VoIP. В этом случае, поскольку в любой отдельно взятый промежуток времени разговор ведет небольшое число людей, информация передается лишь небольшим ограниченным количеством отправителей. Такой поток не нуждается в отдельном резервировании ресурсов для каждого отправителя, для него нужно всего лишь одно резервирование, которое при необходимости можно будет применить к любому отправителю в группе.

В терминах протокола *RSVP* такой поток называется общим потоком (shared flow); он устанавливается с помощью общего явного или группового резервирования. Стили резервирования рассматриваются ниже.

- При общем явном (Shared Explicit – SE) резервировании потоки, которые резервируют сетевые ресурсы, указываются отдельно.
- С помощью группового фильтра (Wildcard Filter – WF) полоса пропускания и характеристики задержки могут быть зарезервированы для любого отправителя. Такой фильтр не позволяет задать отправителей отдельно – он принимает всех отправителей, на что указывает установка адреса источника и порта в ноль.

Типы услуг

Протокол *RSVP* предоставляет два типа интегрированных услуг, которые получатели могут запрашивать с помощью сообщений *RSVP RESV*: службу регулируемой нагрузки и службу гарантированной битовой скорости.

Регулируемая нагрузка

Служба регулируемой нагрузки (controlled load service) обеспечивает гарантию того, что зарезервированный поток достигнет своего пункта назначения с минимальным вмешательством со стороны трафика, доставляемого без гарантий. Более того, в реализации этой услуги компанией Cisco предусмотрена изоляция отдельных зарезервированных потоков. Изоляция потока позволяет исключить влияние других присутствующих в сети зарезервированных потоков при резервировании ресурсов.

Как правило, служба регулируемой нагрузки применяется при передаче трафика Internet-приложений, чувствительных к перегрузкам в сети. Такие приложения отлично работают в незагруженных сетях, но сразу "приходят в негодность" при перегрузке. Примером может служить приложение, работающее по протоколу FTP (File Transfer Protocol – протокол передачи файлов).

Гарантированная битовая скорость

Служба гарантированной битовой скорости (guaranteed bit rate service) обеспечивает ограничение задержки без отбрасывания дейтаграмм, удовлетворяющих

параметрам трафика, в условиях отсутствия сбоев в работе сетевых компонентов или изменений в информации о маршрутах во время жизни потока. Эта служба гарантирует минимальное вмешательство со стороны трафика, доставляемого без гарантий, изоляцию зарезервированных потоков и числовое выражение максимальной задержки.

Служба гарантированной битовой скорости может обеспечить только максимальную, но не минимальную или среднюю задержку дейтаграмм.

Максимальная задержка очереди – это кумулятивная задержка передачи PATH-сообщения от источника до получателя. PATH-сообщение содержит информацию о задержке на всем пути от источника до получателя и в любое время предоставляет получателю ее точную оценку. Получатель использует информацию о задержке во время запроса гарантированного обслуживания.

Служба гарантированной битовой скорости лучше всего подходит для тех приложений масштаба реального времени, которые позволяют воспроизводить аудио- и видеофайлы.

Службы регулируемой нагрузки и гарантированной битовой скорости используют корзину маркеров для описания параметров потока данных.

Корзина маркеров – это механизм регулирования интенсивности трафика, определяющий среднюю скорость (средний объем данных, который можно передать за единицу времени), размер всплеска (объем данных, который можно отправить в течение заданного промежутка времени без ущерба для планирования очереди) и интервал измерения (квант времени).

При использовании обеих служб получатель запрашивает в RESV-сообщении определенную битовую скорость и размер всплеска. Планировщик WFQ и механизм управления очередью WRED с предпочтительным весом гарантируют, что трафик достигнет получателя через строго определенное время.

Масштабируемость протокола RSVP

Недостатком протокола *RSVP* является то, что объем требуемой информации о состоянии потоков увеличивается с ростом числа резервирований ресурсов для потоков трафика.

Так как в Internet-магистрали в любое время могут существовать многие сотни тысяч одноадресных и многоадресных потоков, использование информации о состоянии каждого потока считается неподходящим решением для магистралей Internet.

Архитектура дифференцированных услуг DiffServ

В 1998 году организация IETF сформировала рабочую группу по созданию дифференцированных услуг (***diffserv Working Group***). Архитектурную модель *diffserv* можно сравнить с мостом, соединяющим механизм гарантированного *качества обслуживания* модели *intserv* с механизмом негарантированной доставки трафика. Модель *diffserv* обеспечивает дифференцирование трафика путем его разбивки на классы с различным приоритетом.

Главной задачей подхода *diffserv* является определение стандартизированного байта дифференцированной услуги (DS) – байта типа обслуживания (Type of Service – ToS) из заголовка пакета IPv4 и байта класса трафика (Traffic Class) пакета IPv6. От данной маркировки зависит принятие решения о продвижении пакета данных на каждом переходе (per-hop behavior – PHB), т.е. в каждом промежуточном узле.

Архитектура дифференцированных услуг обеспечивает базовую основу (A Framework for Differentiated Services/Bemet Y. et al, Internet Draft), которая может быть использована поставщиками услуг для предоставления своим клиентам большого диапазона различных предложений в зависимости от предъявляемых требований к *качеству обслуживания*. Клиент может выбрать требуемый уровень услуг путем установки соответствующего значения поля кода дифференцированной услуги (Differentiated Services Code Point – DSCP) для пакетов определенного приложения. Код дифференцированной услуги определяет цепочку решений о продвижении пакета в каждом промежуточном узле сети поставщика услуг (PHB-политика).

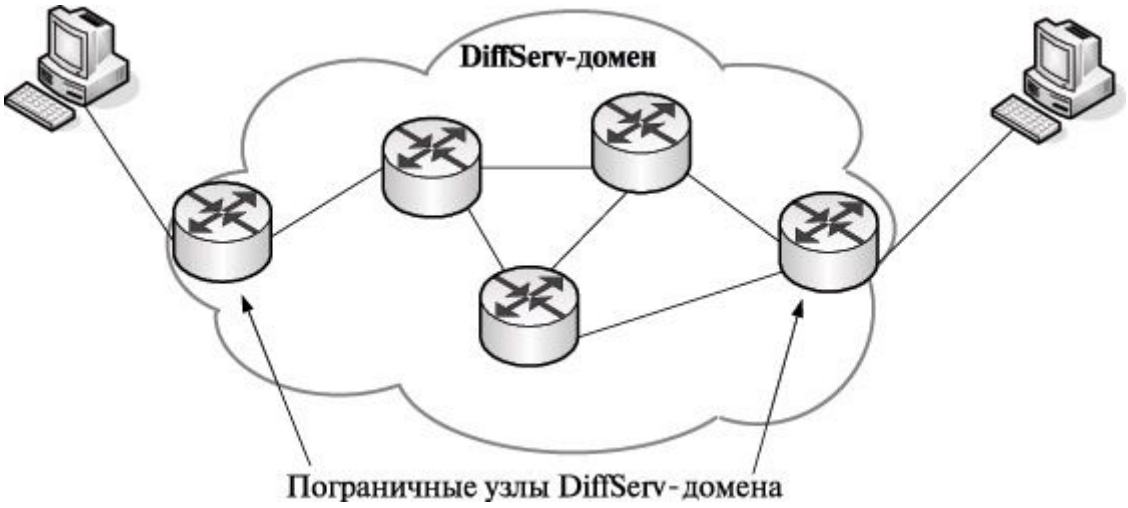


Рис. 8.3. Архитектура метода DiffServ

PHB-политика – политика пошагового обслуживания, определяет поведение сетевого узла в отношении пакетов с определенным значением поля кода дифференцированной услуги (DSCP). Все пакеты потока трафика со специфическим требованием к обслуживанию несут в себе одно и то же значение поля DSCP.

Таблица 8.1. Функциональные блоки архитектуры дифференцированных услуг

Функциональный блок	**Расположение**	**Функция**	**Действие**
Формирователи трафика	Входной интерфейс пограничного маршрутизатора *diffserv*-домена	Классификация пакетов, выравнивание и ограничение трафика	Ограничение входящего трафика и установка значения поля DSCP на основе профиля трафика
Устройства, реализующие PHB-политику	Все маршрутизаторы *diffserv*-домена	Распределение ресурсов и политика отбрасывания пакетов	PHB-политика обработки пакетов определяется на основе характеристик *качества обслуживания* соответствующих заданному значению поля DSC

Все узлы внутри *diffserv*-домена определяют PHB-политику, которая должна быть применена к пакету на основе хранящегося в нем значения поля кода дифференцированной услуги. Кроме того, пограничные узлы *diffserv*-домена выполняют

важную функцию формирования поступающего в *diffserv*-домен трафика. Формирование трафика включает в себя выполнение таких функций, как:

- классификация пакетов (установка значения поля DSCP);
- ограничение трафика.

Формирование трафика обычно выносится на входной интерфейс поступающих в *diffserv*-домен пакетов. Формирование играет решающую роль в управлении поступающим в *diffserv*-домен трафиком, поскольку в этом случае для каждого пакета сеть может определить соответствующую ему PHB-политику.

На рис. 8.3 схематически представлена архитектура дифференцированных услуг. Описание двух основных функциональных блоков этой архитектуры приведено в таблице 8.1.

Формирователи трафика, расположенные на границе сети

Формирователи трафика – это различные функции *качества обслуживания*, которые должны быть реализованы в пограничных устройствах сети. Граничные функции классифицируют или маркируют трафик путем установки соответствующего значения поля DSCP, а также проводят мониторинг входящего в сеть трафика с целью проверки его соответствия установленному профилю.

Код дифференцированной услуги представляет собой поле, на основании значения которого определяется способ обработки пакета в *diffserv*-домене. В качестве обрабатывающей трафик функции может выступать функция классификации пакетов, функция маркировки DSCP-поля или же функция дозирования трафика, наделенная либо полномочиями выравнивания трафика, либо полномочиями отбрасывания пакетов.

Классификатор пакетов

Классификатор пакетов выбирает пакет из потока трафика на основании анализа части содержимого заголовка пакета. Наиболее распространенный способ классификации пакетов заключается в анализе поля DSCP, однако теоретически возможна классификация пакета на основании значения других полей его заголовка. Функция классификации пакета определяет соответствующий этому пакету класс трафика.

Маркер

Эта функция предназначена для записи/перезаписи поля DSCP в зависимости от класса трафика, к которому относится данный пакет.

Дозирование трафика

Функция дозирования проверяет трафик на соответствие заданному профилю на основании дескриптора трафика, такого как корзина маркеров. Результаты проверки передаются функции маркировки трафика, а также либо функции выравнивания трафика, либо функции отбрасывания пакетов — для принятия соответствующего решения в отношении "плановых" и "внеплановых" пакетов.

Функция выравнивания трафика

Функция выравнивания трафика (traffic shaping) осуществляет задержку пакетов путем их буферизации с целью удовлетворения параметров заданного профиля.

Функция отбрасывания пакетов

Функция отбрасывания пакетов осуществляет отбрасывание всех пакетов, не удовлетворяющих параметрам заданного профиля трафика. Это действие часто называют также ограничением трафика (traffic policing).

PHB-политика

Сетевые узлы с поддержкой дифференцированного обслуживания используют поле DSCP в заголовке IP-пакета для определения соответствующей этому пакету PHB-политики.

PHB-политика может быть определена в терминах приоритета в предоставлении ресурсов по отношению к другим PHB-политикам или же с помощью таких измеряемых характеристик трафика, как задержка пакетов, уровень потери пакетов или дрожание трафика. В некоторой степени PHB-политику можно рассматривать как своеобразный "черный ящик", поскольку она определяет некоторое наблюдаемое извне поведение сетевого узла в отношении поступающих пакетов, не навязывая при этом конкретную реализацию.

В качестве стандартной PHB-политики в *diffserv*-сети можно рассматривать негарантированную доставку трафика. В соответствии с архитектурой дифференцированного обслуживания каждой PHB-политике рекомендуется назначить определенный код DSCP, однако поставщик услуг волен выбрать отличные от рекомендованных значения поля DSCP для своей собственной сети. Рекомендованное значение поля DSCP для политики негарантированной доставки пакетов равняется 000 000.

PHB-политика, соответствующая определенному классу трафика, зависит от целого ряда факторов:

- интенсивность входного потока или нагрузки для заданного класса трафика. Этот параметр контролируется пограничным формирователем трафика;
- распределение ресурсов для заданного класса трафика. Этот параметр контролируется функциями распределения ресурсов, реализованными в узлах *diffserv*-домена;
- уровень потери трафика. Этот параметр зависит от политики отбрасывания пакетов, проводимой в узлах *diffserv*-домена.

Существуют две стандартные PHB-политики – PHB-политика немедленной передачи (EF PHB) и PHB-политика гарантированной доставки (AF PHB).

PHB-политика немедленной передачи пакетов (Expedited Forwarding PHB – EF PHB)

Используется для обеспечения сквозного обслуживания пакетов в узлах *diffserv*-домена, характерными чертами которого являются низкий уровень потери пакетов, малая задержка, незначительное дрожание трафика, а также гарантированная полоса пропускания. Политика EF PHB применяется для обслуживания трафика таких

приложений, как передача голоса по сетям IP (Voice over IP – VoIP), приложений видеоконференций, а также для обеспечения таких услуг, как передача информации по виртуальным арендуемым каналам, поскольку эта услуга представляет собой двухточечное соединение конечных узлов *diffserv*-домена. Подобный тип обслуживания достаточно часто называют также услугами высокого класса (premium service).

Один из способов избежать задержки пакетов, связанной с возникновением больших очередей, – ограничение максимальной интенсивности входного потока трафика минимальной интенсивностью его выходного потока. PHB-политика немедленной передачи пакетов предусматривает установку значения интенсивности выходного потока трафика, в то время как интенсивность входного потока контролируется формирователями трафика, реализованными в пограничных устройствах сети.

Поскольку в соответствии с политикой EF PHB входящие пакеты не должны образовывать очередь (допускается очередь очень малого размера), интенсивность исходящего потока трафика должна быть равной интенсивности входящего потока или превышать ее. Следует отметить, что интенсивность исходящего потока (полоса пропускания) не должна зависеть от других потоков трафика. Как правило, интенсивность входящего и исходящего потоков измеряется с интервалами, равными времени, которое требуется для передачи MTU-пакета (пакета максимального размера, который может быть передан через интерфейс маршрутизатора) по данной линии связи.

Маршрутизатор может выделить ресурсы, достаточные для обеспечения определенной интенсивности исходящего трафика для заданного интерфейса, путем использования различных функциональных реализаций политики EF PHB. Когда речь идет о передаче трафика через перегруженный сегмент сети (а это предполагает наличие больших накопленных очередей), данная функциональная возможность может быть реализована за счет применения различных механизмов обслуживания очередей.

PHB-политика гарантированной доставки пакетов (AF PHB)

PHB-политика гарантированной доставки пакетов (Assured Forwarding PHB – AF PHB) представляет собой средство, с помощью которого поставщик услуг может обеспечить несколько различных уровней надежности доставки IP-пакетов, полученных из *diffserv*-домена клиента. Политика AF PHB является приемлемой для большинства TCP-приложений.

PHB-политика гарантированной доставки пакетов подразумевает наличие различных уровней обслуживания для каждого из четырех классов AF-трафика. Каждому классу AF-трафика соответствует собственная очередь пакетов, что позволяет проводить эффективное управление полосой пропускания. Каждый класс AF-трафика характеризуется тремя уровнями приоритета отбрасывания пакетов (низкий, средний и высокий), что позволяет реализовать механизм управления очередью по типу механизма произвольного раннего обнаружения (Random Early Detection – RED).

Политика AF PHB представляет собой средство, с помощью которого поставщик услуг может обеспечить несколько различных уровней надежности доставки IP-пакетов в зависимости от значения поля DSCP.

Существует три решения формирования политики PHB:

- инициализация сети;

- сигнализация о *качестве обслуживания*;
- диспетчер политик.

Инициализация сети

Один из способов распределения ресурсов заключается в инициализации ресурсов сети с использованием эвристических методов или техники систематического моделирования. Следует отметить, что этот метод может быть применен только в сетях небольшого размера, для которых политики *QoS* и профили трафика остаются неизменными на протяжении достаточно долгого промежутка времени.

Сигнализация о качестве обслуживания

В соответствии с этим методом реализации PHB-политики приложения извещают сеть о требованиях к *качеству обслуживания* с помощью сигнального протокола *RSVP* . С точки зрения протокола *RSVP diffserv*-домен рассматривается как еще одно звено сети, требующее управления доступом.

Диспетчер политик QoS

Определение политики обусловливает выбор уровней *QoS*, применяемой к потоку трафика. Политики назначаются с помощью протокола распространения политик – COPS (Common Open Policy Service) разработанного группой IETF.

Механизмы обработки очередей FIFO

Элементарная очередь с последовательным прохождением пакетов, работающая по принципу "первым пришел – первым ушел" (first-in first-out – FIFO). По сути, здесь нет никакой приоритезации.

PQ. Очереди приоритетов

Priority Queuing (PQ) обеспечивает безусловный приоритет одних пакетов над другими. Всего 4 очереди: high, medium, normal и low. Обработка ведется последовательно (от high до low), начиная с высокоприоритетной очереди, и до ее полной очистки не переходит к менее приоритетным очередям. Таким образом, возможна монополизация канала высокоприоритетными очередями. Трафик, приоритет которого явно не указан, попадет в очередь по умолчанию (default).

CQ. Произвольные очереди

Custom Queuing (CQ) обеспечивает настраиваемые очереди. Предусматривается управление долей полосы пропускания канала для каждой очереди. Поддерживается 17 очередей. Системная 0 очередь зарезервирована для управляющих высокоприоритетных пакетов (маршрутизация и т.п.) и пользователю недоступна.

Очереди обходятся последовательно, начиная с первой. Каждая очередь содержит счетчик байтов, который в начале обхода содержит заданное значение и уменьшается на размер пакета, пропущенного из этой очереди. Если счетчик не 0, то пропускается следующий пакет целиком, а не его фрагмент, равный остатку счетчика.

WFQ. Взвешенные справедливые очереди

Weighted Fair Queuing (WFQ) автоматически разбивает трафик на потоки (flows). По умолчанию их число равно 256, но может быть изменено. Если потоков больше, чем очередей, то в одну очередь помещается несколько потоков. Принадлежность пакета к потоку (классификация) определяется на основе ToS, IP-адреса источника, IP-адреса назначения, порта источника и порта назначения (протокол IP). Каждый поток использует отдельную очередь.

Обработчик WFQ (scheduler) обеспечивает равномерное (fair – справедливое) разделение полосы между существующими потоками. Для этого доступная полоса делится на число потоков, и каждый получает равную часть. Кроме того, каждый поток получает свой вес (weight), с некоторым коэффициентом обратно пропорциональный IP-приоритету (TOS). Вес потока также учитывается обработчиком.

В итоге WFQ автоматически справедливо распределяет доступную пропускную способность, дополнительно учитывая ToS. Потоки с одинаковыми IP-приоритетами ToS получат равные доли полосы пропускания; потоки с большим IP-приоритетом – большую долю полосы. В случае перегрузок ненагруженные высокоприоритетные потоки функционируют без изменений, а низкоприоритетные высоконагруженные – ограничиваются.

Вместе с WFQ работает *RSVP* . По умолчанию WFQ включается на низкоскоростных интерфейсах.

WRED. Взвешенный алгоритм произвольного раннего обнаружения

Взвешенный алгоритм произвольного раннего обнаружения (Weighted Random Early Detection – WRED) предоставляет различные уровни обслуживания пакетов в зависимости от вероятности их отбрасывания и обеспечивает избирательную установку параметров механизма RED на основании значения поля IP-приоритета. Другими словами, алгоритм WRED предусматривает возможность более интенсивного отбрасывания пакетов, принадлежащих определенным типам трафика, и менее интенсивного отбрасывания всех остальных пакетов.

CBWFQ

Class Based Weighted Fair Queuing (CBWFQ) соответствует механизму обслуживания очередей на основе классов. Весь трафик разбивается на 64 класса на основании следующих параметров: входной интерфейс, лист доступа (access list), протокол, значение DSCP, метка MPLS *QoS*.

Общая пропускная способность выходного интерфейса распределяется по классам. Выделяемую каждому классу полосу пропускания можно определять как в абсолютном значении (bandwidth в kbit/s) или в процентах (bandwidth percent) относительно установленного значения на интерфейсе.

Пакеты, не попадающие в сконфигурированные классы, попадают в класс по умолчанию, который можно дополнительно настроить и который получает оставшуюся свободной полосу пропускания канала. При переполнении очереди любого класса пакеты данного класса игнорируются.

LLQ

Low Latency Queuing (LLQ) – очередность с низкой задержкой. LLQ можно рассматривать как механизм CBWFQ с приоритетной очередью PQ (LLQ = PQ + CBWFQ).

PQ в LLQ позволяет обеспечить обслуживание чувствительного к задержке трафика. LLQ рекомендуется в случае наличия голосового (VoIP) трафика. Кроме того, он хорошо работает с видеоконференциями.

Лекция 9. Технология MPLS

Основное достоинство TCP/IP – его многофункциональность и гибкость. Вот уже три десятка лет этот протокол является основным для сети Internet, объединяющей сейчас более 500 миллионов пользователей. За это время семейство TCP/IP, с одной стороны, пополнилось протоколами прикладного уровня, (такими как HTTP – гипертекстовый протокол, SMTP – почтовый протокол, FTP – протокол пересылки файлов и многие другие) а с другой – обрело совместимость со всеми популярными стандартами физического, канального и сетевого уровней, в том числе и X.25. Однако широкие возможности сети TCP/IP не отменяют ее недостатки. Основные из них – это проблемы безопасности и гарантии качества связи. И если задачу по обеспечению безопасности IP-сети еще можно решить, используя различные механизмы шифрования и защиты (например стандарты IPSec), то проблема отсутствия гарантированной скорости передачи данных, которую требуют такие чувствительные к задержкам приложения, как системы передачи голоса и видео, пока остается нерешенной.

Что касается протокола X.25, то в нем изначально была заложена высокая надежность. Когда X.25 создавался, преобладали аналоговые системы передачи данных и медные линии связи. Стремясь нивелировать невысокое качество каналов того времени, стандарт использует систему обнаружения и коррекции ошибок, что существенно повышает надежность связи, но зато замедляет общую скорость передачи данных. Кроме того, каждый коммутатор, через который проходит пакет информации, выполняет анализ его содержимого, что также требует времени и больших процессорных мощностей. С появлением оптоволоконных сетей столь высокие требования надежности, реализуемые X.25, стали излишними – достоинство протокола превратилось в его недостаток. Скорость передачи по протоколу X.25 не превышает 64 Кб/с.

Протоколом, призванным исправить недостатки X.25, стал Frame Relay. Он использует тот же принцип виртуальных каналов, однако анализ ошибок осуществляется только на пограничных точках сети, что привело к существенному увеличению скорости (в настоящее время – до 45 Мб/с). Существенным достоинством протокола стала возможность приоритезации разнородного трафика (включая данные, голос и видео), то есть пакетам различных приложений могут предоставляться различные классы обслуживания, благодаря чему пакеты с более высоким приоритетом доставляются "вне очереди". Эти преимущества Frame Relay были развиты при создании технологии асинхронной передачи (ATM).

Протокол ATM разбивает весь трафик на пакеты строго фиксированной длины (их называют ячейками), которые асинхронно мультиплексируются в единый цифровой тракт в соответствии с присвоенным приоритетом. Благодаря малой длине ячеек (53 байта), можно организовать одновременную передачу потока данных сразу нескольких служб, критичных ко времени доставки – ячейки с данными различных приложений будут вставляться в поток попеременно, обеспечивая каждому приложению необходимую скорость обмена данными. Технология ATM обеспечивает совместный пропуск трафика на скоростях от 1,5 Мб/с до 40 Гб/с. Как Frame Relay, так и ATM обеспечивают высокую степень безопасности — благодаря тому, что весь трафик в магистральной сети не маршрутизируется, а коммутируется на основе локальных меток DLCI (Frame Relay) или VPI/VCI (ATM) по виртуальным каналам, к которым несанкционированный пользователь не может подключиться, не изменив таблицы коммутации узлов сети.

