

## Сети связи (часть 2)

### Лекция 9.

#### Концепция сети следующего поколения NGN

##### 9.1 Предпосылки появления NGN

В настоящее время связь превратилась в бурно развивающуюся отрасль, приносящую операторам значительную прибыль.

Пользователи получили доступ к новым услугам: E-mail, Интернет, сотовый телефон стали обычными атрибутами повседневной жизни. 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, так как 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.

Это привело к тому, что в настоящее время происходит стремительное развитие телекоммуникационных услуг, имеющее следующие особенности:

1. Снижается объем предоставляемых речевых услуг, а объем услуг передачи данных быстро растет, в некоторых странах (США) он превысил объем речевых услуг.

2. Развитие сети Интернет, рост ее пропускной способности и надежности, улучшение эксплуатационных характеристик сделали возможным предоставление речевых услуг на базе Интернет.

3. Сети ПД с коммутацией пакетов, сливаются с ССОП с коммутацией каналов.

##### 9.2 Требования к сетям связи

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

- мультисервисность, под которой понимается независимость технологий предоставления услуг от транспортных технологий;

- широкополосность - это возможность гибкого и динамического изменения скорости передачи информации в широком диапазоне в зависимости от текущих потребностей пользователя;

- мультимедийность - это способность сети передавать многокомпонентную информацию (речь, данные видео, аудио) с необходимой синхронизацией этих компонент в реальном времени и использованием сложных конфигураций соединений;

- интеллектуальность - это возможность управления услугой, вызовом и соединением со стороны пользователя или поставщика услуг;

- инвариантность доступа - это под которой понимается возможность организации доступа к услугам независимо от используемой технологии;

- многооператорность, возможность участия нескольких операторов в процессе предоставления услуги и разделение их ответственности и доходов в соответствии с областью деятельности.

При этом необходимо учитывать особенности деятельности поставщиков услуг. В частности, современные подходы к регламентации услуг 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.

### **9.3 Определение NGN**

Эти условия развития телекоммуникации привели к созданию концепции NGN.

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.

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

В рекомендациях International Telecommunication Unit (ITU-T) дано следующее определение NGN (Next Generation Network): "NGN – это сеть с коммутацией пакетов, способная предоставлять телекоммуникационные услуги посредством широкополосных транспортных технологий, поддерживающих качество обслуживания, и в которой функции услуг не зависят от используемых транспортных технологий".

NGN, которая потенциально должна объединить существующие сети связи (сети связи общего пользования – ССОП, 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 NGN, обладают следующими преимуществами перед традиционными сетями электросвязи.

С точки зрения оператора:

- построение одной универсальной сети для оказания различных услуг;
- повышение среднего дохода с абонента за счет оказания дополнительных мультимедийных услуг;
- оператор NGN может наиболее оптимально реализовывать полосу пропускания для интеграции различных видов трафика и оказания различных услуг;
- NGN лучше приспособлена к модернизации и расширению;
- NGN обладает легкостью в управлении и эксплуатации;
- оператор NGN располагает возможностью быстрого внедрения новых услуг и приложений с различным требованием к объему передаваемой информации и качеству ее передачи.

С точки зрения пользователя:

- абстрагирование от технологий реализации услуг электросвязи (принцип черного ящика);
- гибкое получение необходимого набора, объема и качества услуг;
- мобильность получения услуг.

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

NGN представляет собой универсальную многоцелевую сеть, предназначенную для передачи речи, изображений и данных с использованием технологии коммутации пакетов. По сути, NGN является результатом слияния Internet и телефонных сетей, объединяя в себе их лучшие черты. На практике это означает гарантированное качество голосовой связи и передачи данных в критически важных приложениях. Таким образом, NGN имеет степень надежности, характерную для ТфОП (в противоположность негарантированному качеству связи через Internet) и обеспечивает низкую стоимость передачи в расчете на единицу объема информации (приближенную к стоимости передачи данных по Internet, а не ТфОП).