Однако, при создании сетей с большим количеством точек доступа по виртуальным каналам, тот самый, "телефонный" принцип соединения, заложенный еще в технологии X.25 начинает доставлять определенные неудобства пользователям. Виртуальные сети (VPN) на основе протоколов Frame Relay и ATM становятся слишком громоздкими и трудно управляемыми. Действительно, чтобы обеспечить связь "каждый с каждым" необходимо выполнить операции по конфигурированию каждого канала. Сколько? Количество виртуальных каналов можно посчитать по формуле N*(N – 1)/2, где N – количество точек доступа. Допустим, что у компании 50 подразделений. В таком случае ей придется организовать 2450 двунаправленных каналов или 4900 однонаправленных. То есть при увеличении числа точек доступа вероятность ошибки в конфигурировании сети возрастает в квадратичной прогрессии. Да и стоить такая сеть будет немало, ведь операторы обычно требуют оплату в зависимости от количества каналов. Построение же сети на основе протокола ATM является и само по себе достаточно дорогой технологией, не считая необходимости адаптации оконечного оборудования к ATM. Поэтому сейчас этот протокол используется в основном для предоставления услуг на магистральном уровне, для передачи больших объемов информации.

По данным операторов сетей, до 90% от информации, пересылаемой в сетях Frame Relay и ATM, составляет IP-трафик. Таким образом, абсолютно логичной выглядит идея объединить в одной технологии те преимущества, что дает протокол IP, одновременно предоставляя гарантию качества и надежность протоколов ATM и Frame Relay.

В 1996 году Ipsilon, Cisco, IBM и несколько других компаний объединили свои фирменные разработки и создали технологию многопротокольной коммутации на основе меток (***MPLS – Multiprotocol Label Switching***). Основная идея разработки состояла в том, чтобы реализовать возможность передачи трафика по наименее загруженным маршрутам IP-сети и обеспечить легкость конфигурирования VPN с одновременной поддержкой гарантии качества передачи, а также присвоения приоритетов различным видам трафика.

Введение в MPLS

Многопротокольная коммутация меток ***MPLS*** – технология, разработанная рабочей группой по созданию интегрированных услуг IETF. Это новая архитектура построения магистральных сетей, которая значительно расширяет имеющиеся перспективы масштабирования, повышает скорость обработки трафика и предоставляет огромные возможности для организации дополнительных услуг.

Технология *MPLS* сочетает в себе возможности управления трафиком, присущие технологиям канального уровня, и масштабируемость и гибкость протоколов, характерные для сетевого уровня. Являясь результатом слияния механизмов разных компаний, она впитала в себя наиболее эффективные решения каждой. *MPLS* соединила в себе надежность ATM, удобные и мощные средства доставки и обеспечения гарантированного *качества обслуживания* IP-сетей, — такая интеграция сетей позволяет получить дополнительную выгоду из совместного использования протоколов IP и ATM.

Главная особенность технологии *MPLS* – отделение процесса коммутации пакета от анализа IP-адреса в его заголовке, что позволяет осуществлять коммутацию пакетов значительно быстрее. В соответствии с протоколом *MPLS* маршрутизаторы и коммутаторы присваивают на каждой точке входа в таблицу маршрутизации особую метку и сообщают эту метку соседним устройствам.

Наличие таких меток позволяет маршрутизаторам и коммутаторам, поддерживающим технологию *MPLS*, определять следующий шаг в маршруте пакета без выполнения процедуры поиска адреса. На сегодняшний день существуют три основные области применения *MPLS*:

- управление трафиком;
- поддержка классов обслуживания (CoS);
- организация виртуальных частных сетей (VPN).

Расположение технологии *MPLS* в семиуровневой модели ВОС показано на рис. 9.1.

Рис. 9.1. Плоскости MPLS

Сетевой уровень – это комплексный уровень, который обеспечивает возможность соединения и выбор маршрута между двумя конечными системами, подключенными к разным "подсетям", которые могут находиться в разных географических пунктах. В данном случае "подсеть" – это, по сути, независимый сетевой кабель (иногда называемый сегментом). Так как две конечные системы, желающие организовать связь, может разделять значительное географическое расстояние и множество подсетей, сетевой уровень является доменом маршрутизации. Протоколы маршрутизации выбирают оптимальные маршруты через последовательность соединенных между собой подсетей. Традиционные протоколы сетевого уровня передают информацию вдоль этих маршрутов.

Канальный уровень (формально называемый информационно-канальным уровнем) обеспечивает надежный транзит данных через физический канал. Выполняя эту задачу, канальный уровень решает вопросы физической адресации (в противоположность сетевой или логической адресации), топологии сети, линейной дисциплины (каким образом конечной системе использовать сетевой канал), уведомления о неисправностях, а также вопросы упорядоченной доставки блоков данных и управления потоком информации.

Физический уровень определяет электротехнические, механические, процедурные и функциональные характеристики активации, поддержания и дезактивации физического

канала между конечными системами. Спецификации физического уровня определяют такие характеристики, как уровни напряжений, синхронизацию изменения напряжений, скорость передачи физической информации, максимальные расстояния передачи информации, физические соединители и другие аналогичные характеристики.

"Multiprotocol" в названии технологии означает "многопротокольный". Это говорит о том, что технология *MPLS* применима к любому протоколу сетевого уровня, т.е. *MPLS* – это своего рода инкапсулирующий протокол, способный транспонировать информацию множества других протоколов высших уровней модели OSI. Таким образом, технология *MPLS* остается независимой от протоколов уровней 2 и 3 в сетях IP, ATM и Frame Relay, а также взаимодействует с существующими протоколами маршрутизации, такими как протокол резервирования ресурсов RSVP или сетевой протокол преимущественного выбора кратчайших маршрутов OSPF.

Представленная на рис. 9.1 плоскость пересылки данных *MPLS* не образует полноценного уровня, она "вклинивается" в сети IP, ATM или Frame Relay между 2-м и 3-м уровнями модели OSI, оставаясь независимой от этих уровней. Можно сказать, что одновременное функционирование *MPLS* на сетевом уровне и на уровне звена данных приводит к образованию так называемого уровня 2.5, где, собственно, и выполняется коммутация по меткам.

Основные понятия

Комитет IETF определил три основных элемента технологии *MPLS*:

- метка;
- ***FEC*** – класс эквивалентности пересылки;
- LSP – коммутируемый по меткам тракт;

Рассмотрим каждый из них подробно.

Метки

Метка – это идентификатор фиксированной длины, определяющий класс эквивалентности пересылки *FEC*. Метки имеют локальное значение, т.е. привязка метки к *FEC* используется только для пары маршрутизаторов. Метка используется для пересылки пакетов от верхнего маршрутизатора к нижнему, где, являясь входящей, заменяется на исходящую метку, имеющую также локальное значение на следующем участке пути. Метка передается в составе любого пакета, при этом ее место в пакете зависит от используемой технологии канального уровня.

Протокол *MPLS* поддерживает различные типы меток: это может быть 4-байтовая метка, которая вставляется между заголовками канального и сетевого уровня. Являясь протокольно независимой, она может использоваться для инкапсуляции пакетов любого протокола сетевого уровня. Это может быть метка идентификаторов виртуального канала и виртуального пути (VCI/VPI) или метка идентификатора соединения канального уровня (DLCI).

Размер метки составляет 4 байта. Идентификатор самой метки занимает первые 20 бит. Информация об уровне *качества обслуживания* в сети *MPLS* передается в поле CoS, занимающем следующие три бита в поле метки.

Подробнее поля метки будут рассмотрены в следующей лекции.

Стек меток

Пакет, передаваемый по сети *MPLS*, как правило, содержит не одну, а несколько меток. Такой набор меток образует стек. Основное назначение стека меток – поддержание древовидности множества трактов LSP, заканчивающихся в одном входном LSR, а, кроме того, в том, чтобы использовать метки при создании так называемых LSP- туннелей.

Стек меток будет рассмотрен подробнее в следующей лекции.

Класс эквивалентности пересылки FEC

FEC – это форма представления группы пакетов с одинаковыми требованиями к передаче. Как говорилось ранее, в заголовке IP-пакета содержится гораздо больше информации, чем требуется для выбора следующего маршрутизатора. Этот выбор можно организовать путем выполнения следующих двух групп функций в маршрутизаторе:

- относит пакет к определенному классу *FEC*;
- ставит в соответствие каждому *FEC* следующий шаг маршрутизации.

При традиционной IP-маршрутизации конкретный маршрутизатор тоже может считать, что два пакета принадлежат одному и тому же условному классу эквивалентности, если в его таблицах маршрутизации используется некий адресный префикс, идентифицирующий направление, в котором предполагаемые маршруты транспортировки этих двух пакетов совпадают наиболее долго. По мере продвижения пакета по сети каждый следующий маршрутизатор анализирует его заголовок и приписывает этот пакет к тому из собственных, принадлежащих только этому маршрутизатору классов эквивалентности, который соответствует тому же направлению. В отличие от традиционной маршрутизации, при использовании многопротокольной коммутации на основе меток пакет ставится в соответствие определенному классу *FEC* только один раз на входе в сеть *MPLS*. Этому *FEC* присваивается метка, передаваемая затем вместе с пакетом при его пересылке к следующему маршрутизатору. В остальных маршрутизаторах заголовок пакета не анализируется. Определение *FECs* реализуется на основе требований к обслуживанию данной совокупности пакетов или просто адресного префикса.

Таким образом, подводя итог вышесказанного, можно дать следующее определение *FEC*. *Класс эквивалентности пересылки FEC* – это форма представления группы пакетов с одинаковыми требованиями к их передаче, т.е. все пакеты такой группы обрабатываются одинаково на пути их следования к пункту назначения.

Примером *FEC* могут служить все IP-пакеты с адресами пунктов назначения, соответствующими некоторому префиксу, например 212.18.6. Возможны также *FEC* на основе префикса адреса и еще какого-нибудь поля IP-заголовка, например тип обслуживания (ToS). Каждый маршрутизатор сети *MPLS* создает таблицу, с помощью которой определяет, каким образом должен пересылаться пакет. Эта таблица, которая называется *информационной базой LIB*, содержит используемое множество меток и для

каждой из них – привязку "*FEC*-метка". Метки, используемые маршрутизатором LSR при привязке "*FEC*-метка", подразделяются на следующие категории:

- *на платформенной основе*, когда значения меток уникальны по всему тракту LSP; метки выбираются из общего пула меток, и никакие две метки, распределяемые по разным интерфейсам, не имеют одинаковых значений;
- *на интерфейсной основе*, когда значения меток связаны с интерфейсами: для каждого интерфейса определяется отдельный пул меток, из которого для этого интерфейса и выбираются метки. При этом метки, назначаемые для разных интерфейсов, могут быть одинаковыми.

Класс *FEC* представляет собой набор *FEC*-элементов, каждый из которых идентифицируется определенной меткой. На сегодняшний день существует всего два *FEC*-элемента: Address Prefix и Host Address.

При соотнесении пакетов по различным *FEC* большую роль играют IP-адреса, приоритеты обслуживания и другие параметры трафика. Каждый *FEC* обрабатывается отдельно, что позволяет поддерживать требуемое *качество обслуживания* в сети *MPLS*.

Метод пересылки пакетов на основе пар "*FEC*-метка", принятый в *MPLS*, имеет ряд преимуществ перед методами, основанными на анализе заголовка блоков сетевого уровня. В частности, пересылку по методу *MPLS* могут выполнять маршрутизаторы, которые способны читать и заменять метки, но при этом либо вообще не способны анализировать заголовки блоков сетевого уровня, либо не способны делать это достаточно быстро.

Коммутируемый по меткам тракт LSP

Коммутируемый по меткам тракт – это последовательность *MPLS*-маршрутизаторов. Набор пакетов, передаваемый по LSP, относится к одному *FEC*, и каждый маршрутизатор LSR в LSP-туннеле назначает для него свою метку. LSP-туннель создается внутри LSP-тракта. Следует отметить, что зачастую начало и конец туннеля не совпадают с началом и концом LSP-тракта. Как правило, туннель короче. Для каждого туннеля подсчитывается число пропущенных пакетов и байт. Иногда поток данных может быть настолько велик, что для него создается несколько LSP-туннелей между отправителем и получателем. В одном LSP может быть создано несколько LSP-туннелей с различными точками приема и передачи, а в каждом туннеле могут быть созданы LSP-туннели другого уровня. В этом проявляется иерархичность структуры *MPLS*. Возможны два варианта создания туннелей: по принципу hop-by-hop, который предполагает, что каждый маршрутизатор самостоятельно выбирает дальнейший путь следования пакета, или по принципу явной маршрутизации, в котором маршрутизаторы передают пакет в соответствии с указаниями, полученными от верхнего в данном тракте LSR. Таким образом, в первом случае маршрут следования пакетов определяется случайным образом, а в случае явной маршрутизации он известен заранее. В сети *MPLS* может существовать набор маршрутизаторов, которые являются входными для конкретного *FEC*, тогда считается, что для этого *FEC* существует LSP-туннель с разными точками входа и выхода. Если для некоторых из этих LSP выходным является один и тот же LER, то можно говорить о дереве LSP, корнем которого служит данный выходной маршрутизатор. LSP можно рассматривать как тракт, создаваемый путем сцепления одного и более участков маршрута, который позволяет пересылать пакет, заменяя на каждом узле сети *MPLS* входящую метку исходящей меткой (так называемый алгоритм перестановки меток). Таким образом, тракт сети *MPLS* можно рассматривать как туннель, для создания которого в IP-пакет вставляется заголовок – метка, о котором речь шла ранее. LSP

устанавливаются либо перед передачей данных (с управлением от программы), либо при обнаружении определенного потока данных (управляемые данными LSP). На сегодняшний день применение туннелирования реализовано во многих технологиях. Образование в виртуальном тракте туннелей, по которым проходят другие виртуальные тракты, основывается на инкапсуляции передаваемых пакетов в пакеты, следующие по этому тракту к данному адресу назначения.

Основные понятия (таблица 9.1)

Таблица 9.1. Основные термины *MPLS*

Понятие	
FEC – Forwarding Equivalence Class – класс эквивалентности пересылки	Множество пакетов, которые пересылаются одинаково, например, с целью обеспечить заданное *QoS*
Label – метка	Короткий идентификатор фиксированной длины, определяющий принадлежность пакета тому или иному *FEC*
Label swapping – замена меток	Замена метки принятого узлом сети *MPLS* пакета новой меткой, связанной с тем же *FEC*, при пересылке этого пакета к нижестоящему узлу
LER – *MPLS* edge router – пограничный узел сети *MPLS*	Пограничный узел сети *MPLS*, который соединяет домен *MPLS* с узлом, находящимся вне этого домена
Loop detection - выявление закольцованных маршрутов	Метод выявления и устранения закольцованных маршрутов
Loop prevention – предотвращение образования закольцованных маршрутов	Метод, позволяющий обнаружить, что пакет прошел через узел более одного раза
LSP – Label Switched Path – коммутируемый по меткам тракт	Приходящий через один или более LSR тракт, по которому следуют пакеты одного и того же *FEC*
ER–LSP – explicitly routed LSP – LSP с явно заданным маршрутом	Тракт LSP, который организован способом, отличным от традиционной маршрутизации пакетов IP
LSR – label switching router – маршрутизатор коммутации по меткам	Маршутизатор, способный пересылать пакеты по технологии *MPLS*
MPLS domain – домен *MPLS*	Совокупность узлов *MPLS*, между которыми существуют непрерывные LSP
MPLS egress node – выходной узел сети *MPLS*	Последний *MPLS*-узел в LSP, направляющий исходный пакет к адресату, который находится вне *MPLS*-сети
MPLS ingress node	Первый *MPLS*-узел в LSP, принимающий исходный пакет и помещающий в него метку *MPLS*

Принцип работы

Рассмотренные более подробно опишем функционирование сети *MPLS*.

Любой IP-пакет на входе в сеть *MPLS*, независимо от того, поступает этот пакет от отправителя или же он пришел из смежной сети, которая может быть *MPLS*-сетью более высокого уровня, относится к определенному классу эквивалентной пересылки *FEC* (Forwarding Equivalence Class). Напомним, что анализ заголовка IP-пакета и назначение *FEC* производится только один раз на входе в сеть (рис. 9.2).

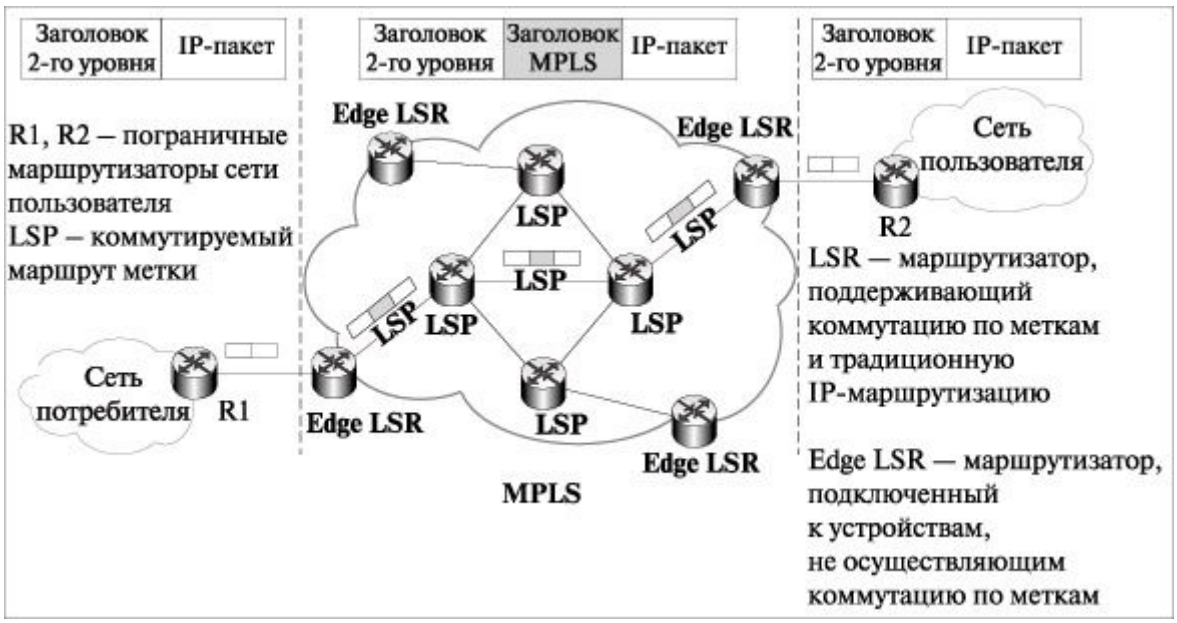


Рис. 9.2. Фрагмент MPLS-сети

Этап 1. Сеть автоматически формирует таблицы маршрутизации. В этом процессе участвуют маршрутизаторы или коммутаторы IP+ATM, установленные в сети сервис-провайдера. При этом применяются внутренние протоколы маршрутизации, такие как OSPF или IS-IS.

Этап 2. Протокол распределения меток (Label Distribution Protocol — LDP) использует отраженную в таблицах топологию маршрутизации для определения значений меток, указывающих на соседние устройства. В результате этой операции формируются маршруты с коммутацией по меткам (Label Switched Paths – LSP).Автоматическое присвоение меток *MPLS* выгодно отличает эту технологию от технологии частных виртуальных каналов ATM PVC, требующих ручного присвоения VCI/VPI.

Этап 3. Входящий пакет поступает на пограничный Label Switch Router (LSR), который определяет, какие услуги 3-го уровня необходимы этому пакету (например *QoS* или управление полосой пропускания). На основе учета всех требований маршрутизации и правил высокого уровня (policies), пограничный LSR выбирает и присваивает метку, которая записывается в заголовок пакета, после чего пакет передается дальше.

Этап 4. Устройство LSR, находящееся в опорной сети, считывает метки каждого пакета, заменяет старые метки новыми (новые метки определяются по локальной таблице) и передает пакет дальше. Эта операция повторяется в каждой точке передачи пакета по опорной сети.

Этап 5. На выходе пакет попадает в пограничный LSR, который удаляет метку, считывает заголовок пакета и передает его по месту назначения. В магистральных LSR метка *MPLS* сравнивается с заранее рассчитанными таблицами коммутации и содержит информацию 3-го уровня. Это позволяет каждому устройству LSR автоматически оказывать каждому пакету необходимые IP-услуги. Таблицы рассчитываются заранее, что снимает необходимость повторной обработки пакетов в каждой точке передачи. Такая схема не только позволяет разделить разные типы трафика (например, отделить неприоритетный трафик от критически важного); она делает решения *MPLS* хорошо масштабируемыми. Поскольку для присвоения меток технология *MPLS* использует разные наборы правил (policy mechanisms), она отделяет передачу пакетов от содержания

заголовков IP. Метки имеют только локальное значение и многократно переиспользуются в крупных сетях, поэтому исчерпать запас меток практически невозможно. В рамках предоставления корпоративных IP-услуг самое главное преимущество *MPLS* заключается в способности присваивать метки, имеющие специальное значение. Наборы меток определяют не только место назначения, но и тип приложения и класс обслуживания.

Лекция 10. Метки и механизмы MPLS

Метка

Метка представляет собой последовательность записей. Каждая запись в стек имеет длину 4 октета. Формат такой записи показан на рис. 10.1.

Запись меток размещается после заголовка канального уровня, и перед заголовком сетевого уровня (например между Ethernet- и IP-заголовком). Верх стека записывается первым, а дно – последним. Сетевой заголовок следует сразу за записью стека меток с битом S=1 . Каждая запись стека меток содержит в себе следующие поля.

1. **Дно стека (S)**

Является средством поддержки иерархической структуры стека меток *MPLS*. В заголовке последней (т. е. самой глубокой или нижней) метки бит S=1, а во всех остальных метках в стеке бит S=0. Подробнее стек меток рассматривается ниже.

2. **Время жизни (TTL)**

Это 8-битовое поле служит для представления значения времени жизни пакета. Данное поле является механизмом, предотвращающим возможность бесконечной циркуляции пакетов по сети вследствие образования закольцованных маршрутов. Байт TTL находится в конце заголовка метки.

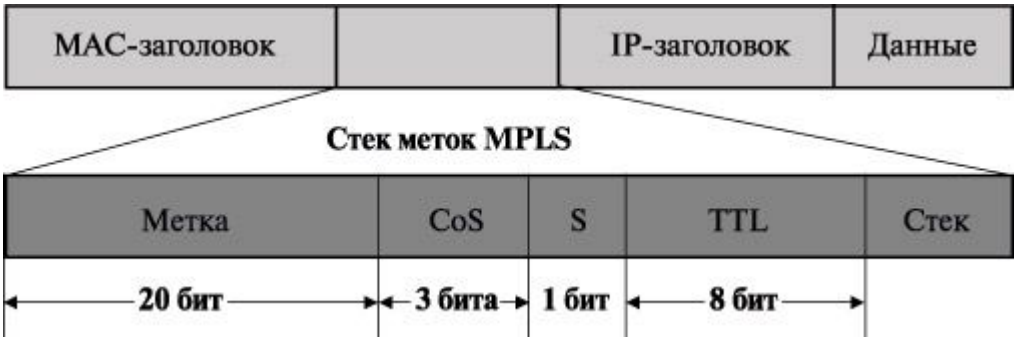


Рис. 10.1. Формат записи стека меток

3. **Экспериментальное поле (CoS)**

Это 3-битовое поле зарезервировано для экспериментальных целей (*QoS*). В настоящее время проводится работа на создание согласованного стандарта использования этих битов для поддержки дифференцированного обслуживания разнотипного трафика и идентификации класса обслуживания. Первоначально это поле так и называлось – "Класс обслуживания" (CoS), и это название до сих пор широко распространено. При предоставлении дифференцированных услуг MPSL-сети это поле может указывать определенный класс обслуживания, например аналогичный классам DiffServ.

4. **Значение метки**

Это 20-битовое поле несет в себе код метки. Может быть любым числом в диапазоне от 0 до 220- 1, за исключением резервных значений (0, 1, 2, 3 и др.), определением использования которых занимается рабочая группа *MPLS* в составе комитета IETF.

Когда получен помеченный пакет, анализируется значение метки наверху стека. В результате этого анализа определяется:

- следующий шаг, куда должен быть переадресован пакет;
- операция, которая должна быть выполнена со стеком меток до переадресации. Эта операция может быть заменой метки на вершине стека, или удалением записи из стека, или замещением верхней позиции в стеке и занесением туда затем одной или более новых записей.

В дополнение к определению следующего шага и операции со стеком меток можно также получить данные об инкапсуляции выходной информации и возможно другие данные, которые необходимы для того, чтобы корректно переадресовывать пакеты.

Существует несколько зарезервированных значений меток.

Значение 0 представляет "IPv4 Explicit NULL Label". Это значение метки является единственно допустимым для дна стека меток. Оно указывает, что стек должен быть очищен и переадресация пакета должна основываться на IPv4-заголовке.

Значение 1 представляет "Router Alert Label". Это значение метки является легальным в любом месте стека меток, за исключением дна. Когда полученный пакет содержит такую метку на вершине стека, он доставляется локальному модулю для обработки. Действительная переадресация пакета определяется меткой в его стеке. Однако если пакет переадресовывается дальше, еще до переадресации в стек должна быть занесена метка "Router Alert". Использование этой метки сходно с применением опции "Router Alert" в IP-пакетах. Так как эта метка не может лежать на дне стека, она не ассоциируется с определенным протоколом сетевого уровня.

Значение 2 представляет "IPv6 Explicit NULL Label". Это значение метки является единственно допустимым для записи на дне стека. Оно указывает, что стек должен быть очищен, а переадресация пакетов должна после этого основываться на заголовке IPv6.

Значение 3 представляет "Implicit NULL Label". Это метка, которую LSR может присваивать и рассылать, но которая в действительности никогда не используется при инкапсуляции. Когда LSR замещает метку на верху стека на новую и эта новая метка является "Implicit NULL", LSR очистит стек, вместо того чтобы осуществить замену. Хотя это значение не может появиться при инкапсуляции, оно должно быть специфицировано в протоколе рассылки меток, так что значение может считаться зарезервированным.

Значения 4–15 зарезервированы.

Стек меток MPLS

Спецификация кодирования стека меток *MPLS* определена в RFC3032 "*MPLS* Label Stack Encoding". Данный документ содержит детальную информацию о метках и о том, как они используются с различными сетевыми технологиями, а также определяет ключевое для технологии *MPLS* понятие – *стек меток*. Возможность иметь в пакете более

одной метки в виде стека позволяет создавать иерархию меток, что открывает дорогу многим приложениям.

MPLS может выполнить со стеком следующие операции: помещать метку в стек, удалять метку из стека и заменять метку. Эти операции могут использоваться для слияния и разветвления информационных потоков. Операция помещения метки в стек (push operation) добавляет новую метку поверх стека, а операция удаления метки из стека (pop operation) удаляет верхнюю метку стека.

Функциональные возможности стека *MPLS* позволяют объединять несколько LSP в один. К стеку меток каждого из этих LSP сверху добавляется общая метка, в результате чего образуется агрегированный тракт *MPLS*. В точке окончания такого тракта происходит его разветвление на составляющие его индивидуальные LSP. Так могут объединиться тракты, имеющие общую часть маршрута. Следовательно, *MPLS* способна обеспечивать иерархическую пересылку, что может стать важной и востребованной функциональной возможностью. При ее использовании не нужно переносить глобальную маршрутную информацию, и это делает сеть *MPLS* более стабильной и масштабируемой, чем сеть с традиционной маршрутизацией.

Согласно рассматриваемым ниже правилам инкапсуляции меток, за меткой *MPLS* в пакете всегда должен следовать заголовок сетевого уровня. Так как *MPLS* начинает работу верхнего уровня стека, этот стек используется по принципу LIFO "последним пришел, первым ушел".

Пример четырехуровневого стека меток представлен на рис. 10.2.

Заголовок *MPLS* № 1 был первым заголовком *MPLS*, помещенным в пакет, затем в него были помещены заголовки № 2, № 3 и, наконец, заголовок № 4. Коммутация по меткам всегда использует верхнюю метку стека, и метки удаляются из пакета так, как это определено выходным узлом для каждого LSP, по которому следует пакет. Рассмотренный в предыдущем параграфе бит S имеет значение 1 в нижней метке стека и 0 – во всех остальных метках. Это позволяет привязывать префикс к нескольким меткам, другими словами – к стеку меток (Label Stack). Каждая метка стека имеет собственные значения поля EXP, S-бита и поля TTL.

Рис. 10.2. Четырехуровневый стек меток

Инкапсуляция меток

При использовании протоколов коммутации на уровне звена данных, таких как ATM и Frame Relay, верхняя *MPLS*-метка вписывается в поле идентификаторов этих протоколов. Далее будет показано, как при применении ATM для размещения *MPLS*-метки используется поле VPI/VCI, а при применении Frame Relay – поле DLCI (Data LinkConnection Identifier). В тех случаях, когда *MPLS* обеспечивает пересылку IP-пакетов сетевого уровня и когда технология уровня звена данных не поддерживает собственное поле меток, *MPLS*-заголовок должен инкапсулироваться между заголовками уровня звена данных и сетевого уровня.

Механизм инкапсуляции переносит один или более протоколов верхних уровней внутри полезной нагрузки дейтаграммы инкапсулирующего протокола. В сущности, вводится новый заголовок, который делает из инкапсулированного заголовка и поля данных новое поле данных. Общая модель инкапсуляции представлена на рис. 10.3, где подразумевается, что инкапсуляция *MPLS* может быть использована с любой технологией уровня 2. Метка *MPLS* может быть помещена в существующий формат заголовка уровня 2, как в случае ATM или FR, или вписана в специальный заголовок *MPLS*, как в случае Ethernet или PPP. Во всех случаях любые дополнительные метки находятся между верхней меткой стека и IP-заголовком уровня 3.

Показанный на рис 10.3 заголовок *MPLS* часто называют shim header ("заголовком — клином"), подчеркивая в метафорической форме тот факт, что этот заголовок "уровня 2.5" вклинивается в пакет между заголовками уровня данных и сетевого уровня.

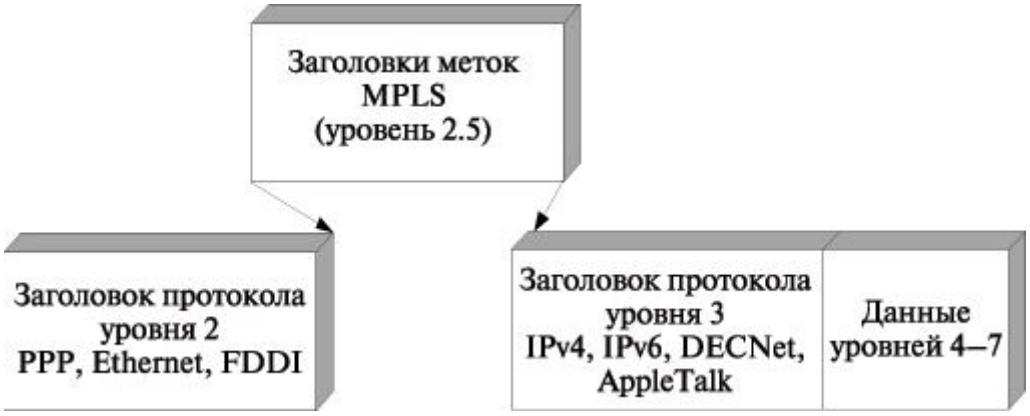


Рис. 10.3. Принцип инкапсуляции заголовка MPLS

Одной из самых сильных сторон технологии *MPLS* (и потому отраженной в ее названии) является то, что она может использоваться совместно с различными протоколами уровня 2. Среди этих протоколов – ATM, Frame Relay, PPP и Ethernet, FDDI и другие, предусмотренные документами по *MPLS*.

Покажем, как метка может вписываться в заголовок уровня звена данных (VCI/VPI для сети ATM, DLCI для сети Frame Relay и т.п.) или "вставляться" между заголовками уровня звена данных и сетевого уровня. С самого начала рабочая группа IETF *MPLS* решила, что во всех случаях, когда это возможно, *MPLS* должна использовать имеющиеся форматы. По этой причине информация метки *MPLS* может передаваться в пакете несколькими разными методами:

- как часть заголовка второго уровня ATM, когда информация метки передается в идентификаторах виртуального канала VCI и виртуального тракта VPI, что показано на рис. 10.4;
- как часть кадра AAL5 уровня адаптации ATM (ATM Adaptation Layer 5) перед сегментацией и сборкой SAR (Segmentation and Reassembly), что выполняется в ATM-окружении в случае, когда эта информация содержит данные о стеке меток (несколько полей *MPLS*-меток);
- как часть заголовка второго уровня Frame Relay, когда информация метки передается в идентификаторах DLCI, что изображено на рис. 10.5;
- как новая 4-байтовая метка, называемая клином или прокладкой (shim), которая вставляется между заголовками второго и третьего уровней, что показано на рис. 10.5, – во всех остальных случаях.

Размещение метки *MPLS* в заголовке ATM представлено на рис. 10.4.

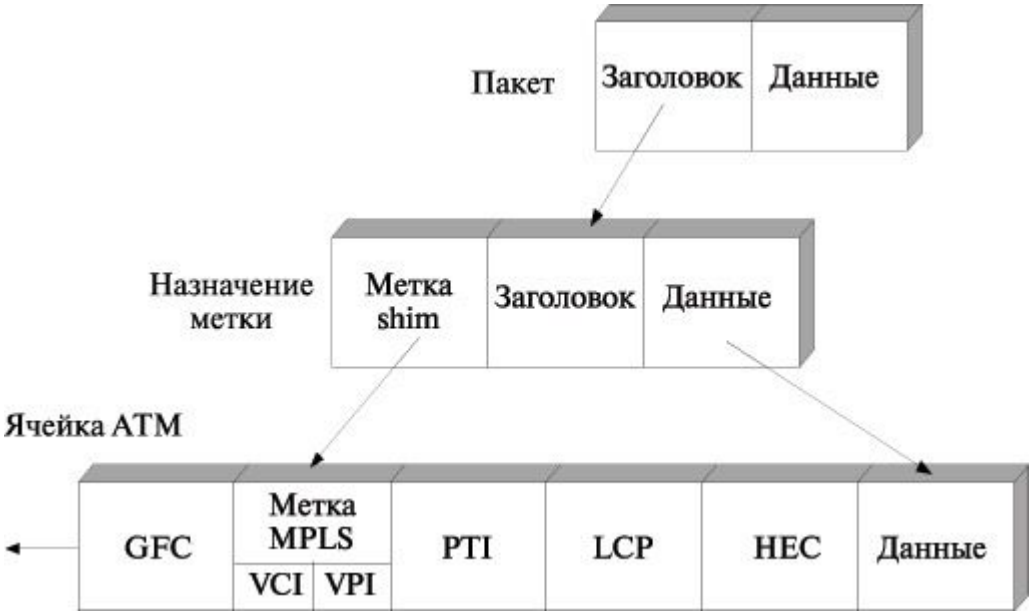


Рис. 10.4. MPLS-метка, передаваемая в полях VPI/VCI заголовка ATM

Использование *MPLS* поверх ATM сейчас довольно распространено, особенно для транспортировки по сетям ATM трафика IP. ATM-коммутаторы, которые конфигурированы для поддержки *MPLS* (ATM-LSR), выполняют протоколы маршрутизации TCP/IP и используют пересылку данных в ATM фиксированной длины 53 байта. Внутри этих ATM-LSR верхняя метка *MPLS* помещается в поля VCI/VPI заголовка ячейки ATM, а данные о стеке меток *MPLS* — в поле данных ячеек ATM.

MPLS в сетях Frame Relay была развернута рядом крупных поставщиков услуг и до сих пор широко используется. Подобно ATM, FR-коммутаторы, поддерживающие *MPLS*, применяют протоколы маршрутизации TCP/IP для пересылки данных под управлением FR. При использовании FR текущая метка помещается в поле идентификатора канала звена данных DLCI в заголовке FR. Любые дополнительные записи в стек меток *MPLS* переносятся после заголовка FR, но до заголовка сетевого уровня, содержащегося в поле данных кадра FR. Стандарт *MPLS* позволяет FR использовать адрес Q.922 длиной либо 2 октета, либо 4 октета. Формат представлен на рис. 10.5.

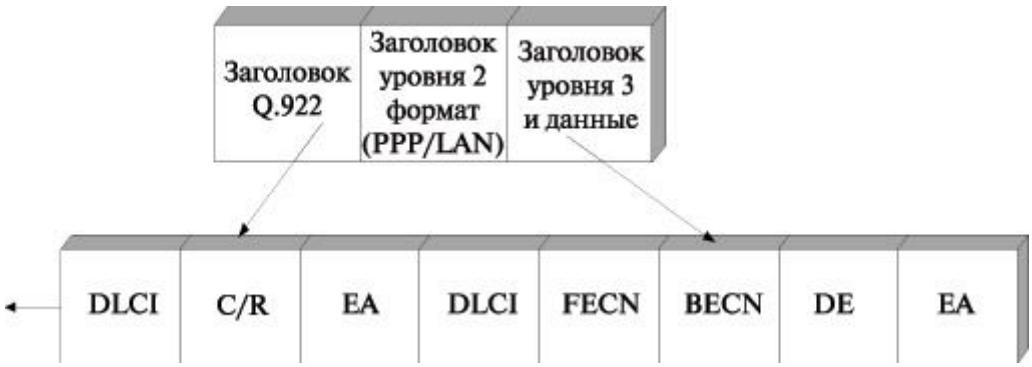


Рис. 10.5. Размещение метки MPLS в кадре FR
Примечание. Длина поля DLCI может составлять 10, 17 или 23 бита

В отношении ячеек ATM и кадров Frame Relay договорились использовать для *MPLS* имеющиеся форматы заголовков, а во всех остальных случаях – собственную метку *MPLS*, "прокладку" между заголовками второго и третьего уровней. Отсюда видно, что *MPLS* позволяет создавать новые форматы меток без изменения протоколов маршрутизации, а потому распространение этой технологии на вновь появляющиеся виды оптического транспорта, такие как плотное мультиплексирование с разделением по длине волны DWDM (Dense Wave Division Multiplexing) и оптическая коммутация, представляет собой относительно простую задачу.

Принцип, представленный на рис. 10.3, подходит для каналов типа "точка-точка" (Point-to-Point – PPP) и для локальных сетей Ethernet (всех типов). Подобным методом можно передать одну *MPLS*-метку или стек меток.

Протокол PPP фактически представляет собой семейство родственных протоколов IETF, используемое для передачи многопротокольных дейтаграмм по двухточечным каналам связи. PPP определяет метод инкапсуляции дейтаграмм разных протоколов сетевого уровня, протокола управления звеном данных LCP и набора протоколов управления сетью NCP. Для использования *MPLSCP* с управлением коммутацией по меткам через звено PPP был определен специальный протокол, который управляет передачей пакетов *MPLS* по каналу PPP. Этот протокол обозначается аббревиатурой *MPLS*CP. Формат показан на рис. 10.6.

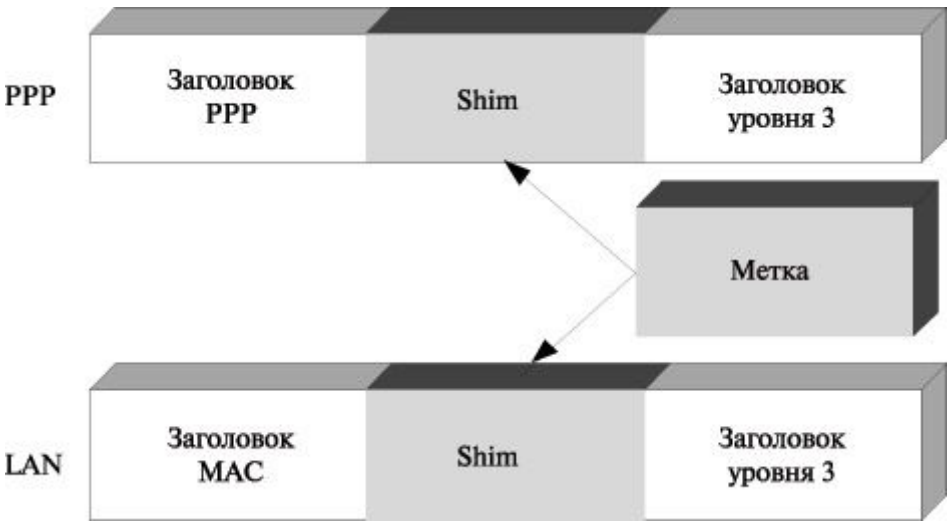


Рис. 10.6. Формат для введения MPLS-метки в пакет PPP и в кадр Ethernet

Когда пакеты *MPLS* передаются по Ethernet, в каждом кадре Ethernet переносится только один снабженный меткой пакет. Метка помещается между заголовком уровня звена данных и заголовком сетевого уровня. Использование *MPLS* в сетях Ethernet, особенно в городских сетях, является еще одной перспективной возможностью *MPLS*. В стандарт Ethernet вносятся изменения, позволяющие увеличить скорость и дальность передачи Ethernet-пакетов. В настоящее время начинают применяться Ethernet-интерфейсы на скоростях 10 Гбит/с, а в скором времени появятся Ethernet-интерфейсы и на еще больших скоростях.

К сожалению, добавление *MPLS*-метки или стека меток к 1492-байтовому пакету может привести к необходимости его фрагментации. При передаче пакетов MTU-размера (Maximum Transmission Unit – максимально возможный размер передаваемого блока данных) с *MPLS*-меткой протокол управления передачей TCP определяет, что в *MPLS*-сети нужно произвести фрагментацию. Однако следует отметить, что многие Ethernet-каналы поддерживают передачу 1500-байтовых или 1508-байтовых пакетов. Более того, в большинстве сетей пакеты с метками обычно передаются по ATM- или PPP-каналам, а не по сегментам локальных сетей.

Итак, метка может быть помещена в пакет разными способами – вписывается в специальный заголовок, помещаемый либо между заголовками уровня 2 и уровня 3, либо в свободное и доступное поле заголовка одного из этих двух уровней, если, конечно, таковое имеется. Очевидно, что вопрос о том, куда следует помещать заголовок, содержащий метку, должен согласовываться между объектами, ее использующими.

Таблицы пересылки

Ранее отмечалось, что когда пакет *MPLS* попадает в маршрутизатор коммутации по меткам LSR, этот маршрутизатор просматривает имеющуюся у него таблицу с так называемой информационной базой меток LIB (Label Information Base) для того, чтобы принять решение о дальнейшей обработке пакета. Эту информационную базу иногда называют также **Next Hop Label Forwarding Entry (NHLFE)**, и, согласно RFC 3031, в нее обычно входит следующая информация:

- операция, которую надо произвести со стеком меток пакета (заменить верхнюю метку стека, удалить верхнюю метку, поместить поверх стека новую метку);
- следующий маршрутизатор в LSP, причем "следующим" может быть тот же самый LSR;
- используемая при передаче пакета инкапсуляция на уровне звена данных;
- способ кодирования стека меток при передаче пакета;
- другая информация, относящаяся к пересылке пакета.

Содержащая эту информацию таблица пересылки, которую ведет каждый LSR, как, впрочем, и любые другие таблицы, представляет собой последовательность записей. Каждая запись таблицы пересылки LSR состоит из входящей метки и одной или более подзаписей, причем каждая подзапись содержит значение исходящей метки, идентификатор выходного интерфейса и адрес следующего маршрутизатора в LSP. Пример простой таблицы пересылки LIB представлен в таблице 10.1.

Таблица 10.1. Таблица пересылки LIB		
Входящая метка	**Первая подзапись**	**Вторая подзапись**
Значение входящей метки	Исходящая метка	Исходящая метка
	Выходной интерфейс	Выходной интерфейс
	Адрес следующего LSR	Адрес следующего LSR

Разные подзаписи внутри одной записи могут иметь либо одинаковые, либо разные значения исходящих меток. Более одной подзаписи бывает нужно для поддержки многоадресной рассылки пакета, когда пакет, который поступил к одному входящему интерфейсу, должен затем рассылаться через несколько исходящих интерфейсов. Обращение к таблице записей производится по значению входящей метки, т.е. по входящей метке к происходит обращение к к-й записи в таблице.

Запись в таблице может также содержать информацию, указывающую, какие ресурсы имеет возможность использовать пакет, например, определенную выходную очередь.

LSR может поддерживать либо одну общую таблицу, либо отдельные таблицы для каждого из своих интерфейсов. В первом варианте обработка пакета определяется исключительно меткой, переносимой в пакете. Во втором варианте обработка пакета определяется не только меткой, но и интерфейсом, к которому поступил пакет. LSR может использовать либо первый вариант, либо второй, либо их сочетание.

Привязка "метка-FEC"

Каждая запись в таблице пересылки, которую ведет LSR, содержит одну входящую метку и одну или более исходящих меток. В соответствии с этими двумя типами меток обеспечивается два типа привязки меток к *FEC*:

- первый тип – метка для привязки выбирается и назначается в LSR локально. Такая привязка называется локальной;
- второй тип – LSR получает от некоторого другого LSR информацию о привязке метки, которая соответствует привязке, созданной на этом другом LSR. Такая привязка называется удаленной.

Средства управления коммутацией по меткам используют для заполнения таблиц пересылки как локальную, так и удаленную привязку меток к *FEC*. Это может делаться в двух вариантах: upstream и downstream. Первый: когда метки на локальной привязке используются как входящие метки, а метки из удаленной привязки — как исходящие. Второй вариант – прямо противоположный, т.е. метки из локальной привязки используются как исходящие метки, а метки из удаленной привязки – как входящие. Рассмотрим каждый из этих вариантов.

Первый вариант называется привязкой метки к *FEC "снизу"* (downstream label binding), потому что в этом случае привязка переносимой пакетом метки к тому *FEC*, которому принадлежит этот пакет, создается нижестоящим LSR, т.е. LSR, расположенным ближе к адресату пакета, чем LSR, который помещает метку в пакет. При привязке "снизу" пакеты, которые переносят определенную метку, передаются в направлении, противоположном направлению передачи информации о привязке этой метки к *FEC*.

Второй вариант называется привязкой метки к *FEC "сверху"* (upstream label binding), потому что в этом случае привязка переносимой пакетом метки к тому *FEC*, которому принадлежит этот пакет, создается тем же LSR, который помещает метку в пакет; т.е. создатель привязки расположен "выше" (ближе к отправителю пакета), чем LSR, к которому пересылается этот пакет. При привязке "сверху" пакеты, которые переносят определенную метку, передаются в том же направлении, что и информация о привязке этой метки к *FEC*.

LSR обслуживает также пул "свободных" меток (т.е. меток без привязки). При начальной установке LSR пул содержит все метки, которые может использовать LSR для их локальной привязки к *FEC*. Именно емкость этого пула и определяет, в конечном счете, сколько пар "метка-*FEC*" может одновременно поддерживать LSR. Когда маршрутизатор создает новую локальную привязку, он берет метку из пула; когда маршрутизатор уничтожает ранее созданную привязку, он возвращает метку, связанную с этой привязкой, обратно в пул.

Вспомним, что LSR может вести либо одну общую таблицу пересылки, либо несколько таблиц – по одной на каждый интерфейс. Когда маршрутизатор ведет общую таблицу пересылки, он имеет один пул меток. Когда LSR ведет несколько таблиц, он имеет отдельный пул меток для каждого интерфейса.

LSR создает или уничтожает привязку метки к *FEC* вследствие определенного события. Такое событие может инициироваться либо пакетами данных, которые должны пересылаться маршрутизатором LSR, либо управляющей (маршрутной) информацией, которая должна обрабатываться LSR. Когда создание или уничтожение привязки инициируется пакетами данных, эта привязка называется *привязкой под воздействием данных (data-driven)*. Когда создание или уничтожение привязки инициируется управляющей информацией, данная привязка называется *привязкой под воздействием управляющей информации (control-driven)*.

Привязка под воздействием данных предполагает, что LSR поддерживает как функции пересылки при коммутации по меткам, так и функции пересылки при традиционной маршрутизации. Поддержка функций пересылки при традиционной маршрутизации необходима потому, что привязка метки представляет собой эффект, сопутствующий традиционной маршрутизации пакета.

Важной проблемой качества функционирования, возникающей при использовании схем привязки под воздействием данных (и, в меньшей степени, – схем привязки под воздействием управляющей информации), является производительность. Каждый раз, когда LSR решает, что поток должен коммутироваться по меткам, ему необходимо обмениваться информацией о привязке меток со смежными LSR, и ему может также потребоваться внести некоторые изменения в привязке меток к *FEC*. Все эти процедуры требуют передачи трафика, управляющего раздачей информации о привязке, и, следовательно, потребляют ресурсы средств управления коммутацией по меткам. Более того, эти процедуры потребляют тем больше ресурсов средств управления, чем больше доля потоков, выбранных для коммутации по меткам. Трудно количественно оценить, насколько дорогой является процедура назначения и распределения меток, но не подлежит сомнению, что производительность схем, работающих под воздействием данных, чувствительна к этому фактору. Если LSR не может назначать и распределять метки со скоростью, требуемой алгоритмом обнаружения потоков, то коммутироваться по меткам будет меньший процент потоков, и от этого будет страдать общая производительность.