Концепция NGN предусматривает поддержку неограниченного набора услуг с гибкими возможностями по их управлению, реализацию универсальной транспортной мультипротокольной сети с распределенной коммутацией, интеграцию с традиционными сетями связи.

Особенностью сетей NGN является то, что передача и маршрутизация пакетов и элементы оборудования передачи (каналы, маршрутизаторы, коммутаторы, шлюзы) физически и логически отделены от устройств и логики управления вызовами и услугами.

Используемая в сети логика поддерживает все типы услуг в сети с коммутацией пакетов, начиная от базовой телефонной связи и заканчивая передачей данных, изображений, мультимедийной информации, широкополосными приложениями и приложениями управления.

Указанные особенности отличают сети NGN от обычных телефонных и IP-сетей, наиболее широко распространенных в мире телекоммуникаций.

NGN обеспечивает свободный доступ для пользователей к любым сетям и конкурирующим поставщикам услуг, или службам (услугам).

Сети NGN обладают следующими характеристиками:

1. Передача с пакетной коммутацией.
2. Разделение функций управления между пропускной способностью канала – носителя, вызовом/сеансом, а также приложением/услугой.
3. Развязка между предоставлением услуг и транспортировкой и предоставлением открытых интерфейсов.
4. Поддержка широкого спектра услуг на основе унифицированных блоков обслуживания, включая услуги в реальном масштабе времени, в потоковом режиме, в автономном режиме и мультимедийные услуги.
5. Возможность широкополосной передачи со сквозной функцией качества обслуживания.
6. Взаимодействие с существующими сетями с помощью открытых интерфейсов.

7. Универсальная мобильность NGN.
8. Неограниченный доступ пользователей к разным поставщикам услуг.
9. Разнообразие схем идентификации.
10. Единые характеристики обслуживания для одной и той же услуги с точки зрения пользователя.
11. Сближение услуг между фиксированной и подвижной связью.
12. Независимость функций обслуживания от технологий транспортировки.
13. Поддержка различных технологий «последней мили».
14. Выполнение всех регламентных требований для аварийной связи, защиты информации, конфиденциальности, законного перехвата и т.д.
15. Адаптируемость для передачи трафика любого вида.
16. Гарантированное качество голосовой связи и критически важных приложений передачи данных.
17. Низкая стоимость передачи в расчете на единицу объема информации приближается к стоимости передачи данных в сети Интернет (общий объем трафика данных и голосового трафика в сети Интернет каждый год утраивается).

Сети NGN базируются на интернет-технологиях, включающих в себя IP протокол и технологию MPLS, а на высшем уровне-SIP протокол, заменяющий ITU-T H.323. Изначально предпочтение отдавалось протоколу H.323, но затем более широкое применение стал получать протокол SIP. На данный момент протокол SIP широко применяется для предоставления VoIP услуг. Основным устройством для голосовых услуг в сетях NGN является Softswitch — так называется программный коммутатор, который управляет VoIP сессиями. Также немаловажной функцией программного коммутатора является связь сетей следующего поколения NGN с существующими традиционными сетями связи общего пользования (ССОП), посредством сигнального (SG) и медиа-шлюзов (MG), которые могут быть выполнены в одном устройстве.

## Лекция 10. Архитектура NGN

В настоящее время наибольшее распространение получила четырехуровневая архитектура NGN (рисунок 10.1):



Рисунок 10.1 - Архитектура сети следующего поколения NGN

Архитектура NGN содержит следующие уровни:

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

### 10.1 Уровень управления услугами

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 работу других уровней.

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

Уровень управления услугами содержит:

- сервер приложений;
- сервер дополнительных услуг;
- интегрированную систему поддержки эксплуатации;
- сервер политик;
- сервер локализации;
- сервер медиаресурсов;
- устройства организации конференций;
- пункт управления услугами.

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 - открытый сервисный доступ) – 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:

- 1) открытая среда для создания услуг;
- 2) 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 (*переговорная группа*), который занимается созданием спецификаций открытого API (Application Programming Interface - *обращение международного планирования*), позволяющего управлять сетевыми ресурсами и получать доступ к сетевой информации.