В меньшей степени это относится к схемам, работающим под воздействием управляющей информации. Пока топология остается стабильной, весь трафик, который поступает в непограничный маршрутизатор LSR, может коммутироваться по меткам без обработки пакетов управляющим процессором. Схемы, работающие под воздействием управляющей информации, могли получить информацию о привязке маршрутов от соседних LSR, которые не являлись следующими участками этих маршрутов. Когда топология изменится так, что эти "соседи" станут следующими участками маршрутов, коммутация по меткам будет продолжаться без прерывания. Но на производительность схем, работающих под воздействием данных, изменение топологии влияет. Если изменяется маршрут прохождения потока, новые LSR на этом маршруте воспринимают это так, как если бы был создан новый поток. Любой такой новый поток должен вначале пересылаться традиционно. Таким образом, изменение топологии может налагать очень тяжелое бремя на LSR, который только что стал новым следующим маршрутизатором для некоторого другого LSR. Во-первых, он внезапно получает большое число потоков, которые ранее шли по другому маршруту. Кроме того, не прекращается поступление новых потоков от вновь запущенных приложений. Все эти потоки должны пересылаться и анализироваться алгоритмами обнаружения потоков. Это в свою очередь создает дополнительную нагрузку как на средства пересылки при традиционной маршрутизации, так и на средства управления коммутацией по меткам. Во время таких переходных процессов производительность средств пересылки LSR может приблизиться к производительности его средств пересылки при традиционной маршрутизации, т.е. стать примерно на порядок ниже, чем максимальная производительность LSR.

Режимы операций с метками

Рассмотрим режимы трех базовых операций, которые представляют, по сути, основные принципы механизма коммутации по меткам: назначение меток, распределение меток и сохранение меток.

Назначение меток. Когда *FEC* создается путем анализа адресных префиксов, которые распределяются протоколом внутренней маршрутизации и используются для создания трактов LSP по участкам, возможны два режима назначения меток:

- независимое назначение (т.е. независимое создание трактов LSP);
- упорядоченное назначение (т.е. упорядоченное создание трактов LSP).

Независимое назначение. При таком назначении меток каждый LSR сам, независимо от других событий, принимает решение о привязке метки к обнаруженному *FEC* и об уведомлении вышестоящего LSR об этой привязке. Такая ситуация аналогична традиционной маршрутизации, выполняемой в обычных IP-сетях, когда обнаруживаются новые маршруты.

Если LSR настроен на режим независимого назначения меток, то сообщение Label Mapping протокола LDP передается этим LSR при возникновении любой из следующих ситуаций:

- LSR распознает новый *FEC* с помощью таблицы пересылки и назначает метку снизу по собственной инициативе;

- LSR получает от вышестоящего маршрутизатора сообщение Label Request для *FEC*, присутствующего в его таблице пересылки;
- следующий маршрутизатор для *FEC* заменяется другим одноранговым узлом LDP-сеанса, и при этом активизирован механизм выявления закольцованных маршрутов;
- изменяются атрибуты привязки "метка-*FEC*";
- информация о привязке метки получена от нижестоящего маршрутизатора в ситуации, когда не было создано никакой привязки сверху, или активизирован механизм обнаружения закольцованных маршрутов, или изменились атрибуты привязки "метка-FEC".

Упорядоченное назначение. Этот способ назначения меток имеет больше ограничений, чем предыдущий, в том смысле, что привязка метки к определенному *FEC* происходит только тогда, когда LSR либо выступает в роли выходного узла для этого *FEC*, либо уже получил информацию о привязке "метка-FEC" от нижестоящего маршрутизатора.

Если LSR использует режим упорядоченного назначения меток, то сообщение Label Mapping передается нижестоящими LSR при возникновении любой из следующих ситуаций:

- LSR распознает новый *FEC* с помощью таблицы пересылки и является для этого *FEC* выходным маршрутизатором;
- LSR получает от вышестоящего маршрутизатора сообщение Label Request для *FEC*, присутствующего в его таблице пересылки, и либо является выходным маршрутизатором для этого *FEC*, либо имеет привязку к нему метки, назначенную снизу;
- следующий маршрутизатор для *FEC* заменяется другим одноранговым узлом LDP-сеанса и при этом активизирован механизм выявления закольцованных маршрутов;
- изменяются атрибуты привязки "метка-*FEC*";
- информация о привязке метки получена от нижестоящего маршрутизатора в ситуации, когда не было создано никакой привязки сверху, или активизирован механизм обнаружения закольцованных маршрутов, или изменились атрибуты привязки "метка-*FEC*".

Режимы сохранения меток. Еще одной характеристикой использования меток является режим их сохранения. Когда вышестоящий LSR получает метку от нижестоящего LSR, который в данный момент не является для него смежным с точки зрения данного *FEC*, он должен принять относительно этой метки решение: либо использовать ее (т.е. "сохранить" у себя ее привязку к *FEC*), либо отбросить.

В *MPLS* используются два основных режима сохранения меток:

- либеральный режим,
- консервативный режим.

При либеральном режиме вышестоящий LSR сохраняет у себя любую привязку к *FEC* меток, которые он получил от несмежных нижестоящих LSR (т.е. метки пришли к нему транзитом).

При консервативном режиме вышестоящий LSR отказывается от таких меток, т.е. отбрасывает их.

Преимуществом либерального режима является то, что если нижестоящий LSR станет с точки зрения данного *FEC* смежным маршрутизатором, изменять привязку "метка-*FEC*" не понадобится. Это позволяет намного быстрее реагировать на изменения маршрутов. Конечно, если привязка метки к *FEC* уже была отброшена, то ее придется назначить повторно до того, как можно будет использовать LSR.

При консервативном режиме требуется меньше ресурсов, но реакция на изменения в следующих участках маршрута происходит намного медленнее.

Распределение меток. В технологии *MPLS* могут использоваться два режима распределения меток: нижестоящим LSR по запросу вышестоящего или нижестоящим LSR по собственной инициативе.

Режим распределения нижестоящим по запросу вышестоящего используется для создания трактов LSP по участкам. Он позволяет вышестоящему LSR в явном виде запрашивать привязку метки к определенному *FEC* у соседнего с ним нижестоящего LSR.

Режим распределения меток нижестоящим по собственной инициативе используется тогда, когда нижестоящему LSR нужно "раздать" метки вышестоящим, хотя те не передавали запроса в явном виде.

Архитектура *MPLS* не предполагает применения какого-то единственного протокола распределения меток. В одной и той же сети *MPLS* могут использоваться:

- специальный протокол распределения меток Label Distribution Protocol (LDP);
- протокол сигнализации RSVP;
- расширения возможностей протоколов маршрутизации, например протокола междоменовой маршрутизации Border Gateway Protocol (BGP).

Лекция 11. Протоколы распределения меток

Протокол LDP

Классы эквивалентности пересылки и LDP

Понятие *класс эквивалентности пересылки FEC* уже обсуждалось в предыдущих лекциях. Там же говорилось о том, что для переноса через сеть *MPLS* пакетов, принадлежащих разным *FEC*, в сети создаются *виртуальные тракты LSP*, и было показано, как с помощью метки *MPLS* устанавливается соответствие "пакет-*FEC*", определяющее, по какому LSP должен быть направлен пакет с этой меткой. В этой лекции речь пойдет о том, каким образом производится *распределение меток* по всем LSR сети *MPLS* с использованием протокола *LDP (Label Distribution Protocol)*.

В спецификации *LDP* к настоящему моменту установлены два типа элементов, с помощью которых может определяться *FEC*:

- *Address Prefix* – адресный префикс любой длины от нуля до полного адреса;
- *Host Address* – полный адрес хоста.

Решения о назначении меток могут основываться на критериях пересылки, таких как:

- одноадресная маршрутизация к получателю;
- оптимизация распределения трафика в сети;
- многоадресная рассылка;
- виртуальная частная сеть VPN;
- механизмы обеспечения *качества обслуживания QoS* и др.

Спецификация же протокола *LDP* определяет правила, по которым устанавливается соответствие между входным пакетом и его LSR.

Для *распределения меток* могут использоваться *разные методы*:

- метод на основе топологии (topology-based method); использует стандартную обработку протоколов маршрутизации (например OSPF и BGP, рассматриваемых ниже);
- метод на основе запросов (request-based method); использует обработку управляющего протокола на основе запросов (например, протокола RSVP);
- метод на основе трафика (traffic-based method); запускает процедуру присвоения и *распределения меток* при получении пакета.

Во всех этих случаях архитектурой *MPLS* предусматривается, что назначение метки, то есть ее привязку к определенному *FEC*, производит LSR, который является выходным пограничным маршрутизатором для пакетов этого *FEC* (рис. 11.1).

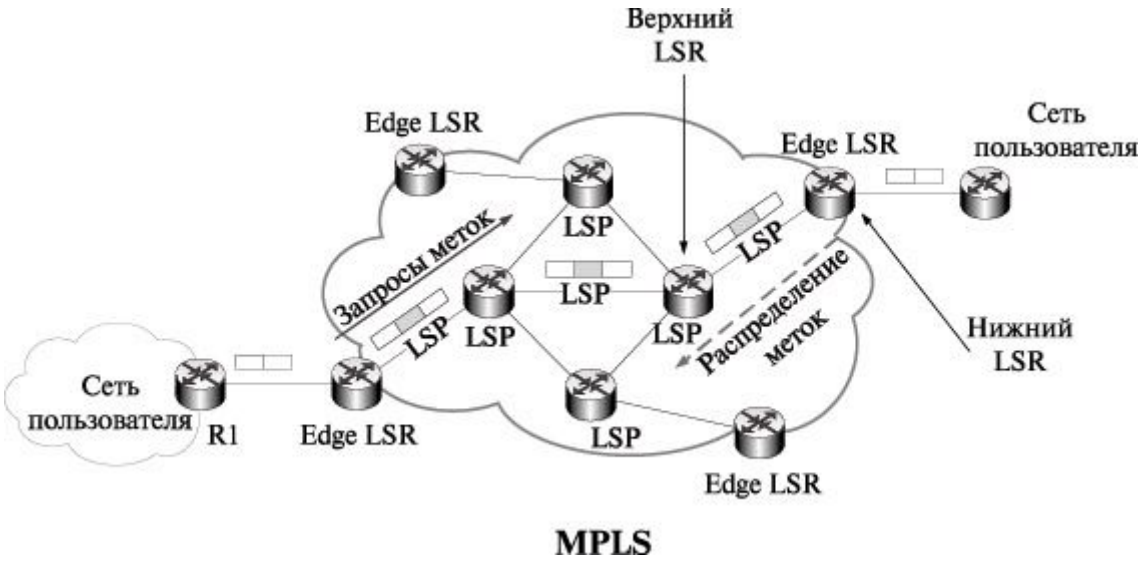


Рис. 11.1. Фрагмент MPLS-сети

Таким образом, назначение меток всегда производится снизу, то есть в сторону, противоположную направлению трафика. Нижний LSR информирует соседние верхние LSR о том, какие метки он привязал к каждому *FEC* поступающих к нему пакетов. Этот процесс и называется ***распределением меток***, а обеспечивает его протокол *распределения меток*.

Архитектура *MPLS* не требует обязательного применения *LDP*. Для *распределения меток* могут применяться модификации существующих протоколов маршрутизации, позволяющие использовать их для передачи информации о метках, например рассматриваемый протокол BGP, RSVP, который рассматривается ниже, также имеет расширения, обеспечивающие поддержку обмена метками с уведомлением.

Но все же протокол *распределения меток LDP* был признан комитетом IETF наиболее удачным и, что еще важнее, хорошо специфицирован им. Кроме того, определено расширение базового протокола *LDP* для поддержки явной маршрутизации с учетом обеспечения *качества обслуживанияя QoS* и управления трафиком TE – протокол *LDP* с учетом ограничивающих условий *CR-LDP(Constraint-Based LDP)*. Ко всему прочему *LDP* устанавливает надежные транспортные соединения со смежными маршрутизаторами LSR по протоколу TCP, причем в случае, если между двумя LSR надо одновременно установить несколько *LDP*-сеансов, используется единственное TCP-соединение.

Имеются следующие схемы обмена метками:

- *LDP* преобразует в метки IP-адреса получателя при одноадресной передаче;
- RSVP и *CR-LDP* используются для оптимизации распределения трафика в сети и для резервирования ресурсов;
- BGP работает с внешними метками VPN.

Основы протокола LDP

В связи с тем, что протокол *LDP* тесно взаимодействует с протоколами внутренней маршрутизации IPG, его часто называют протоколом пересылки по участкам.

Протокол распределения меток LDP представляет собой набор процедур и сообщений, при помощи которых LSR организует тракты коммутации по меткам, обмениваясь информацией о привязке меток в *FEC* с "соседними" LSR, поддерживает и прекращает LSP-сеансы (двусторонний диалог взаимодействующих LSR, являющихся в данном контексте одноранговыми узлами *LDP*, в ходе которого каждый из взаимодействующих LSR получает сведения о привязке меток к *FEC* в другом LSR).

Также в протоколе определен механизм передачи уведомлений и обнаружения в LSP закольцованных маршрутов, уже обсуждавшийся ранее.

Процедуры протокола *LDP* позволяют LSR, выполняющему этот протокол, создавать тракты LSP. Конечной точкой такого тракта является либо смежный LSR, имеющий прямую связь с данным LSR, либо выходной LSR, доступный этому LSR через некоторое количество транзитных LSR. Процессы обнаружения конечных точек этих двух типов называются соответственно процессом *базового обнаружения* и *процессом расширенного обнаружения*. *LDP* создает двустороннюю связь двух смежных LSR, которые становятся одноранговыми узлами *LDP*, взаимодействующими друг с другом посредством *LDP*-сеанса.

При обмене между LSR информацией, связанной с привязкой "метка-*FEC*", используются четыре категории сообщений *LDP*:

- сообщения обнаружения (discovery messages), используемые для того, чтобы объявить и поддерживать присутствие LSR в сети;
- сеансовые сообщения (session messages), предназначенные для создания, поддержки и прекращения *LDP*-сеансов между LSR;
- сообщения-объявления (advertisement messages), используемые для создания, изменения и отмены привязки метки к *FEC*;
- уведомляющие сообщения (notification messages), содержащие вспомогательную информацию и информацию об ошибках.

Хотя "раздает" метки всегда нижний LSR, инициатором их распределения не обязательно должен быть он; процесс может инициировать и верхний LSR, направив к нижнему LSR соответствующий запрос; такой режим называется downstream on-demand. В той или иной сети может использоваться *распределение меток* либо только по запросам сверху, либо только по инициативе нижнего LSR (unsolicited downstream), либо и то и другое вместе.

распределение меток может быть независимым или упорядоченным. В первом случае LSR может уведомить вышестоящий LSR о привязке метки к *FEC* до того, как получит информацию о привязке от нижестоящего LSR. Во втором случае высылать подобное уведомление "наверх" разрешается только после получения таких сведений "снизу".

Нижний LSR распределяет метки не только по тем верхним LSR, которые имеют с ним прямые связи. Протокол *распределения меток* может быть использован и для диалога двух LSR, между которыми существует лишь коммутируемая связь, однако результат распределения в этом случае зависит от того, в каком из двух режимов, либеральном или консервативном, работает верхний LSR.

Консервативный режим *распределения меток* – в этом режиме сообщения-объявления о привязке "метка-*FEC*", получаемые от несмежных LSR, не принимаются и отбрасываются. LSR привязывает метку к *FEC* только в том случае, если он является выходным маршрутизатором или если он получил сообщение о привязке от смежного с ним LSR. Такой режим позволяет LSR обслуживать меньшее число меток.

Либеральный режим распределения меток – в этом режиме привязка метки, выданная тем нижним LSR, с которым нет прямой связи, запоминается и используется. Такой режим удобен тем, что при реконфигурации сети соответствие между меткой и *FEC* сохраняется, даже если связь с LSR, определившим это соответствие, стала не коммутируемой, а прямой. Недостаток либерального режима состоит в том, что в верхнем LSR приходится хранить и обрабатывать заметно больше информации о соответствии между метками и *FEC*.

Как уже говорилось, метка всегда локальна, то есть обозначает некоторый *FEC* только для пары маршрутизаторов, между которыми имеется прямая или коммутируемая связь, и используется при пересылке пакетов этого *FEC* от того из маршрутизаторов данной пары, который является в ней верхним (upstream LSR), к тому, который является нижним (downstream LSR). Для пересылки пакетов того же *FEC* к следующему маршрутизатору используется другая метка, идентифицирующая этот *FEC* для новой пары маршрутизаторов, в которой маршрутизатор, бывший в предыдущей паре нижним, приобретает статус верхнего, а статус нижнего получает второй маршрутизатор этой новой пары. Отсюда ясно, что каждый маршрутизатор *MPLS*-сети должен хранить соответствие между входящими и исходящими метками для всех *FEC*, которыми он оперирует.

Одной из важнейших функций протокола *LDP* является обнаружение петель. Для этой цели можно использовать два поля в сообщениях Label Request и Label mapping, а именно Path Vector и Hop Count.

Поле Path Vector содержит список LSR-идентификаторов (первые 4 октета *LDP*-идентификатора), принадлежащих тем LSR, через которые прошло содержащее его сообщение. Если LSR получает сообщение и обнаруживает в поле Path Vector свой собственный LSR-идентификатор, он "понимает", что возникла петля. В протоколе *LDP* предусматривается возможность задать максимально допустимое значение поля Path Length, по достижении которого тоже принимается решение о возникновении петли.

Второй вариант — поле Hop Count, которое содержит счетчик LSR, пройденных сообщением LSR. Каждый пройденный LSR увеличивает его значение на единицу. Маршрутизатор, обнаруживший, что счетчик достиг максимально допустимой величины, обрабатывает сообщение как сделавшее петлю.

Протокол CR-LDP

Протокол *LDP* может следовать только таблицам маршрутизации IP. Чтобы преодолеть ограничение, было предложено расширение *LDP*, названное CR-LDP.

Протокол CR-LDP является вариантом LDP, в котором определены механизмы создания и поддержания трактов LSP с явно заданным маршрутом. Для создания тракта CR-LSP используется больше информации, чем можно получить от традиционных протоколов внутренней маршрутизации. *CR-LDP* применяется для таких приложений *MPLS*, как TE (Traffic Engineering) – управление трафиком и *QoS*, где требуется

дополнительная информация о маршрутах. В этом протоколе запрос метки может не следовать слепо вдоль дерева маршрутизации для данного адресата, т.к. предусмотрена возможность точно сообщить, как он должен следовать, включив в сообщение явно заданный маршрут. При этом программное обеспечение *CR-LDP* не использует для маршрутизации таблицы пересылки, а маршрутизирует запрос в соответствии с содержащимися в сообщении инструкциями.

Протокол *CR-LDP* не поддерживает динамического вычисления явно задаваемых маршрутов, поэтому сведения о динамическом резервировании пропускной способности должны включаться в вещательную информацию протоколов OSPF или IS-IS, или в извещения о состоянии каналов LSA. Используя эти механизмы, *CR-LDP* может занимать и резервировать пропускную способность. Доступная пропускная способность изменяется в соответствии с запросом, и ее новое значение рассылается другим узлам с помощью расширений протоколов OSPF и IS-IS, которые будут рассмотрены ниже.

В результате протокол *CR-LDP* получает в свое распоряжение явный маршрут для организации LSR. Тракт создается посредством сообщения запроса метки, содержащего динамически вычисляемый явный маршрут.

Протокол *CR-LDP* имеет также другие, новые по сравнению с базовой версией *LDP* функциональные возможности:

- явная маршрутизация с точно определенными и свободными маршрутами, при которой маршрут задается в виде последовательности групп узлов. В том случае, если в группе указано более одного маршрутизатора, при создании явного маршрута возможна определенная гибкость;
- спецификация параметров трафика (например пиковая скорость передачи, гарантированная скорость передачи и допустимая вариация задержки);
- закрепление маршрута (route pinning), которое может использоваться в тех случаях, когда изменять трассу LSP нежелательно, например, в сегментах со свободной маршрутизацией, когда в этом сегменте становится доступным лучший маршрут;
- механизм приоритетного вытеснения LSP с помощью системы приоритетов создания и удержания. Ранжируются существующие тракты LSP (приоритет удержания) и новые тракты LSP (приоритет создания) с тем, чтобы определить, может ли новый LSP вытеснять существующий LSR. Для приоритетов предложен диапазон значений от 0 (высший приоритет) до 7 (низший приоритет);
- введены новые коды состояний LSR;
- введен LSPID – уникальный идентификатор тракта CR-LSP в сети;
- введены классы (цвета) сетевых ресурсов, назначаемые администратором сети.

Хотя *CR-LDP* обладает довольно широкими возможностями инжиниринга трафика (TE – Traffic Engineering) в сетях *MPLS* и не требует реализации в оборудовании дополнительного протокола, а лишь расширения уже существующего, но в самое последнее время по ряду косвенных данных прослеживается сворачивание работ над *CR-LDP* в IETF в пользу протокола *RSVP-TE*.

RSVP для MPLS

RSVP, как и DiffServ, не найдя широкого самостоятельного применения, успешно влился в технологию *MPLS*, способствуя, наряду с *CR-LDP*, улучшению ее характеристик.

Протокол RSVP был изучен в предыдущих лекциях, а здесь рассмотрим применение протокола RSVP и его расширения *RSVP-TE* в *MPLS*.

Первой из двух функций, возложенных на RSVP технологией *MPLS*, является *распределение меток* (вместо протокола *LDP*). Вторая, традиционная для RSVP роль заключается в поддержании *QoS* в сети *MPLS*. Вне зависимости от используемого протокола *распределения меток*, маршрутизаторы LSR должны согласовать между собой параметры *QoS* для каждого *FEC*. Метки позволяют определить огромное число классов *QoS*, но реально в типичных мультисервисных сетях, даже при очень большом количестве классов *FEC*, будут существовать, как правило, всего несколько классов *QoS*.

Роль RSVP и RSVP-TE в MPLS

Первая цель введения в сеть *MPLS* функций поддержки протокола RSVP состоит в том, чтобы LSR, которые классифицируют пакеты, анализируя их метки, а не IP-заголовки, могли распознавать пакеты, принадлежащие тем потокам, для которых было сделано резервирование ресурсов. Другими словами, нужно создавать привязку меток к *FEC* для потоков, которые обеспечены резервированными ресурсами с помощью протокола RSVP. Можно рассматривать совокупность пакетов, для которых было выполнено резервирование по протоколу RSVP, как совокупность пакетов, принадлежащих некоторому новому классу *FEC*.

В расширенной версии протокола, описанной в RFC 3209 "Extensions to RSVP for LSP Tunnels" и получившей название RSVP-TE, определен новый объект LABEL, который переносится в сообщении Resv. Таким образом, RSVP становится инструментом для *распределения меток MPLS*. Когда маршрутизатору LSR нужно передать сообщение Resv для нового потока, он выбирает из своего пула свободную метку, создает запись в своей таблице LIB, определяя выбранную метку как входящую, и затем передает сообщение Resv, содержащее эту метку в объекте LABEL. Следует отметить, что, поскольку сообщения Resv идут от получателя к отправителю, это – разновидность *распределения меток* снизу.

При получении сообщения Resv, содержащего метку потока, маршрутизатор записывает ее в своей базе LIB как исходящую, назначает для данной исходящей метки входящую и пересылает ее вышестоящему LSR. Таким образом, по пути распространения сообщения создается тракт LSP. Поскольку в сообщениях Resv указываются метки, каждый LSR может легко связать соответствующие ресурсы *QoS* с трактом LSP. Протокол RSVP, расширенный объектом LABEL, может создать тракт LSP только вдоль маршрута, вычисленного схемой традиционной маршрутизации пакетов IP. Причина в том, что при использовании обычного протокола RSVP путь, по которому идет сообщение Path, управляется парадигмой пересылки на основе пункта назначения, а маршрут, по которому идет сообщение Path, задает путь LSP. Когда маршрутизатор должен переслать сообщение Path, он для определения следующего маршрутизатора, к которому он должен переслать сообщение, использует имеющуюся у него таблицу маршрутизации, которая формируется с помощью таких протоколов, как IS-IS, OSPF, RIP или BGP, и адрес получателя, содержащийся в заголовке IP-пакета. При этом отсутствует способность "управлять" сообщением Path, отправляя его вдоль конкретного, явно заданного маршрута.

Для возможности задания явного маршрута в протокол *RSVP-TE* ввели еще один объект – Explicit Route Object (ERO). ERO содержит последовательность маршрутизаторов, представляющую собой явно заданный маршрут, и включается в

сообщении Path. В ответ на это сообщение по данному маршруту передается сообщение Resv, благодаря чему резервируются ресурсы сети и устанавливается путь LSP.

Поскольку трафик, проходящий по LSP, определяется меткой, присвоенной на входном маршрутизаторе, то данный путь можно считать своеобразным туннелем, находящемся под уровнем IP-маршрутизации, причем трафик, идущий по нему, непрозрачен для промежуточных узлов. Таким образом, появилось понятие LSP-туннеля.

Управление трафиком в MPLS

Протокол *MPLS* стратегически достаточен для управления трафиком, и существует возможность автоматизировать функции такого управления. Для этого сигнальные протоколы *MPLS* должны переносить информацию, которая необходима для работы механизмов управления трафиком, находящихся на прикладном уровне, а также создавать LSP с явно заданными маршрутами. При этом есть возможность получить дополнительную гибкость, если маршрут может быть задан как строго, так и не строго, т.е. если группа узлов может быть задана как "абстрактный узел", в рамках которого существует известная свобода выбора маршрута.

Перед IETF, точнее, перед ее рабочей группой *MPLS*, возникла задача выбора такого протокола. Лучшими оказались два варианта:

- *RSVP-TE*;
- *CR-LDP*.

В первом варианте протокол RSVP должен делать в сети *MPLS* то же, что он делает в сетях IP, а именно – обрабатывать информацию, связанную с *QoS*, и резервировать ресурсы. Необходимо лишь добавить к этому возможности *распределения меток*. Во втором варианте в протокол *LDP* добавлено несколько новых объектов, обеспечивающих перенос информации о *QoS*.

На сегодняшний день оба протокола достаточно развиты.

Лекция 12. Протоколы маршрутизации

OSPF

При рассмотрении принципов *MPLS* обсуждалась необходимость заполнения в маршрутизаторах LSR таблиц меток, используемых при маршрутизации пакетов по сети *MPLS* . Для этого в каждом из узлов сети с использованием протокола маршрутизации создается база топологической информации о сетевых маршрутах. Наряду с рассматриваемыми протоколами *BGP4* и *IS-IS*, для этой цели может быть применен *протокол маршрутизации по состояниям каналов* ***OSPF (Open Shortest Path First*** *— "первым выбирается кратчайший путь")*. Поскольку *OSPF* используется наиболее часто, рассмотрение протоколов маршрутизации для *MPLS* в начинается именно с него.

Протокол *OSPF* относится к *протоколам внутреннего шлюза IGP (Interior Gateway Protocol)*. К этой категории принадлежат протоколы маршрутизации, обеспечивающие обмен информацией в пределах *автономной системы AS (Autonomous System* представляет собой сеть, находящуюся под единым административным управлением).

Метрики OSPF

В *OSPF* используется принцип контроля состояния канала (link-state protocol), а метрика представляет собой оценку эффективности связи в этом канале: чем меньше метрика, тем эффективнее организация связи. В простейшем случае метрика маршрута может равняться его длине в пересылках (hops), как это происходит в протоколе RIP. Но в общем случае значения метрики могут определяться в гораздо более широком диапазоне.

Метрика, оценивающая пропускную способность канала, определяется, например, компанией CISCO, как количество секунд, нужное для передачи 100 Мбит. Имеется следующая формула для вычисления метрики доставки информации через каналы сети *OSPF*: метрика = 10^8/скорость передачи в битах в секунду.

По этой формуле вычислены, например, следующие метрики:

- канал со скоростью 100 Мбит/с соответствует метрике 1;
- сеть Ethernet / 802.3 соответствует метрике 10;
- тракт E1 2,048 Мбит/с соответствует метрике 48;
- тракт T1 1,544 Мбит/с соответствует метрике 65;
- канал 64 Кбит/с соответствует метрике 1562;
- канал 56 Кбит/с соответствует метрике 1785;
- канал 19,2 Кбит/с соответствует метрике 5208;
- канал 9,6 Кбит/с соответствует метрике 10416.

Кроме того, протокол *OSPF* позволяет определить для любой сети значения метрики в зависимости от типа услуги ToS (Type of Service). Для каждой из метрик протокол *OSPF* строит отдельную таблицу маршрутизации. Чаще всего *OSPF* выбирает маршрут на основании полосы пропускания канала.

Загрузка канала представляет собой величину, которая изменяется в зависимости от использования канала, причем интенсивная эксплуатация канала повышает его загрузку, и поэтому при маршрутизации бывает целесообразно выбирать менее нагруженные каналы. Еще одна возможная метрика – задержка – определяет время в

микросекундах, которое требуется маршрутизатору для обработки, установки в очередь и передачи пакетов.

В случае, когда имеется несколько маршрутов с одинаковым значением метрики, маршрутизаторы могут использовать для передачи пакетов все эти маршруты, обеспечивая балансировку нагрузки. Маршрутизатор *OSPF* помещает в таблицу маршрутизации все маршруты с одинаковыми значениями метрики, и балансировка нагрузки между маршрутами происходит автоматически. Стандартизованный порядок расчета метрик, оценивающих надежность, задержку и стоимость, пока не определен. Эти вопросы решаются администратором сети.

Итак,***OSPF представляет собой протокол***, основанный на контроле состояния каналов, распространяющий эту информацию и определяющий на ее основе маршруты наименьшей стоимости в заданной метрике. Именно с его помощью LSR отображает видимый ему граф домена сети *MPLS* , где для каждой пары смежных вершин графа (маршрутизаторов) указано ребро (канал), их соединяющее, и метрика этого ребра. Граф считается ориентированным, т.е. ребро, соединяющее LSR1 с LSR2, и ребро, соединяющее LSR2 с LSR1, могут быть разными, или это может быть одно и то же ребро, но с разными метриками.

Маршрутизатор, работающий по протоколу *OSPF*, выполняет последовательно три операции: определяет отношения соседства и смежности с другими маршрутизаторами, обменивается с ними *OSPF*-пакетами извещений LSA, формируя таким образом полную топологическую карту сети, а затем вычисляет дерево маршрутов, используя алгоритм "первым выбирается кратчайший путь" SPF (Shortest Path First), известный также по имени его создателя как алгоритм Дейкстры.

Для сети *MPLS* с помощью этого алгоритма протокол *OSPF*, основываясь на базе данных об условиях использования возможных связей, вычисляет кратчайшие пути между заданным LSR – вершиной графа и всеми остальными вершинами. Результатом работы алгоритма является таблица, где для каждой вершины графа сети *MPLS* указан список ребер, соединяющих ее со всеми другими вершинами этого графа по кратчайшему пути.

Суть алгоритма иллюстрирует следующая процедура. Представим изображенную на рис. 12.1 сеть *MPLS* , содержащую 7 LSR, как набор из 7 фишек, лежащих на поверхности стола и соединенных между собой нитями разной длины. Пусть, например, алгоритм Дейкстры выполняется в маршрутизаторе LSR4. Постепенно поднимаем со стола фишку, соответствующую LSR4. Нити, связывающие эту фишку с другими, начинают натягиваться, и следующей со стола будет поднята фишка LSR2, связанная с LSR4 самой короткой нитью. При дальнейшем подъеме фишки LSR4 мы поднимем с поверхности стола и фишку LSR5. Кратчайший (в рассмотренном выше смысле) путь между LSR4 и LSR5 представит либо нить, связывающая соответствующие этим двум LSR фишки непосредственно, либо составной путь из нитей между фишками LSR4 и LSR2, LSR2 и LSR3, LSR3 и LSR5. Продолжая процедуру подъема фишки LSR4, мы шаг за шагом поднимем все фишки, находя каждый раз кратчайший путь между LSR4 и тем LSR, которому соответствует очередная поднимаемая нитью фишка.

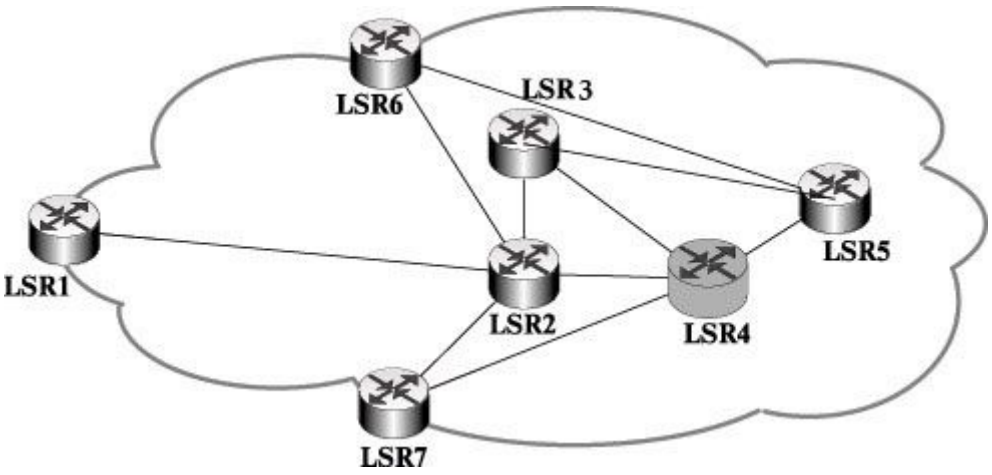


Рис. 12.1. Иллюстрация алгоритма Дейкстры

Существует два разных маршрута между LSR4 и LSR5: прямой и составленный из участков между LSR4 и LSR2, LSR2 и LSR3, LSR3 и LSR5. В том случае, если между двумя узлами сети существует несколько маршрутов с близкими по значению метриками, протокол *OSPF* позволяет распределять трафик по этим маршрутам в пропорции, соответствующей значениям метрик. Например, если прямой маршрут между LSR4 и LSR5 имеет метрику 4, а составной маршрут из участков LSR4 и LSR2, LSR2 и LSR3, LSR3 и LSR5 имеет метрику 8, то две трети трафика будет направлено по первому из них, а оставшаяся треть – по второму.

Суммарный эффект такого решения заключается в уменьшении средней задержки прохождения дейтаграмм от отправителя к получателю, а также в сглаживании колебаний задержки.

Еще одно преимущество поддержки альтернативных маршрутов связано с соображениями надежности. Когда используется только один из возможных маршрутов и он внезапно выходит из строя, весь трафик должен быть срочно переведен на альтернативный маршрут. При массовом переключении больших объемов трафика с одного маршрута на другой весьма велики потери и даже вероятно образование затора на новом маршруте. Если же до аварии использовалось разделение трафика по нескольким маршрутам, отказ одного из них вызовет ремаршрутизацию лишь части трафика, и это может сгладить отрицательные последствия аварии.

Области OSPF

Автономная система AS(Autonomous System) представляет собой сеть, находящуюся под единым административным управлением.

Область OSPF(OSPF area) — это логическая подсистема автономной системы, в которой *OSPF* функционирует в качестве ее протокола внутренней маршрутизации. Области "укрупняют" маршрутную информацию протокола *OSPF* и помогают скрывать детали топологии сети. Так, топология одной области не известна ни в какой другой области. Внутренние маршрутизаторы области вообще не владеют информацией о топологии использующих *OSPF* сетей, которые находятся за пределами этой области, что дает выигрыш в затратах на поддержание маршрутной информации. Эта, а также некоторые другие возможности делают *OSPF* хорошо масштабируемым протоколом маршрутизации для крупных сетей. А сам протокол *OSPF* основан на концепции областей

как совокупностей смежных сетей и относящихся к ним маршрутизаторов с интерфейсами, связывающими их с этими сетями и с узлами в них.

Автономная система, базирующаяся на протоколе *OSPF*, может представлять собой одну область или состоять из нескольких областей. В каждой области работает собственная копия алгоритма маршрутизации по состоянию каналов, что позволяет каждой области формировать свою базу данных сетевой топологии. Именно область ограничивает охват лавинной рассылки уведомлений, т.к. уведомления не выходят за пределы области, в которой они были сформированы.

Протокол *OSPF* разграничивает функции маршрутизаторов в зависимости от того, какое место они занимают в автономной системе *OSPF*, объединяющей все маршрутизаторы, которые ведут обмен информацией под управлением общего протокола. Разумеется, маршрутизаторы разделяются на классы протокола *OSPF*, а не технологии *MPLS* , но так как все маршрутизаторы *MPLS* поддерживают протокол *OSPF* (если он выбран в качестве протокола, с помощью которого составляется топологическая карта сети), подобная классификация полностью к ним применима. Таким образом, термины "маршрутизатор LSR" и "*OSPF*-маршрутизатор" используются в лекции как синонимы.

Договорившись об этом, отметим, что, с точки зрения протокола *OSPF*, имеются маршрутизаторы четырех типов:

- внутренний маршрутизатор IR (Internal Router), все интерфейсы которого находятся внутри одной области *OSPF*;
- маршрутизатор опорной области BR (Backbone Router), все интерфейсы которого находятся внутри опорной области;
- пограничный маршрутизатор области ABR (Area Border Router), располагающийся на границе двух областей *OSPF*;
- пограничный маршрутизатор автономной системы ASBR (Autonomous System Boundary Router), который располагается на границе двух автономных систем, поддерживающих *OSPF*.

Кроме этого назначаются два маршрутизатора, так и называемые: назначенный маршрутизатор DR (Designated Router) и резервный назначенный маршрутизатор BDR (Backup Designated Router), которые являются центральными узлами сбора всех сообщений о корректировках. Все остальные маршрутизаторы являются по отношению к маршрутизаторам DR и BDR подчиненными.

Здесь лишь отметим, что один и тот же маршрутизатор может выполнять в системе несколько функций одновременно.

Принципы работы OSPF

Первым этапом является распространение информации о топологии сети, инициирование отношений соседства и смежности. После инициирования каждый *OSPF*-маршрутизатор начинает обмен LSA, передает пакеты HELLO через все свои интерфейсы, распространяя эту информацию по всем соседним маршрутизаторам, так что каждый из них узнает идентификаторы своих ближайших соседей. Эта топологическая информация начинает распространяться по сети от соседа к соседу, пополняя топологические карты в маршрутизаторах LSR новыми данными, и через некоторое время достигает самых удаленных маршрутизаторов. В результате все маршрутизаторы сети получают сведения о графе сети, которые хранятся в их топологических базах данных.

Впоследствии, при появлении новой связи или нового соседа, маршрутизатор узнает об этом из новых пакетов HELLO. В них указывается достаточно детальная информация о том маршрутизаторе, который передал этот пакет, а также о его ближайших соседях, так что этот маршрутизатор можно однозначно идентифицировать.

Таким образом, на первом шаге каждый маршрутизатор *OSPF* строит граф связей сети, в котором вершинами графа являются маршрутизаторы, а ребрами – каналы, включенные в интерфейсы маршрутизаторов. Для построения этого графа все маршрутизаторы обмениваются со своими соседями той информацией о сети, которой они располагают в данный момент.

Далее с помощью полученного графа находятся оптимальные маршруты, причем каждый маршрутизатор считает себя центром сети и ищет оптимальный маршрут к каждому известному ему маршрутизатору (или к известной ему сети). В любом найденном таким образом маршруте, в соответствии с принципом одношаговой маршрутизации, запоминается только первый шаг – к следующему маршрутизатору. Если несколько маршрутов к сети назначения имеют одинаковую метрику, то в таблице маршрутизации запоминаются первые шаги всех этих маршрутов. Данные об этих шагах попадают в таблицу маршрутизации.

Благодаря иерархической структуре областей уменьшаются перегрузки, связанные с поддержкой огромных таблиц маршрутизации и с пересчетом этих таблиц при изменениях маршрутов. Извещения о корректировках передаются только в случае, если в сети происходят изменения. Эти извещения рассылаются всем маршрутизаторам *OSPF*, что сокращает время сходимости.

Протокол IS-IS

Протокол маршрутизации OSI под названием "протокол обмена данными между промежуточными системами *IS-IS*" (Intermediate System – to – Intermediate System) использует тот же принцип маршрутизации по состоянию каналов, что и рассмотренный выше протокол *OSPF*. Но если *OSPF* является разработкой IETF, то протокол *IS-IS* был создан ISO (International Standard Organization).

Как раз в терминологии ISO маршрутизаторы называются "промежуточными системами" (Intermediate System, IS), а хосты – "конечными системами" (End System, ES). Существует также протокол ES-IS, с помощью которого маршрутизаторы узнают о подключенных к ним хостах, а хосты – о маршрутизаторах.

Оказалось, что протокол *IS-IS* очень хорошо работает в весьма больших сетях, содержащих более 500 маршрутизаторов.

Подобно *OSPF*, протокол *IS-IS* разделяет сеть на области, чтобы не распространять информацию о маршрутах среди всех маршрутизаторов сети, обеспечивая разумные размеры их таблиц маршрутизации, а тем самым – быструю сходимость поиска маршрута.

В технологии *MPLS* протокол *IS-IS* применяется почти таким же образом, как и рассмотренный протокол *OSPF*. Оба они относятся к классу протоколов IGP и служат для создания и поддержки топологической карты, используемой протоколом LDP.

Протоколы динамической маршрутизации задействованы в LSR с целью идентифицировать соседние LSR одного сетевого домена и периодически обновлять

информацию о топологии сети при помощи рассмотренных извещений о состоянии каналов. Это является и главным преимуществом такой маршрутизации, т.к. для передачи данных между двумя конечными пунктами используется кратчайший на данный момент маршрут.

Названное преимущество протокола *IS-IS* — в то же время и его существенный недостаток. Этот недостаток связан с так называемой лавинной рассылкой пакетов (flooding), вызываемой внезапным изменением состояния каналов (либо канал неожиданно стал недоступен, либо, наоборот, возобновил свою работу после перерыва). Flooding характеризуется обменом между маршрутизаторами огромным количеством служебных пакетов, т.к. каждый маршрутизатор, соседний с данным, приняв очередное извещение об изменении состояния каналов и обновив свои таблицы маршрутизации, пересылает его дальше.

В *IS-IS* присутствуют аналогичные *OSPF* механизмы обнаружения соседей с помощью пакетов HELLO, синхронизации баз данных и оповещения об изменении состояния связи путем рассылки пакетов (flooding). Аналогами *OSPF*-пакетов LSU (Link State Update) в *IS-IS* являются пакеты LSP (Link State Packet, не путать с LSP–коммутируемым по меткам тракт).

Метрики IS-IS

Основная метрика, используемая в *IS-IS*, – это некоторое число, не превышающее 1024 для маршрута и 64 – для канала. Смысл и числовые значения этой метрики для каждого канала и маршрута определяет системный администратор. Метрика маршрута вычисляется как сумма метрик составляющих его каналов.

Кроме того, можно задать три дополнительные метрики: "задержка" (delay), отражающая длительность задержки в канале, "стоимость передачи по каналу" (expense), отражающая коммуникационные затраты, и "ошибки" (error), отражающая коэффициент ошибок в канале.

Маршрутизация IS-IS

Принципы маршрутизации *IS-IS* очень похожи на используемые в протоколе *OSPF*. Для синхронизации баз данных маршрутизации *IS-IS* использует пакеты CSNP (Complete Sequence Number Packet) и PSNP (Partial Sequence Number Packet), по своему назначению примерно аналогичные пакетам DD (Database Description) и LSR (Link State Request) протокола *OSPF*. Протокол *IS-IS* поддерживает и двухуровневую иерархическую систему сетей (периферийные области и магистральная область 0), но принцип организации этой системы отличается от принципа ее организации в *OSPF*.

BGP

Использование протокола BGP в MPLS

Третий из используемых технологией *MPLS* протоколов маршрутизации (*OSPF*, *IS-IS*, ***BGP-4***) называется Border Gateway Protocol (*BGP*). Его первая версия *BGP*-1 появилась в 1989 году, а повсеместное внедрение *BGP*-4 началось с 1993 года.

Рассмотрим только основные функции этой последней версии протокола и те, которые непосредственно используются в технологии *MPLS*.

В частности, это относится к многопротокольному расширению протокола *BGP*-4, мало освещенному в существующей литературе, но нашедшему применение при построении *MPLS*-VPN.

Напомним описанное в лекции 9 разделение функций технологии *MPLS* на два компонента – управление и пересылка пакетов, – изображенное на рис. 9.1 в виде двух плоскостей. Управляющий компонент использует протоколы маршрутизации *OSPF*, *IS-IS* и *BGP*-4 для обмена маршрутной информацией между маршрутизаторами. На основе этой информации в каждом маршрутизаторе формируется и модифицируется сначала таблица маршрутизации, а затем, с учетом информации о смежных системах в каждом интерфейсе, – таблица пересылки пакетов. Когда система получает пакет, пересылающий компонент анализирует информацию, содержащуюся в его заголовке, ищет соответствующую запись в таблице пересылки и направляет этот пакет в выходной интерфейс.

Но если рассмотренные выше протоколы *OSPF* и *IS-IS* выполняют эту задачу в пределах одной автономной системы AS, которая представляет собой, по сути, самодостаточную независимую сеть, не имеющую полученных каким-либо логическим путем сведений о других сетях в составе всей сети *MPLS*, то роль протокола *BGP*-4 гораздо шире.

Его основное назначение как раз и состоит в том, чтобы передавать от одного *BGP*-маршрутизатора другим *BGP*-маршрутизаторам информацию о наличии других автономных сетей и об их структуре, формируя тем самым иерархическую схему маршрутизации, связывающую разные узлы и автономные сети в единую *MPLS*/IP-сеть и позволяющую свободно устанавливать связь между собой системам, неизвестным друг другу.

Необходимость декомпозиции глобальной *MPLS*/IP-сети на автономные системы обусловлена очевидными мощностными соображениями: если большое количество маршрутизаторов попытается вступить во взаимодействие, трафик превысит все мыслимые границы.

BGP специфицируется как сеанс связи между двумя узлами, а так как в сети будет параллельно выполняться много *BGP*-сеансов, один маршрутизатор может быть вовлечен в несколько таких сеансов. В ходе *BGP*-сеанса между одноранговыми узлами протокола *BGP* происходит обмен сообщениями по TCP-соединению.

Версия 4 протокола *BGP* значительно отличается от предыдущих реализаций *BGP* и фактически включает в себя два отдельных протокола:

- протокол *EBGP* (External Border Gateway Protocol), используемый для маршрутизации между автономными системами;
- протокол *IBGP* (Internal Border Gateway Protocol), используемый для маршрутизации внутри автономной системы.

Второе принципиальное отличие протокола *BGP* от *OSPF* и *IS-IS* заключается в том, что он относится не к категории протоколов маршрутизации по состоянию каналов, а к категории дистанционно-векторных протоколов.

Принцип вектора расстояния подразумевает выбор маршрута исходя из кратчайшего расстояния между системами, определяемого числом пересылок. Протоколы

на основе вектора расстояния обычно учитывают только число пересылок (hops) в маршруте.

Кроме обычных параметров дистанционно-векторных протоколов в *BGP* используется дополнительный механизм, именуемый маршрутно-векторной маршрутизацией (path-vector routing). Это обусловлено тем, что ни маршрутизация с учетом состояния каналов, ни дистанционно-векторная маршрутизация в чистом виде для внешней маршрутизации не эффективны.

Алгоритм Беллмана-Форда

Метод дистанционно-векторной маршрутизации иногда называют также методом Беллмана или методом Форда-Фалкерсона по имени исследователей, которые первыми опубликовали идею алгоритма. Сама эта идея довольно проста. Маршрутизатор хранит в таблице список всех известных маршрутов с указанием в каждом элементе таблицы сети получателя и целого числа – количества пересылок до этой сети. Время от времени каждый маршрутизатор отсылает копию своей таблицы другим маршрутизаторам, к которым он имеет прямой доступ. Получив такую копию от LSR-B, маршрутизатор LSR-A анализирует полученный набор адресатов и расстояний до них. Маршрутизатор LSR-A заменяет данные в своей таблице, если маршрутизатору LSR-B известен более короткий, чем имеющийся в ней, маршрут к получателю, или если в его списке есть неизвестный ему до сих пор получатель, а также если LSR-A выполняет маршрутизацию через LSR-B, но расстояние от LSR-B до получателя изменилось.