Архитектура Parlay является одной из практических реализаций концепции OSA (рисунок 10.2).

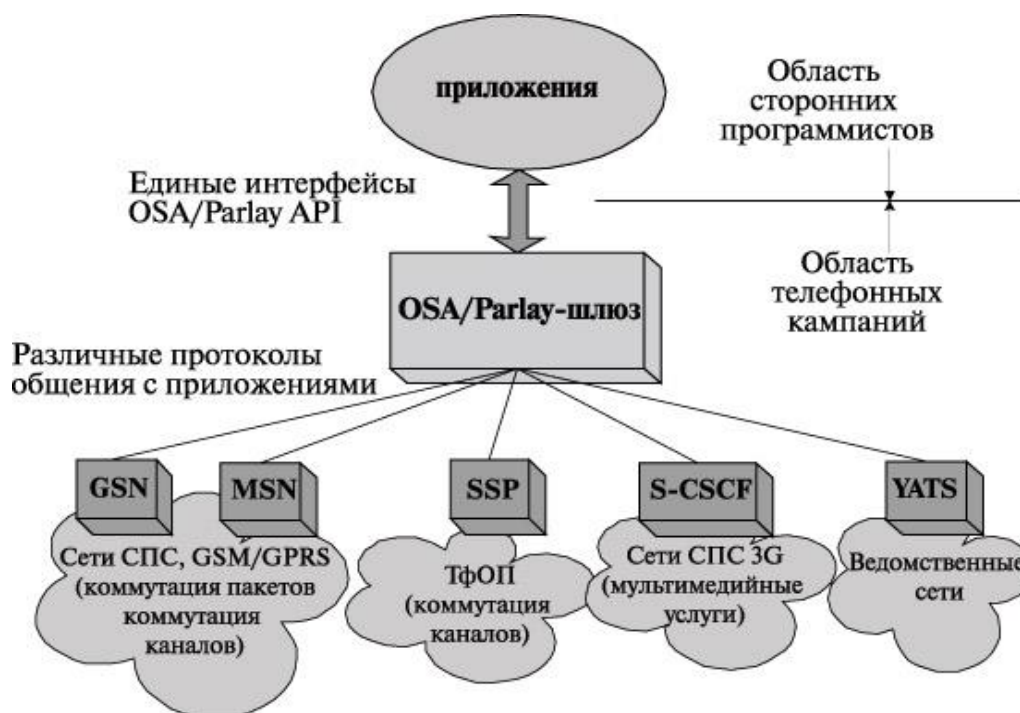


Рисунок 10.2 - Архитектура Parlay

Как показано на рисунке 10.2, 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.

Оказалось, что концепция Parlay является слишком сложной для массового привлечения сторонних программистов. Выяснилось, что для оказания 80% услуг требуется лишь 20% возможностей Parlay-шлюза.

## 10.2 Уровень управления коммутацией

Уровень управления коммутацией включает в себя совокупность всех функций по управлению процессами передачи информации в сети NGN, функции тарификации и начисления оплаты, функции технической эксплуатации.

В настоящее время существует 2 основных подхода для реализации данного уровня:

- 1 - решение на базе гибкого коммутатора Softswitch,
- 2 - решение на базе мультимедийной IP-подсистемы IMS (IP Multimedia Subsystem).

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.

### 10.3 Транспортный уровень

Задача транспортного уровня — коммутация и прозрачная передача информации пользователя. Основой этого уровня считается технология ATM или IP/MPLS.

В NGN операторы получают 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.
- поддержка соединений в реальном времени и соединений, не чувствительных к задержкам;
- гибкость – с точки зрения передачи самого разнородного трафика;
- высокая эффективность использования ресурсов сети;
- стабильность и управляемость работы транспортной сети.

Надежность выходит на первое место, так как NGN 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.

МСЭ-T 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.