На основе этой таблицы, согласно алгоритму Беллмана-Форда, и рассчитывается значение метрики (например стоимости маршрута, задержки и т.п.) для каждой пересылки в сети и поиск минимального суммарного числа пересылок. Обратим внимание на то, что понятие "дистанционный вектор" связано с характером периодически передаваемой протоколом информации. В сообщениях содержится пара чисел {R, D}, где R – вектор, определяющий получателя, а D – расстояние до этого получателя, т.е. один маршрутизатор сообщает другому о своей возможности достичь получателя R за D пересылок.

При маршрутизации по протоколу *BGP* пересылка возможна как между внутренними маршрутизаторами (расположенными внутри одной AS), которые работают под управлением протокола IBGR так и между внешними маршрутизаторами, соединяющими разные автономные системы AS, когда маршрутизация выполняется под управлением протокола EBGR.

Применяемый в *BGP* маршрутно-векторный механизм помогает решить проблему традиционной дистанционно-векторной маршрутизации, возникающую в условиях функционирования между автономными системами. Дело в том, что в разных AS могут применяться разные метрики измерения длины маршрутов, а это может привести к проблемам интерпретации одних и тех же числовых значений во внешних *BGP*-маршрутизаторах. Поэтому механизм маршрутно-векторной маршрутизации предусматривает отказ от метрики маршрута. Тогда маршрутизаторы просто обмениваются информацией об автономных системах, к которым и через которые у них есть доступ.

Существует три класса автономных систем AS:

- системы с множественной адресацией (multihomed);

- тупиковые, имеющие только один выход в Интернет (single-homed);
- многоканальные транзитные сети (multihomed transit).

Системы с множественной адресацией (multihomed) – это системы, имеющие несколько соединений с внешними автономными системами. Такие системы еще называют многоканальными нетранзитными (multihomed nontransit). Автономная система с множественной адресацией может принимать маршрутную информацию от всех соединенных с ней систем, но сама она выполняет только внутреннюю маршрутизацию.

Многие автономные системы на самом деле являются тупиковыми (stub) или одноканальными (single-homed) и имеют лишь один выход во внешнюю сеть. Соответственно, они не требуют никаких дополнительных правил для управления ими и обслуживания большого списка *BGP*-маршрутов в шлюзе, у которого имеется только один выход в Интрасеть.

Третий тип автономной системы – транзитная сеть. Транзитные AS – это системы с множественной адресацией, которые принимают информацию от внешних автономных систем и выполняют маршрутизацию этой информации к другим внешним AS.

Маршрутизаторы BGP

Имеется три типа маршрутизаторов *BGP*: спикеры, пограничные шлюзы и равноправные маршрутизаторы *BGP*.

Спикерами *BGP* (BGP speakers) являются все маршрутизаторы автономной системы *BGP*.

Спикеры *BGP*, соединяющие две или несколько автономных систем, называются пограничными шлюзами (Border Gateways). Они нужны автономным системам только в том случае, если AS использует для связи с другими автономными системами *MPLS*/IP-сети протокол EBGR. Задача пограничного шлюза – извещать о внутренних маршрутах автономной системы (и о других известных ему маршрутах) любой внешний спикер *BGP*, с которым этот шлюз связан.

Согласно принципам сетевой маршрутизации, во время сеансов связи спикеры *BGP* обмениваются маршрутной информацией о топологии и метрических характеристиках соответствующих участков сети. Такой обмен происходит между равноправными маршрутизаторами (*BGP* peer) автономной системы.

Равноправные маршрутизаторы *BGP* не обязательно должны иметь прямые связи друг с другом; однако между двумя спикерами *BGP* всегда должен существовать стандартный способ коммуникации для того, чтобы они могли инициировать сеанс связи.

Когда *BGP* устанавливает сеанс связи двух равноправных маршрутизаторов, между которыми нет прямого соединения, такая связь называется одноранговой связью с пересылкой по протоколу *EBGP* (EBGP multihop peering). Используя внешние соединения по протоколу *EBGP*, спикер *BGP* может инициировать сеанс связи с другими спикерами, находящимися на расстоянии нескольких пересылок. Во всех таких случаях для организации сеансов *BGP* использует протокол TCP.

При одноранговой связи спикеры *BGP* обмениваются полными копиями таблиц маршрутизации во время первоначального двустороннего сеанса, включая повторные запуски.

BGP является протоколом с устойчивым состоянием, и поэтому маршрутная информация, обмен которой между одноранговыми узлами проведен успешно, не нуждается в обновлении. Эта информация считается действительной до тех пор, пока один из одноранговых узлов не уведомит другой о том, что это не так, или пока не закончится *BGP*-сеанс между ними.

Ключевым принципом, лежащим в основе протокола *BGP*, является то, что когда один одноранговый узел информирует своего партнера о том, что IP-адрес доступен по сообщенному маршруту, партнер может быть уверен, что равноправный узел уже успешно использует этот маршрут для передачи собственного трафика. При этом подразумевается, что маршруты, о которых узел извещен, могут использоваться всегда, когда о них объявляется. Наряду с возможностью использовать маршрут предоставляется набор атрибутов, связанных с IP-префиксом.

Протокол EBGP

Протокол EBGP (Exterior Border Gateway Protocol) используется для установления соединения между спикерами *BGP* разных автономных систем, включая коммуникации между Интернет-провайдерами и точками доступа PoP, а также между большими корпоративными сетями и провайдерами услуг.

Протокол IBGP

Очевидно, что *BGP*-маршрутизаторы, находящиеся в одной AS, тоже должны обмениваться между собой маршрутной информацией. Это необходимо для согласованного отбора внешних маршрутов в соответствии с политикой данной AS и для организации транзитных маршрутов через автономную систему. Такой обмен производится по протоколу *BGP*, который в этом случае называется ***IBGP*** (Internal BGP).

Отличие *IBGP* от *EBGP* состоит в том, что при извещении о маршруте соседнего маршрутизатора, находящегося в той же AS, в список номеров автономных систем AS_Path не вводится номер собственной автономной системы (AS_Path — список номеров автономных систем, через которые должна пройти дейтаграмма по пути в указанную сеть).

Лекция 13. Инжиниринг трафика. Виртуальные частные сети

При любом числе пользователей сети *ССП* требуется решение задач по управлению трафиком. По своему замыслу данная сеть предполагает одновременное существование множества разнотипных потоков. Каждый из таких потоков требует безусловного соблюдения одних параметров передачи и допускает некоторые уступки по другим. Поэтому в периоды возникновения перегрузок сеть может для одного потока урезать полосу пропускания, для другого – увеличить время доставки, а для третьего, например, пренебречь целостностью передаваемых данных. Мультисервисная сеть должна обладать более сложной системой управления по сравнению с системами управления традиционными сетями. Она должна обеспечивать одновременное предоставление множества разнообразных сетевых услуг и передачу по сети разнотипного трафика. Для эффективного управления трафиком необходимо располагать соответствующими аппаратными и программными средствами, позволяющими быстро и гибко предоставлять пользователю любую услугу.

Traffic Engineering

Под термином ***Traffic Engineering*** понимают методы и механизмы сбалансированной загрузки всех ресурсов сети за счет рационального выбора пути прохождения трафика через сеть. Механизм управления трафиком предоставляет возможность устанавливать явный путь, по которому будут передаваться потоки данных.

При традиционной маршрутизации IP-трафик маршрутизируется посредством его передачи от одной точки назначения к другой и следует до пункта назначения по пути, имеющему наименьшую суммарную метрику сетевого уровня.

Следует заметить, что при наличии в сети нескольких равноценных альтернативных маршрутов трафик делится между ними, и нагрузка на маршрутизаторы и каналы связи распределяется более сбалансированно. Но если маршруты не являются полностью равноценными, распределение трафика между ними не происходит.

Еще один существенный недостаток традиционных методов маршрутизации трафика в сетях IP заключается в том, что пути выбираются без учета текущей загрузки ресурсов сети. Если кратчайший путь уже перегружен, то пакеты все равно будут посылаться по этому пути. Налицо явная ущербность методов распределения ресурсов сети – одни из них работают с перегрузкой, а другие не используются вовсе. Никакие методы QoS данную проблему решить не могут: нужны качественно иные механизмы. Технология управления трафиком – достаточно эффективный механизм использования ресурсов сети.

Основным инструментом выбора и установления путей в *ССП* сегодня является технология *MPLS*. Она применяет и развивает концепцию виртуальных каналов в сетях X.25, Frame Relay и ATM, объединяя ее с техникой выбора путей на основе информации о топологии и текущей загрузке сети, получаемой с помощью протоколов маршрутизации сетей IP.

MPLS TE

Для решения задачи *TE* технология *MPLS* использует расширения протоколов маршрутизации, работающих на основе алгоритма состояния связей. Сегодня такие

расширения стандартизованы для протоколов OSPF и IS-IS. Данные протоколы, в отличие от дистанционно-векторных протоколов, к которым относится, например, RIP, дают маршрутизатору полную топологическую информацию о сети. Их объявления содержат информацию о маршрутизаторах и сетях, а также о физических связях между ними. Каждая связь характеризуется текущим состоянием работоспособности и метрикой, в качестве которой используется величина, обратная пропускной способности канала.

Для решения задачи *TE* в протоколы OSPF и IS-IS включены новые типы объявлений для распространения по сети информации о номинальной и незарезервированной (доступной для потоков *TE*) пропускной способности каждой связи. Таким образом, ребра результирующего графа сети, создаваемого в топологической базе каждого маршрутизатора, будут маркированы этими двумя дополнительными параметрами (см. рис. 13.1).

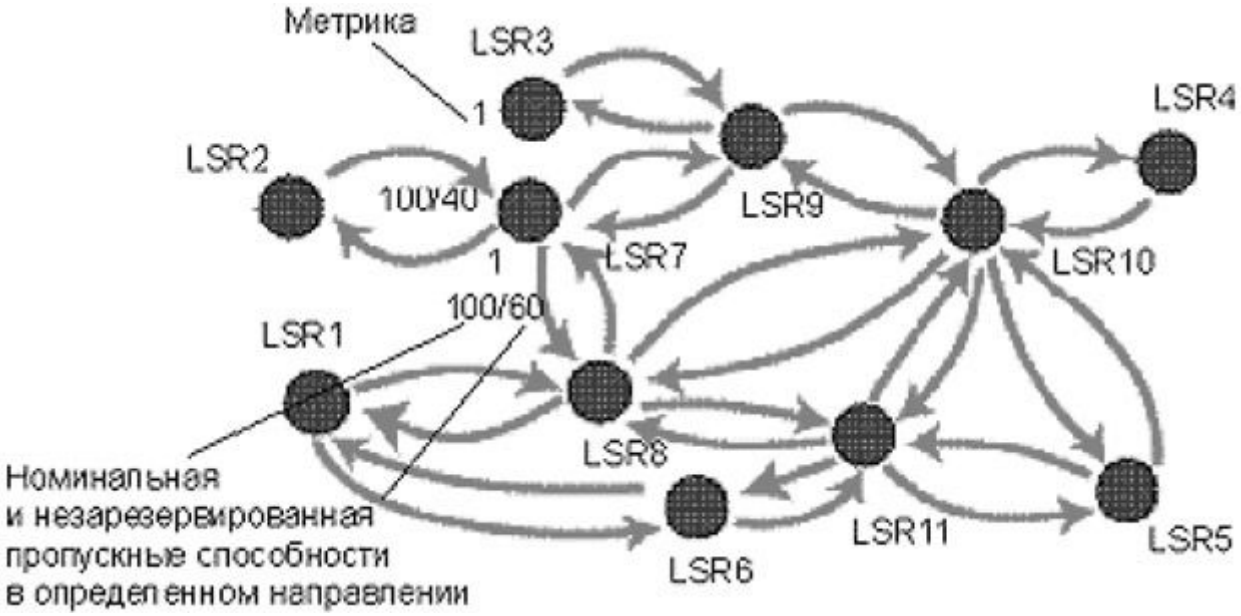


Рис. 13.1. Граф сети

Располагая таким графом, а также параметрами потоков, для которых нужно определить пути *TE*, маршрутизатор может найти рациональное решение, удовлетворяющее, например, одному из сформулированных выше ограничений на коэффициенты использования ресурсов сети, обеспечив тем самым ее сбалансированную загрузку. Для упрощения задачи оптимизации выбор путей для некоторого набора потоков может осуществляется по очереди, при этом в качестве ограничения выступает суммарная загрузка каждого ресурса сети. Обычно считается, что внутренней производительности маршрутизатора достаточно (в среднем) для обслуживания любого трафика, который способны принять интерфейсы маршрутизатора. Поэтому в качестве ограничений выступают только максимально допустимые значения коэффициентов загрузки каналов связи, устанавливаемые индивидуально или же имеющее общее значение. Решение задачи определения маршрута с учетом ограничений получило название Constrained-based Routing, а протокол OSPF с соответствующими расш ирениями – Constrained SPF, или CSPF.

Понятно, что поиск путей *TE* по очереди снижает качество решения – при одновременном рассмотрении всех потоков можно найти более рациональную загрузку ресурсов. В примере, показанном на рис. 13.2, ограничением является максимально допустимое значение коэффициента использования ресурсов, равное 0,65.

В варианте 1 решение было найдено при очередности рассмотрения потоков 1 –> 2 –> 3. Для первого потока был выбран путь A-B-C, так как в этом случае он, с одной стороны, удовлетворяет ограничению (все ресурсы вдоль пути – каналы A-B, A-C и соответствующие интерфейсы маршрутизаторов оказываются загруженными на 0,5/1,5 = 0,33), а с другой – обладает минимальной метрикой (65 + 65 = 130). Для второго потока также был выбран путь A-B-C, так как и в этом случае ограничение удовлетворяется – результирующий коэффициент использования оказывается равным (0,5 + 0,4)/1,5 = 0,6. Третий поток направляется по пути A-D-E-C и загружает ресурсы каналов A-D, D-E и E-C на 0,3 (метод расчета метрик канала был описан в предыдущей лекции).

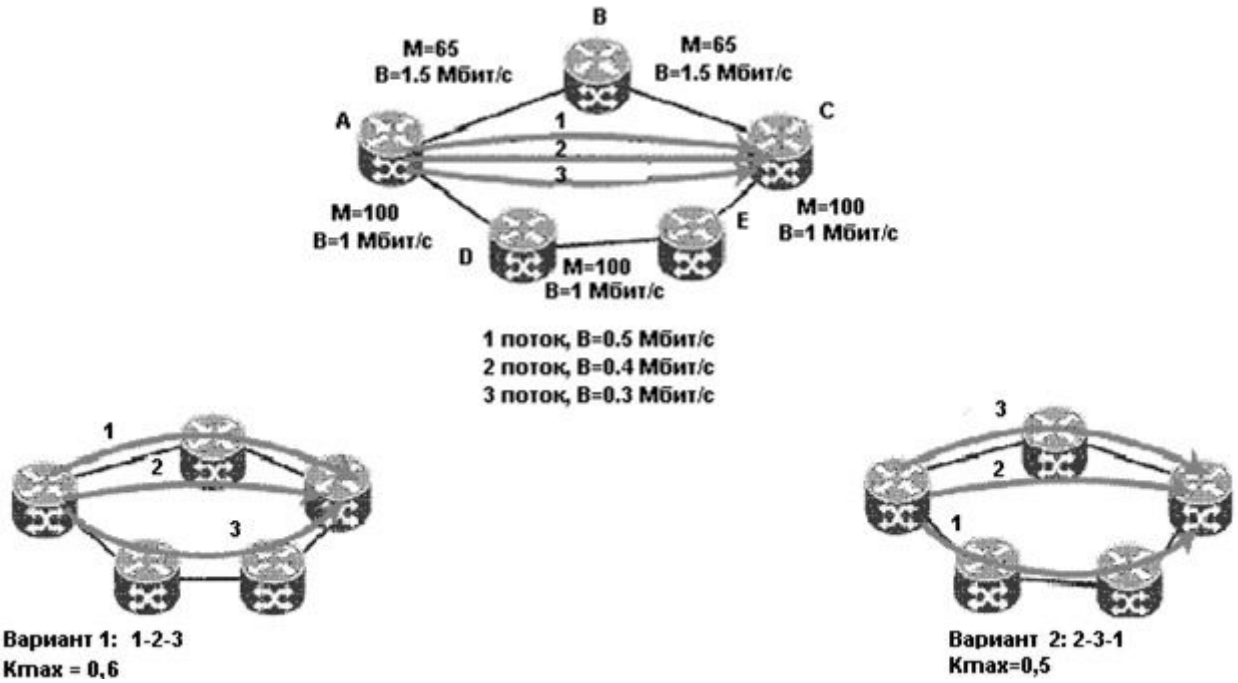


Рис. 13.2. Варианты загрузки ресурсов

Решение 1 можно назвать удовлетворительным, так как коэффициент использования любого ресурса в сети не превышает 0,6.

Однако существует лучший способ, представленный в варианте 2. Здесь по верхнему пути A-B-C были направлены потоки 2 и 3, а поток 1 – по нижнему пути A-D-E-C. Ресурсы верхнего пути оказываются загружены на 0,46, а нижнего – на 0,5, т. е. налицо более равномерная загрузка ресурсов, а максимальный коэффициент использования по всем ресурсам сети не превышает 0,5. Этот вариант может быть получен при одновременном рассмотрении всех трех потоков с учетом ограничения min (max Ki) или же при рассмотрении потоков по очереди в последовательности 2 –> 3 –> 1.

Тем не менее в производимом сегодня оборудовании применяется вариант *MPLS TE* с последовательным рассмотрением потоков. Он проще в реализации и ближе к стандартным для протоколов OSPF и IS-IS процедурам нахождения кратчайшего пути для одной сети назначения.

В технологии *MPLS TE* информация о найденном рациональном пути используется полностью – т. е. запоминается не только первый транзитный узел, как в основном режиме маршрутизации IP, а все промежуточные узлы пути вместе с начальным и конечным, т. е. маршрутизация производится от источника. Поэтому достаточно, чтобы поиском путей занимались только пограничные LSR сети, а внутренние – лишь поставляли им

информацию о текущем состоянии сети, которая необходима для принятия решений. Такой подход обладает несколькими преимуществами по сравнению с распределенной моделью поиска пути, лежащей в основе стандартных протоколов маршрутизации IP:

1. он позволяет использовать "внешние" решения, когда пути находятся какой-либо системой оптимизации сети в автономном режиме, а потом прокладываются в сети;
2. каждый из пограничных LSR может работать по собственной версии алгоритма, в то время как при распределенном поиске на всех LSR необходим идентичный алгоритм, что усложняет построение сети с оборудованием разных производителей;
3. такой подход разгружает внутренние LSR от работы по поиску путей.

После нахождения пути, независимо от того, найден он был пограничным LSR или внешней системой, его необходимо установить. Для этого в *MPLS TE* используется специальный протокол сигнализации, который умеет распространять по сети информацию о явном (explicit) маршруте. Сегодня в *MPLS TE* определено два таких протокола: RSVP с расширениями *TE* и CR-LDP (таблица 13.1).

При установлении нового пути в сообщении сигнализации наряду с последовательностью адресов пути указывается также и резервируемая пропускная способность. Каждый LSR, получив такое сообщение, вычитает запрашиваемую пропускную способность из пула свободной пропускной способности соответствующего интерфейса, а затем объявляет остаток в сообщениях протокола маршрутизации.

Таблица 13.1. Сравнение протоколов CR-LDP, RSVP-TE

	CR-LDP	**RSVP-TE**
Используемый транспортный протокол	TCP	Исходный IP
Надежность операторского класса	Нет	Да
Поддержка трафика "много точек – точка"	Да	Да
Поддержка вещательной рассылки	Нет	Нет
Поддержка слияния LSP	Да	Да
Явная маршрутизация	Со строгими и нестрогими участками маршрута	Со строгими и нестрогими участками маршрута
Ремаршрутизация LSP	Да	Да, путем записи маршрута
Вытеснение потоков в LSP	Да, на основе приоритета	Да, на основе приоритета
Средства безопасности	Да	Да
Защита LSP	Да	Да
Состояние LSP	Жесткое	Нежесткое
Регенерация состояния LSP	Не требуется	Периодическая, по участкам
Резервирование совместно используемых ресурсов	Нет	Да
Обмен параметрами трафика	Да	Да
Управление трафиком	В прямом направлении	В обратном направлении
Авторизация пользователей	Неявная	Явная
Индикация протокола уровня 3	Нет	Да
Ограничения в зависимости от класса ресурса	Да	Нет

Основы VPN

Виртуальная сеть – это выделенная сеть на базе общедоступной сети, поддерживающая конфиденциальность передаваемой информации за счет использования туннелирования и других процедур защиты. В основе технологии *VPN* лежит идея обеспечения доступа удаленных пользователей к корпоративным сетям, содержащим конфиденциальную информацию, через сети общего пользования.

Проводя сравнение между частными и *виртуальными частными сетями*, следует выделить несомненные преимущества *VPN*:

- технология *VPN* позволяет значительно снизить расходы по поддержанию работоспособности сети: пользователь платит только абонентскую плату за аренду канала. Кстати, аренда каналов также не вызывает каких-либо затруднений вследствие широкомасштабности сети Интернет;
- удобство и легкость при организации и перестроении структуры сети.

Разработка единой модели обслуживания *виртуальной частными сетями* сети могла бы упростить сетевые операции, но такой подход не может удовлетворить различным требованиям клиентов, так как они уникальны. Каждый клиент предъявляет свои требования к безопасности, числу сайтов, сложности маршрутизации, критичным приложениям, моделям и объемам трафика. Все сети *VPN* условно можно разделить на три основных вида:

- внутрикорпоративные *VPN* (Intranet VPN);
- межкорпоративные *VPN* (Extranet VPN):
- *VPN* с удаленным доступом (Remote Access VPN).

Интрасеть представляет собой наиболее простой вариант *VPN*, он позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи.

Экстрасеть – вариант построения *VPN* "Экстрасеть", предназначенный для обеспечения доступа из сети одной компании к ресурсам сети другой, уровень доверия к которой намного ниже, чем к своим сотрудникам. Поэтому, когда несколько компаний принимают решение работать вместе и открывают друг для друга свои сети, они должны позаботиться о том, чтобы их новые партнеры имели доступ только к определенной информации.

VPN с удаленным доступом. Принцип работы *VPN* с удаленным доступом прост: пользователи устанавливают соединения с местной точкой доступа к глобальной сети (PoP), после чего их вызовы туннелируются через Интернет, что позволяет избежать платы за междугородную и международную связь. Затем все вызовы концентрируются на соответствующих узлах и передаются в корпоративные сети.

Важную роль при построении *VPN* играют отношения предприятия с провайдером, в частности, распределение между ними функций по конфигурированию и эксплуатации *VPN*-устройств. При создании защищенных каналов *VPN*-средства могут располагаться как в среде оборудования провайдера, так и в оборудовании предприятия. В зависимости от этого выделяют два варианта построения *VPN*:

- пользовательская схема (Customer Provided *VPN*);

- провайдерская схема (Provider Provisioned *VPN*).

Кроме вышеперечисленной классификации, все варианты создания *VPN* можно разделить на две категории: программные и аппаратные.

Программные решения представляют собой готовые приложения, которые устанавливаются на подключенном к сети компьютере со стандартным программным обеспечением.

Аппаратные *VPN*-решения включают в себя компьютер, операционную систему, специальное программное обеспечение. *Виртуальные частные сети* можно считать полноценным видом транспорта для передачи трафика, только если есть гарантии на пропускную способность и другие параметры производительности, а также на безопасность передаваемых данных.

Функции VPN по защите данных

Подключение любой корпоративной сети к публичной вызывает два типа угроз:

- несанкционированный доступ к ресурсам локальной сети, полученный в результате входа в эту сеть;
- несанкционированный доступ к данным при передаче трафика по публичной сети.

Для создания защищенного канала средства *VPN* используют процедуры шифрования, аутентификации и авторизации.

Шифрование. Методов шифрования довольно много, поэтому важно, чтобы на концах туннеля использовался один и тот же алгоритм шифрования. Кроме того, для успешного дешифрования данных источнику и получателю данных необходимо обменяться ключами шифрования. Следует отметить, что шифрование сообщений необходимо не всегда. Часто оно оказывается довольно дорогостоящей процедурой, требующей дополнительных приставок для маршрутизаторов, без которых они не могут одновременно с шифрованием обеспечивать приемлемый уровень быстродействия.

Аутентификация. Под аутентификацией понимается определение пользователя или конечного устройства. Аутентификация позволяет устанавливать соединения только между легальными пользователями и, соответственно, предотвращает доступ к ресурсам сети несанкционированных пользователей.

В процедуре участвуют две стороны: одна доказывает свою аутентичность, а другая ее проверяет и принимает решение.

Авторизация. Авторизация подразумевает предоставление абонентам различных видов услуг. Каждому пользователю предоставляются определенные администратором права доступа. Эта процедура выполняется после процедуры аутентификации и позволяет контролировать доступ санкционированных пользователей к ресурсам сети.

Технологии создания виртуальных частных сетей

Среди технологий построения *VPN* можно назвать такие технологии, как: *IPSec VPN*, *MPLS VPN*, VPN на основе технологий туннелирования PPTP и L2TP. Во всех

перечисленных случаях трафик посылается в сеть провайдера по протоколу IP, что позволяет провайдеру оказывать не только услуги *VPN*, но и различные дополнительные сервисы (контроль за работой клиентской сети, хостинг Web и почтовых служб, хостинг специализированных приложений клиентов).

На рис. 13.3 представлен общий вариант построения *виртуальной частной сети* на базе общедоступной сети провайдера. Сеть каждого клиента состоит из территориально распределенных офисов, которые связаны между туннелями, проложенными через сеть провайдера.

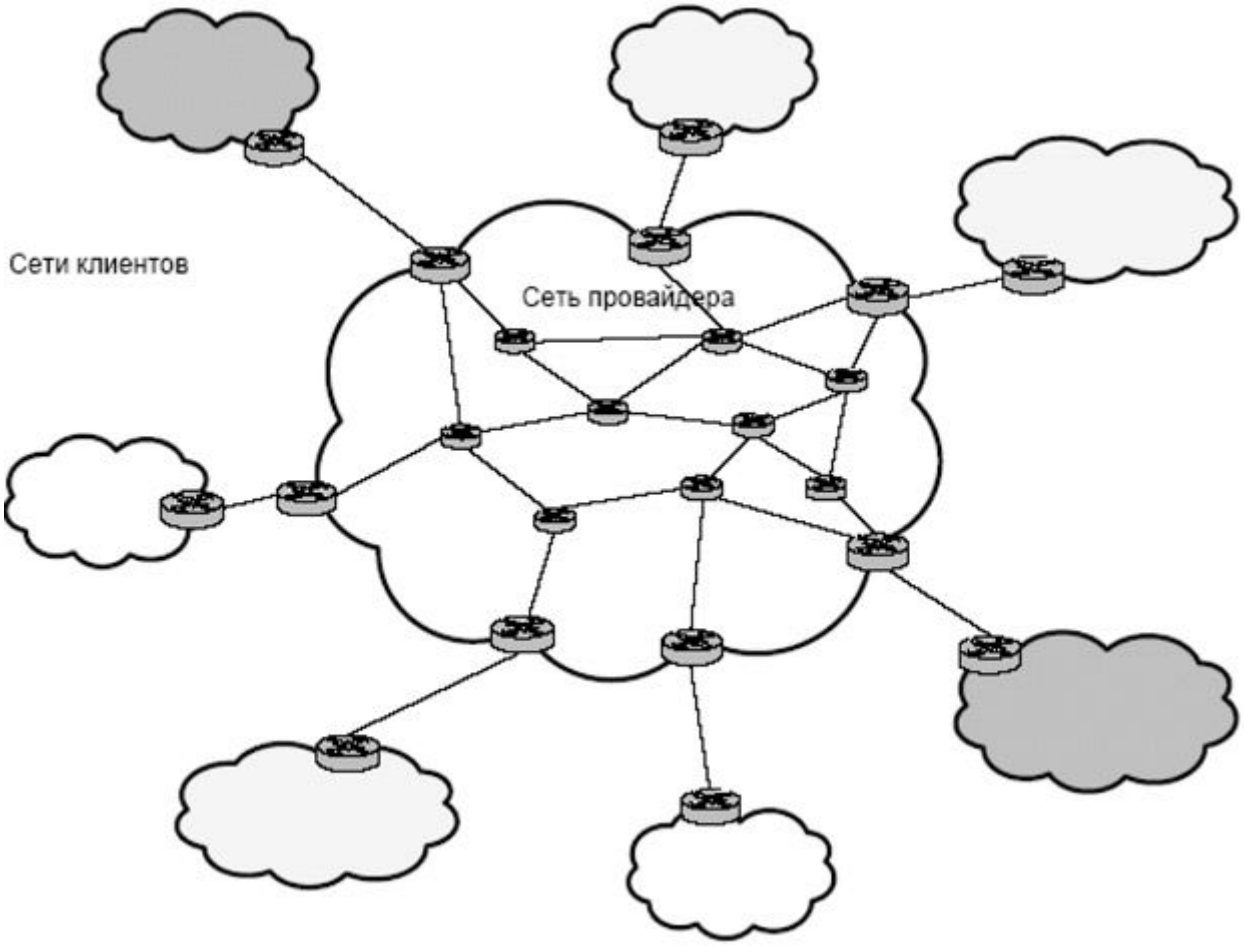


Рис. 13.3. Общий вариант построения виртуальной частной сети

IPSec VPN

Internet Protocol Security относится к наиболее распространенным и популярным технологиям *VPN*. Стандарт *IPSec* обеспечивает высокую степень гибкости, позволяя выбирать нужный режим защиты, а также позволяет использовать различные алгоритмы аутентификации и шифрования данных. Режим инкапсуляции пакетов дает возможность изолировать адресные пространства клиента и провайдера за счет применения двух IP адресов – внешнего и внутреннего.

IPSec, как правило, применяется для создания *VPN*, поддерживаемых провайдером, – туннели в них строятся на базе устройств клиента, но конфигурируются они удаленно и управляются провайдером. Технология *IPSec* позволяет решать следующие задачи по установлению и поддержанию защищенного канала:

- аутентификацию пользователей или компьютеров при инициализации канала;
- шифрование и аутентификацию передаваемых данных между конечными точками канала;
- автоматическое снабжение точек секретными ключами, необходимыми для работы протоколов аутентификации и шифрования данных.

Недостатком данной технологии является тот факт, что из всех свойств виртуальной сети технология *IPSec* реализует только защищенность и изолированность адресного пространства. Пропускную способность и другие параметры QoS она не поддерживает. Кроме того, минусом *IPSec* является и его ориентированность исключительно на IP-протокол.

VPN на основе туннелирования через IP

Сюда входят все технологии для образования VPN, которые используют туннели через IP-сети. Применение туннеля позволяет изолировать адресное пространство клиента, что в свою очередь дает клиенту возможность переносить незашифрованный трафик (L2TP) или шифровать его (PPTP). Протокол PPTP поддерживает управление потоками данных и многопротокольное туннелирование на базе протокола IP. Удаленным пользователям протокол позволяет получать доступ к корпоративной сети, подключаясь по телефонной линии к местному поставщику услуг Интернет вместо прямого подключения к сети компании. PPTP обеспечивает соединение с нужным сервером, создавая для каждого удаленного клиента виртуальную сеть. Протокол решает многие проблемы сетевых администраторов, вынужденных обеспечивать поддержку множества удаленных пользователей, но желающих избежать создания и обслуживания относительно дорогой сети на выделенных каналах.

Спецификации L2TP разрабатывает IETF. Он ориентирован на поддержку многопротокольного туннелирования, но кроме этого обеспечивает совместимость всех L2TP-продуктов. К недостаткам протоколов PPTP и L2TP можно отнести отсутствие встроенных алгоритмов шифрования.

MPLS VPN

Технология MPLS в настоящее время является одной из наиболее перспективных технологий создания VPN.

Использование *MPLS* для построения VPN позволяет сервис-провайдерам быстро и экономично создавать защищенные *виртуальные частныеи сети* любого размера в единой инфраструктуре.

Сеть *MPLS VPN* делится на две области: IP-сети клиентов и внутренняя (магистральная) сеть провайдера, которая служит для объединения клиентских сетей. В общем случае у каждого клиента может быть несколько территориально обособленных сетей IP, каждая из которых в свою очередь может включать несколько подсетей, связанных маршрутизаторами. Такие территориально изолированные сетевые элементы корпоративной сети принято называть сайтами. Принадлежащие одному клиенту сайты обмениваются IP-пакетами через сеть провайдера *MPLS* и образуют *виртуальную частную сеть* этого клиента. Обмен маршрутной информацией в пределах сайта осуществляется по одному из внутренних протоколов маршрутизации IGP. Структура *MPLS VPN* предполагает наличие трех основных компонентов сети:

- Customer Edge Router, CE – пограничный маршрутизатор клиента (Edge LSR в терминологии *MPLS*);
- Provider Router, P – внутренний маршрутизатор магистральной сети провайдера (LSR в терминологии *MPLS*);
- Provider Edge Router, PE – пограничный маршрутизатор сети провайдера.

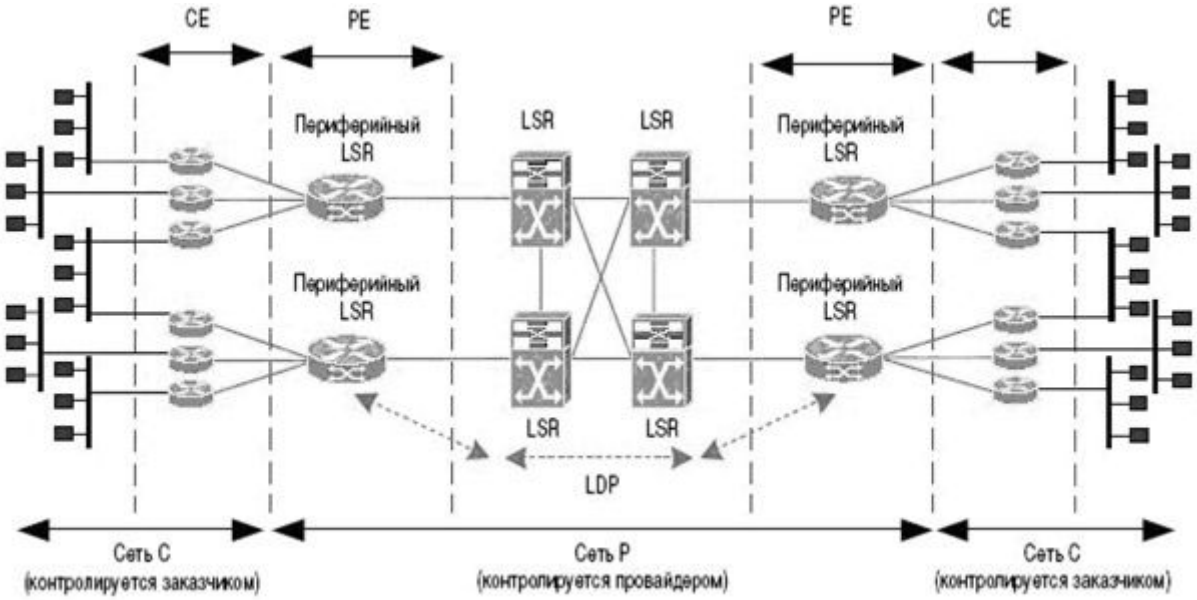


Рис. 13.4. MPLS VPN

Пограничные маршрутизаторы клиента служат для подключения сайта клиента к магистральной сети провайдера. Эти маршрутизаторы принадлежат сети клиента и ничего не знают о существовании *VPN*. CE-маршрутизаторы различных сайтов не обмениваются маршрутной информацией непосредственно и даже могут не знать друг о друге. Адресные пространства подсетей, входящих в состав *VPN*, могут перекрываться, т.е. уникальность адресов должна соблюдаться только в пределах конкретной подсети. Этого удалось добиться преобразованием IP-адреса в *VPN*-IP-адрес и использованием протокола MP-BGP для работы с этими адресами. Считается, что CE-маршрутизатор относится к одному сайту, но сайт может принадлежать к нескольким *VPN*.

К PE-маршрутизатору может быть подключено несколько CE-маршрутизаторов, находящихся в разных сайтах и даже относящихся к разным *VPN*. Маршрутизаторы CE не обязаны поддерживать технологию многопротокольной коммутации, поддержка *MPLS* нужна только для внутренних интерфейсов PE маршрутизаторов и, конечно, для всех интерфейсов маршрутизаторов P. По функциональному построению более сложными являются пограничные маршрутизаторы сети провайдера. На них возлагается функция поддержки *VPN*, а именно, разграничение маршрутов и данных, поступающих от разных клиентов. Кроме того, эти маршрутизаторы служат оконечными точками путей LSP между сайтами заказчика.

Каждый PE-маршрутизатор должен поддерживать столько таблиц маршрутизации, сколько сайтов пользователей к нему подсоединено, то есть на одном физическом маршрутизаторе организуется несколько виртуальных. Причем маршрутная информация, касающаяся конкретной *VPN*, содержится только в PE маршрутизаторах, к которым подсоединены сайты данной *VPN*. Таким образом решается проблема масштабирования,

неизбежно возникающая в случае наличия этой информации во всех маршрутизаторах сети оператора. Под каждый новый сайт клиента PE создает отдельную ассоциированную таблицу маршрутизации. Каждой ассоциированной таблице маршрутизации в маршрутизаторе PE присваивается один или несколько атрибутов RT, которые определяют набор сайтов, входящих в конкретную *VPN*. Помимо этого, маршрут может быть ассоциирован с атрибутом *VPN of Origin*, который однозначно идентифицирует группу сайтов и соответствующий маршрут, объявленный одним из маршрутизаторов этих сайтах; и с атрибутом Site of Origin, идентифицирующим сайт, от которого маршрутизатор PE получил информацию о данном маршруте. Через маршрутизаторы PE проходит невидимая граница между зоной клиентских сайтов и зоной ядра провайдера. По одну сторону располагаются интерфейсы, через которые PE взаимодействует с маршрутизаторами P, а по другую – интерфейсы, к которым подключаются сайты клиентов. С одной стороны на PE поступают объявления о маршрутах магистральной сети, с другой стороны – объявления о маршрутах в сетях клиентов.

Ограничение области распространения маршрутной информации пределами отдельных *VPN* изолирует адресные пространства каждой *VPN*, позволяя применять в ее пределах как публичные адреса Интернет, так и частные (private) адреса.

Всем адресам адресного пространства одной *VPN* добавляется префикс, называемый различителем маршрутов (Route Distinguisher, RD), который уникально идентифицирует эту *VPN*. В результате на маршрутизаторе PE все адреса, относящиеся к разным *VPN*, обязательно будут отличаться друг от друга, даже если они имеют совпадающую часть – адрес IP.

Обмен маршрутной информацией между сайтами каждой отдельной *VPN* выполняется под управлением протокола MP-BGP (Multiprotocol BGP).

MPLS не обеспечивает безопасность за счет шифрования и аутентификации, как это делает *IPSec*, но допускает применение данных технологий как дополнительных мер защиты. Провайдер *MPLS* может предлагать клиентам услуги гарантированного *качества обслуживания* при использовании методов Traffic Engineering или DiffServ.

Виртуальные сети *VPN MPLS* ориентированы на построение защищенной корпоративной сети клиента на базе частной сетевой инфраструктуры одной компании. Данный вариант организации сочетает в себе преимущества применения протокола IP с безопасностью частных сетей и предоставляемым качеством обслуживания, которые дает технология *MPLS*. Сети *MPLS VPN* больше всего подходят для создания корпоративного пространства для электронной коммерции, обеспечивающего единую сетевую среду для подразделений корпорации и организацию экстрасетей. Они также могут стать основой для электронной коммерческой деятельности предприятия.

Применение туннелей для VPN

Протоколы защищенного канала, как правило, используют в своей работе **механизм туннелирования**. С помощью данной методики пакеты данных транслируются через общедоступную сеть как по обычному двухточечному соединению. Между каждой парой "отправитель – получатель данных" устанавливается своеобразный туннель – безопасное логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого.

Технология туннелирования позволяет зашифровать исходный пакет целиком, вместе с заголовком, а не только его поле данных. Такой зашифрованный пакет помещается в другой пакет с открытым заголовком. Этот заголовок используют для транспортировки данных на участке общей сети. В граничной точке защищенного канала извлекается зашифрованный заголовок, который будет использоваться для дальнейшей передачи пакета. Как правило, туннель создается только на участке сети общего пользования, где существует угроза нарушения конфиденциальности и целостности данных. Помимо защиты передаваемой информации, механизм туннелирования используют для обеспечения целостности и аутентичности. При этом защита потока реализуется более полно.

Туннелирование применяется также и для согласования разных транспортных технологий, если данные одного протокола транспортного уровня необходимо передать через транзитную сеть с другим транспортным протоколом. Следует отметить, что процесс туннелирования не зависит от того, с какой целью он применяется. Сам по себе механизм туннелирования не защищает данные от несанкционированного доступа или от искажений, он лишь создает предпосылки для защиты всех полей исходного пакета. Для обеспечения секретности передаваемых данных пакеты на транспортном уровне шифруются и передаются по транзитной сети.

Сравнительный анализ туннелей MPLS и обычных туннелей

Туннели *MPLS* позволяют передавать данные любого протокола вышестоящего уровня (например IP, IPX, кадры Frame Relay, ячейки ATM), так как содержимое пакетов вдоль всего пути следования пакета остается неизменным, меняются только метки. В отличие от них, туннели *IPSec* поддерживают передачу данных только протокола IP, а протоколы PPTP и L2TP позволяют обмениваться данными по протоколам IP, IPX или Net BEUI. Безопасность передачи данных в *MPLS* обеспечивается за счёт определённой сетевой политики, запрещающей принимать пакеты, снабжённые метками, и маршрутную информацию VPN-IP от непроверенных источников. Она может быть повышена использованием стандартных средств аутентификации и/или шифрования (например шифрование *IPSec*). Для безопасной передачи данных в протокол IP Security включены определенные процедуры шифрования IP-пакетов, аутентификации, обеспечения защиты и целостности данных пр и транспортировке, вследствие чего туннели *IPSec* обеспечивают надежную доставку информационного трафика. Протокол L2TP поддерживает процедуры аутентификации и туннелирования информационного потока, а PPTP помимо данных функций снабжен и функциями шифрования. Применение меток *MPLS* позволяет реализовать ускоренное продвижение пакетов по сети провайдера. Транспорт *MPLS* не считывает заголовки транспортируемых пакетов, поэтому используемая в этих пакетах адресация может носить частный характер. Содержимое пакетов не считывается и при передаче IP-пакетов по протоколам *IPSec*, PPTP и L2TP. Однако, в отличие от *MPLS*, традиционные протоколы туннелирования для транспортировки IP-пакетов используют традиционную IP-маршрутизацию. При выборе пути следования пакета в *MPLS* учитываются различные параметры, оказывающие влияние на выбор маршр ута. Совместная работа технологии многопротокольной коммутации и механизмов Traffic Engineering позволяет для каждого туннеля LSP предоставить требуемый уровень качества обслуживания за счет процедуры резервирования ресурсов на каждом маршрутизаторе вдоль пути следования пакета. Помимо этого, появляется возможность отслеживать действительный маршрут, проходящий через сформированный туннель, возможность диагностики и административного контроля туннелей LSP. Различные туннели, в соответствии с необходимым уровнем QoS между двумя точками поддерживает и протокол L2TP.

Технология *VPN IPSec* не поддерживает параметров качества обслуживания установленного соединения, а протокол PPTP поддерживает единственный туннель между двумя точками. Нельзя не отметить и тот факт, что весь трафик при использовании традиционных IP-туннелей следует до адресата вдоль одного и того и того же пути. Технология *MPLS* позволяет контролировать потоки, передаваемые по множеству всех имеющихся путей до адресата. Стоит отметить, что ни одна из рассматриваемых технологий не поддерживает многоадресную рассылку, но для MPLS-TE она находится в разработке. *MPLS VPN* может быть создана для поддержки критически важных приложений на круглосуточной основе. В этом случае провайдер услуг определяет фиксированный путь на срок контракта с пользователем. В случаях сбоя или отсутствия пропускной способности приоритет отдается более важным потокам (с более высоким приоритетом). Одна из функций *MPLS* — объединение виртуальных каналов, когда несколько туннелей *MPLS* объединяются для создания единого туннеля. Такая структура распространяет *VPN* на базе MPLS в сети оператора на сеть внутри офиса и прямо до сервера или клиента. При подобном расширении *VPN* оператору может быть предоставлена ответственность по управлению для обеспечения непрерывного контроля за CoS из конца в конец.

Лекция 14. IMS (IP Multimedia Subsystem)

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.

Ключевые факторы перехода к IMS

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.

Как известно, 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.

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*.

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. 14.1).

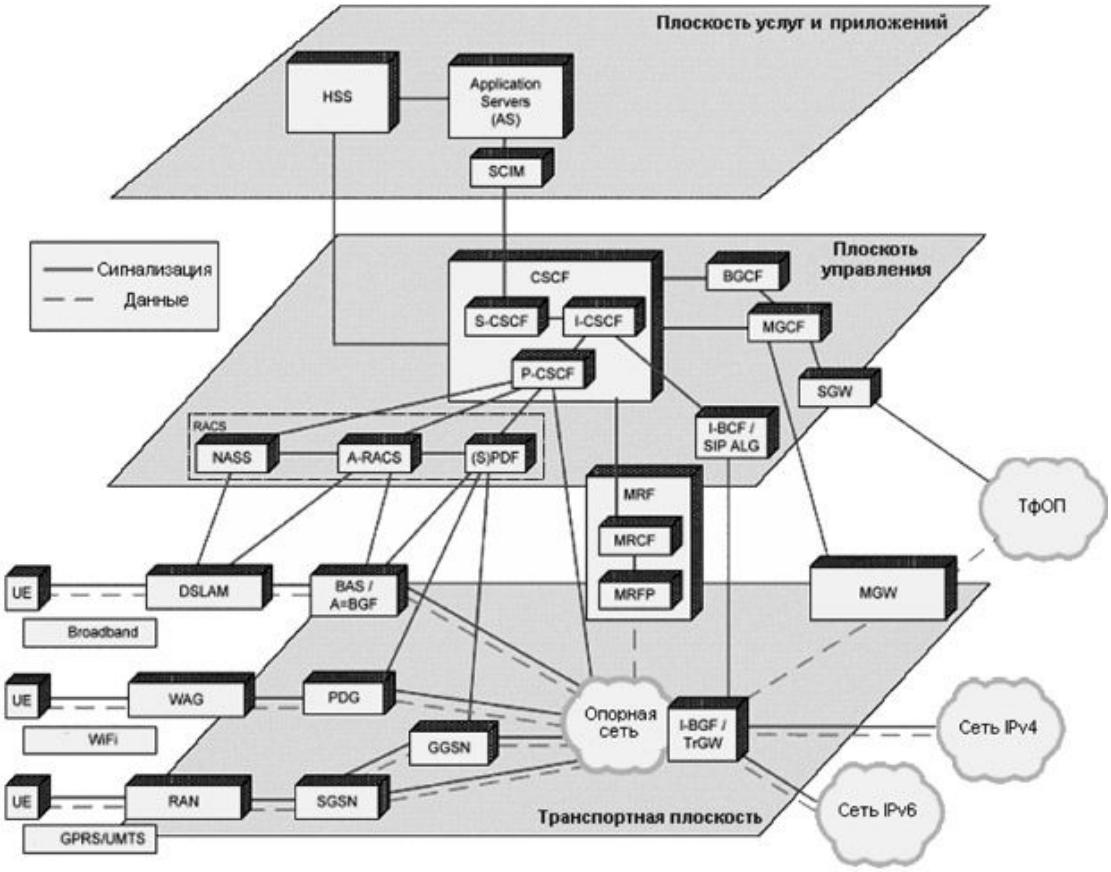


Рис. 14.1. Архитектура IMS

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);
- **I-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*;
- **A-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.;
- **I-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.

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.

Различия

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.

Лекция 15. Техническое описание телекоммуникационного оборудования и комплектующих частей сети сотовой связи стандарта GSM M900/M1800

1. Функциональные блоки базовой станции BTS 312 M900/1800 и их назначение.

Основное оборудование.

Базовая станция состоит из следующих блоков:

Шкаф GM-BTSM-RACK - стандартный шкаф размером 1880X650X500 мм, включает в себя внутренние кабели и материнскую плату. Шкаф сделан из сплава алюминия, служит для размещения в нем блоков:

1.1 CDU GM-CDUM – комбайнер базовой станции, необходим для объединения сигналов нескольких передатчиков на одну антенну, а также для деления приемного сигнала от одной антенны на несколько передатчиков.

1.2 TRX GM-TRXM – приемопередатчик базовой станции, служит для преобразования сигналов одного протокола передачи информации в другой, осуществляет прием и передачу информации в радио эфире, обеспечивает модуляцию, демодуляцию радио сигналов и т. д.

1.3 TMU GM-TMU – устройство передачи и контроля информации, обеспечивает стандартный интерфейс E1 для связи с контроллером базовых станций (BSC), мультиплексирование и демультиплексирование сигналов, синхронизацию станции.

1.4 PSU GM-PSU-DC– блок питания станции, преобразует входное напряжение одного номинала в выходное напряжение другого номинала.

1.5 PMU GM-PMU – устройство управления электропитанием станции, осуществляет контроль PSU блоков.

1.6 TDU – устройство распределения синхросигналов, представляющую собой плату, вмонтированную внутри верхней части шкафа BTS.

1.7 Панель выключателей, вмонтирована в верхней части шкафа.

1.8 FMU – блок вентиляторов, обеспечивает охлаждение блоков и циркуляцию воздуха внутри шкафа.

Функциональное взаимодействие блоков и узлов показано на рис.15. 2.

Конструктивное исполнение станции модульное, т. е. все вышеперечисленное оборудование представляет собой вставные блоки, количество которых зависит от требований к пропускной способности базовой станции.

Дополнительное оборудование.

Дополнительным оборудованием для базовой станции включает в себя следующее:

1.9 Jumper GM-JMP-1 – переходной радиочастотный кабель, соединяющий основной фидер и радио часть базовой станции рис.15. 11)

1.10 Lightning Protection Kit ETS-BLQ2 – устройство молниезащиты, предотвращающее повреждение деталей блоков базовой станции в результате попадания молниеразряда на оборудование станции.

1.11 BTS Installation Bracket GM-BTS-TR – подставка для базовой станции.

1.12 Grounding Hardware GM-HAW-GND – основное заземление.

1.13 120ohm E1 Trunk Cable,DB37 Male CB-EDLA120-10-DB37 – соединительный передающий кабель, обеспечивающий стандартный поток E1 от оборудования трансмиссии до базовой станции.

1.14 Fireproof Electricity-Feeding Wire (-48V/20m) GM-ZRDL48V-20m – Огнеупорный силовой питающий кабель (-48В), монтируется между аккумуляторными батареями и стойкой питания.

1.15 Fireproof Electricity-Feeding Wire (GND/20m) GM-ZRGND-20m – огнеупорный кабель для заземления оборудования.

1.16 Fireproof Electricity-Feeding Wire (PGND/20m) – огнеупорный кабель для основного заземления.

1.17 Jumper Connector DIN GM-JMP-CON-DIN – разъем для радио кабеля (рис. 15.10)

1.18 Lightning Protection Kit-TR ANT GM-LGT-PRT-TR – комплект молниезащиты.

Комплектация станции.

Основное оборудование.

№	Наименование блока	Пояснение	Комплектность	Примечания
1	GM-BTSM-RACK	BTS Rack（MAX:6）	1	
2	GM-PSU-DC	Power Supply Unit (HM48S24/700)	От 2 до 4	В зависимости от емкости станции
3	GM-PMU	Power Management Unit	1	1
4	GM-TMU	Transmission Management Unit	1	1
5	GM-TRXM	Transceiver Unit	От 1 до 12	В зависимости от емкости станции
6	GM-CDUM	Combining And Distribution Unit	От 1 до 6	В зависимости от емкости станции

Дополнительное оборудование.

	Наименование	Пояснение	Комплектность	Примечания
	GM-JMP-1	Jumper (m)	10	Из расчета 6 jumpers на 1 БТС
	ETS-BLQ2	Lightning Protection Kit	1	
	GM-BTS-TR	BTS Installation Bracket	1	
	GM-HAW-GND	Grounding Hardware	2	
	CB-EDLA120-10-DB37	120ohm E1 Trunk Cable,DB37 Male	2	
	GM-ZRDL48V-20m	Fireproof Electricity-Feeding Wire (-48v/20m)	1	
	GM-ZRGND-20m	Fireproof Electricity-Feeding Wire (GND/20m)	1	
	GM-ZRGND-20m	Fireproof Electricity-Feeding Wire (PGND/20m)	1	
	GM-JMP-CON-DIN	Jumper Connector DIN	От 4 до 12	В зависимости от емкости станции
	GM-LGT-PRT-TR	Lightning Protection Kit-TR ANT	2	

2. Оборудование электропитания, входящая в состав БТС.

Для обеспечения базовой станции электропитанием определенных параметров в комплект BTS входит также стойка питания и аккумуляторные батареи.

Стойка питания, также как и сама станция имеет модульную структуру и представляет собой шкаф RACK-300/25, в который входят:

2.1 Модуль контроля PSM-15 – осуществляет функцию контроля и проверки рабочих параметров стойки питания.

2.2 Преобразователи HD4825 – устройство преобразования тока переменного напряжения в постоянное, другого номинала.

2.3 Распределительная панель питания переменного тока ZR-RVVZ3*50+1*25.

2.4 Распределительная панель питания постоянного тока ZR-RVVZ50.

2.5 Кабель заземления ZR-RVVZ50 – используется для заземления оборудования.

2.6 Питающий кабель имеет тот же самый тип, что и кабель заземления.

Комплектация стойки питания.

Основное оборудование

№	**наименование**	Пояснение	Комплектность	Примечания
1	RACK-300/25	Rectifier Rack (AC & DC Distribution Shelf)	1	
2	PSM-15	Monitoring Module	1	
3	HD4825	Rectifier Module	От 2 до 6	В зависимости от емкости станции

Дополнительное оборудование

№	**наименование**	Пояснение	Комплектность	Примечания
7	ZR-RVVZ3*50+1*25	AC Switching Board To AC Distributor	20 m	
8	ZR-RVVZ50	Battery To DC Distributor	40 m	
9	ZR-RVVZ50	DC Distributor To Equipment	20 m	
10	ZR-RVVZ50	Earth Cable	20 m	

3. Описание вспомогательного оборудования.

3.1 Специальный радиочастотный разъем для переходного кабеля БТС (специальный коннектор) 7/16 DIN: монтируется на обоих концах соединительного радио кабеля. Служит для его соединения между основным фидером и базовой станцией. См. рис. 10 в приложении.

3.2 Устройство молниезащиты: срабатывает при попадании разряда молнии. Имеет следующие характеристики - максимальный выдерживаемый импульс: однократный 40kA, длительностью не более 8/20 с, номинальное значение: до двадцати импульсов 20kA, длительностью 8/20 с, габаритные размеры: 150 × 55 × 60 мм.

3.3 Распределительная коробка (коробка кросса) DDF box: применяется для расшивки 2-Мбит потока. Имеет габаритные размеры 350X240X116 мм, вес 4.4 кг. Внутри расположена коммутационная колодка с предохранителями, используется для расшивки

2-Мбит потока. Внешний вид DDF-box на рис.15. 9. Комплектность – на 1 БТС одна распределительная коробка (количество распределительных колодок внутри DDF – одна).

3.4 Аварийная панель (Alarm box): применяется для сбора и передачи аварийной информации, получаемой с сенсоров (инфракрасный сенсор, датчик огня и дыма, датчик влажности и т. п.). Габаритные размеры 270X65X380 мм.

3.5 Питающий кабель:

3.6 Комплектация ящика с инструментами:

	Инструменты, в том числе:		
1	комплект инструментов, в том числе:	1	шт.
	- нож для резки кабеля	1	шт.
	- инструмент для разделки фидера	1	шт.
2	комплект инструментов, в том числе:	1	шт.
	- удлинитель электрический 2м	1	шт.
	- молоток	1	шт.
	- молоток с гвоздодером на деревянной ручке	1	шт.
	- уровень 450мм	1	шт.
	- устройство для снятия изоляции	2	шт.
	- уровень с поворотным механизмом	1	шт.
	- ножевка по металлу	1	шт.
	- полотно для ножевки по металлу	3	шт.
	- торцовый ключ в футляре	1	шт.
	- комплект в футляре: торцовый ключ с 37 головками и отвертка	1	шт.
	- инструмент для обжимки наконечников на кабелях	1	шт.
	- надфили в чехле	10	шт.
	- дискеты 3,5” в пластиковом футляре	10	шт.
	- ручка-фломастер – фонарик	1	шт.
	- тестер VC890C+tm с проводами и наконечниками	1	шт.
	- компас в металлическом корпусе	1	шт.
	- рулетка 5м	1	шт.
	- фен SPEED 1600W	1	шт.
	- бухточка свинцового припоя	1	шт.
	- паста SOLPERING в металлической коробке 100гр.	1	шт.
	- разводные ключи	5	шт.
	- плоскогубцы	1	шт.
	- круглогубцы	1	шт.
	- кусачки	1	шт.
	- кисть 38,1мм	1	шт.
	- специальные ножницы	1	шт.
	- разводной ключ SZNTUS 10	1	шт.
	- торцевые ключи в упаковке	1	шт.
	- приспособление для обжима сетевых коллекторов	1	шт.
	- канцелярский нож	1	шт.
	- комплект запасных лезвий для ножа 10шт.	2	шт.
	- маркер	1	шт.
	- моток изоленты	1	шт.
	- отвертки	8	шт.
	- гаечные ключи	2	шт.
	- батарейки	4	шт.
	- металлический пинцет	2	шт.

	- паяльник 220В	1	шт.
	- перфоратор в пластиковом чемоданчике, там же:	1	шт.
	- буры	6	шт.
	- сверла	4	шт.
	- сменная головка для перфоратора	1	шт.
	- ключ к головке	1	шт.
	- ручной гидравлический пресс	1	шт.
	- насадки к прессу	20	шт.

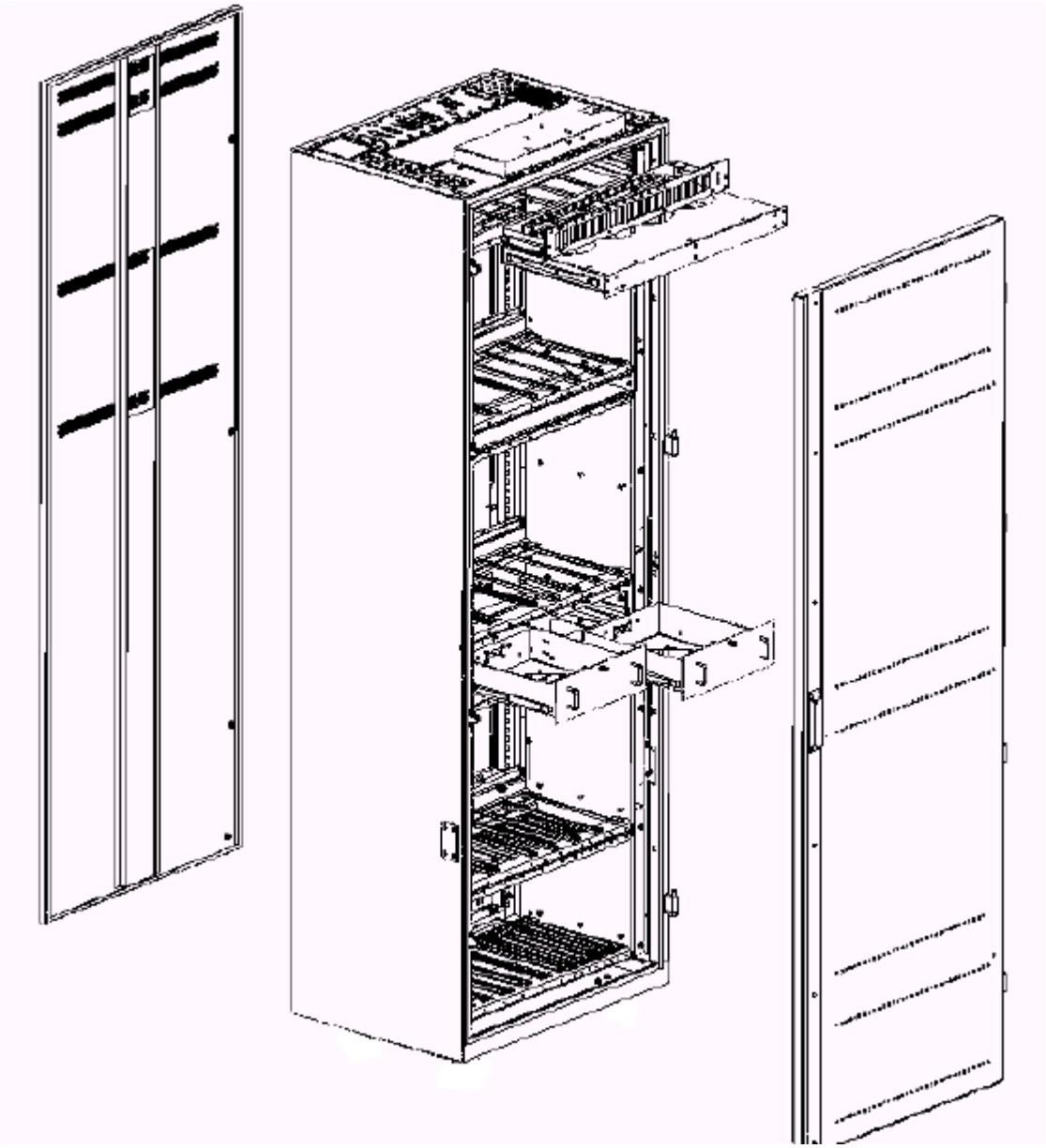


Рис.15.1. Шкаф базовой станции BTS 312 M900/1800.

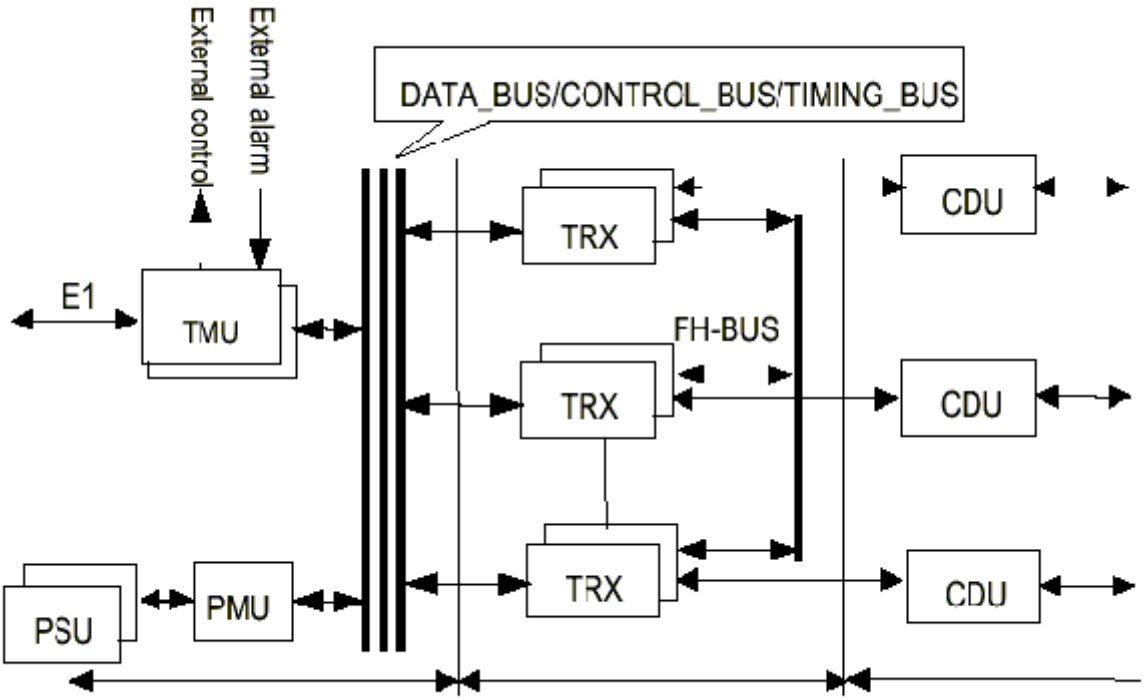


Рис. 15.2. Структура базовой станции

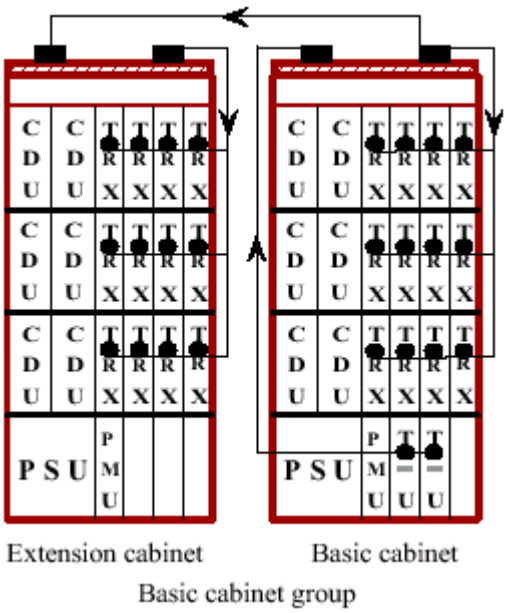


Рис.15.3. Схема поблочного размещения оборудования базовой станции.

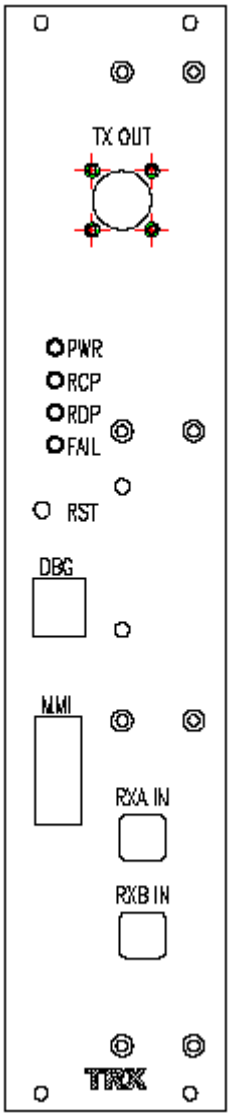


Рис. 15.4. Внешний вид приемопередатчика.

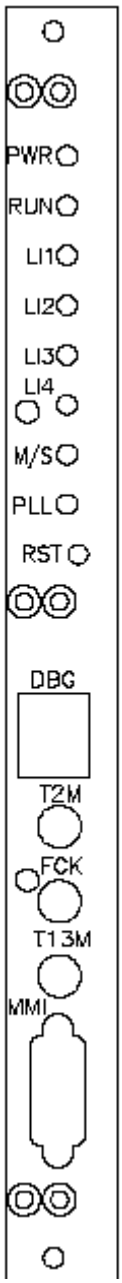


Рис.15.5 . Внешний вид платы TMU.

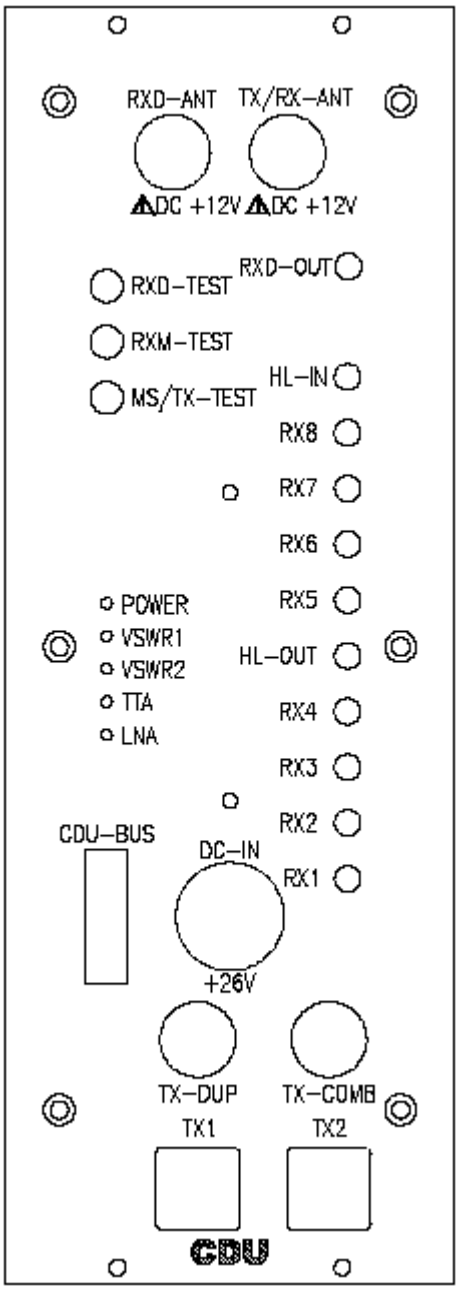


Рис.15.6. Внешний вид блока CDU.

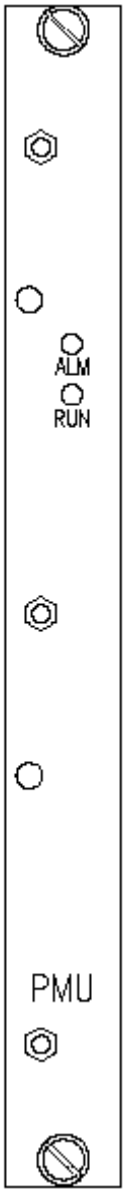


Рис.15.7. Внешний вид блока PMU.

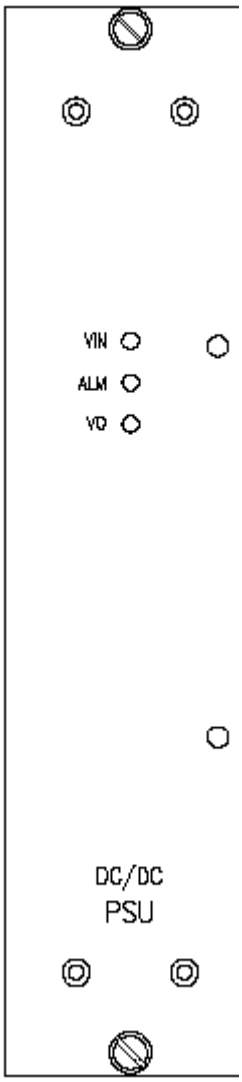


Рис.15.8. Внешний вид блока PSU.

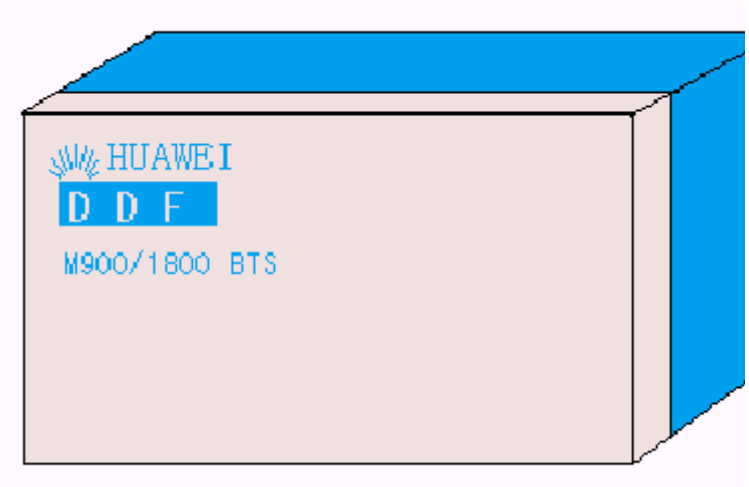


Рис.15.9. Внешний вид кроссовой коробки

Рис. 15.10. Внешний вид специального разъема
для RF переходного кабеля

Рис.15.11. Внешний вид переходного кабеля

Литературные источники

1.Гулевич Д. С. **Сети связи следующего поколения**. БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий – www.intuit.ru

2.Новиков Ю.В., Кондратенко С.В. **Основы локальных сетей**. Интернет-университет информационных технологий - www.intuit.ru

3.Олифер В.Г., Олифер Н.А. **Основы сетей передачи данных**. Интернет-университет информационных технологий - www.intuit.ru