В состав транспортной сети NGN могут входить:

- транзитные узлы, выполняющие функции переноса и коммутации;
- конечные (граничные) узлы, обеспечивающие доступ абонентов к сети NGN;
- контроллеры сигнализации, выполняющие функции обработки информации сигнализации, управления вызовами и соединениями;
- шлюзы, позволяющие осуществить подключение традиционных сетей (ТфОП, СПД, СПС, ISDN и др.).

К оборудованию транспортной сети NGN так же, как и к самим транспортным сетям, предъявляются требования:

- восстановление после отказа должно происходить за время, не превышающее 50 мс.
- наличие соответствующей поддержки большого числа сервисов;
- наличие равного доступа к сетевым ресурсам, совместно используемым абонентами сети;
- администрирование и обслуживание в процессе эксплуатации;
- резервирование сетевых ресурсов для одного или нескольких сервисов;

- оптимизация использования сетевых ресурсов и трафика.

Транспортный уровень NGN рассматривается как уровень, составными частями которого являются *сеть доступа и базовая сеть*.

*Базовая сеть* – это универсальная сеть, реализующая функции транспортировки и коммутации и базирующаяся на технологиях пакетной коммутации. В соответствии с данными функциями базовая сеть представляется в виде трех уровней (рисунок 10.3):

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

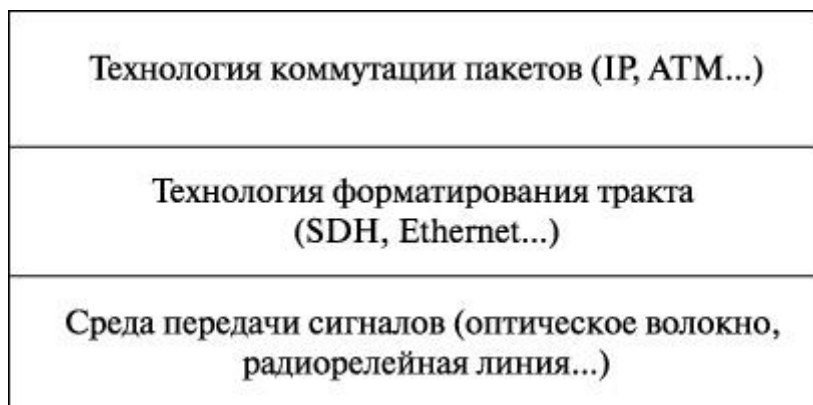


Рисунок 10.3 - Модель базовой сети

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, из-за 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 NGN входят основные составляющие части транспортного уровня: транзитные и оконечные узлы, контроллеры сигнализации, шлюзы для подключения сетей связи общего пользования.

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.



*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 NGN или к традиционным сетям электросвязи).

К сети доступа предъявляются следующие требования:

- рост пропускной способности трактов обмена информацией;
- ужесточение требований к показателям качества обслуживания;
- поддержка функций мобильности терминала и ряда приложений, включая функциональные возможности услуг Triple Play.
- снижение затрат, необходимых для создания и дальнейшего развития всех элементов сети NGN.

#### **10.4 Уровень доступа**

Уровень доступа обеспечивает подключение любых других сетей к сети NGN или непосредственно терминалов пользователей, поддерживающие пакетные технологии. Для сетей и терминалов, не поддерживающих пакетные технологии, подключение осуществляется через медиашлюзы MG. Пакетные терминалы подключаются к сети доступа через интегрированные устройства доступа IAD.

К уровню доступа относятся:

- шлюзы (MG или MAK);
- сеть доступа;
- оконечное абонентское оборудование.

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.

При работе оборудования доступа в сети NGN должны выполняться условия:

- поддержка любой сетевой топологии;
- поддержка различных сред передачи;
- поддержка различных интерфейсов и протоколов связи с ТфОП;
- поддержка различных интерфейсов сетей передачи данных;
- поддержка различных протоколов сети NGN;
- поддержка различных абонентских интерфейсов.

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.

Сеть NGN имеет распределённую архитектуру, в которой связь между компонентами осуществляется исключительно через открытые интерфейсы.

Структура сети электросвязи, построенной в соответствии с концепцией NGN, представлена на рисунке 10.4.

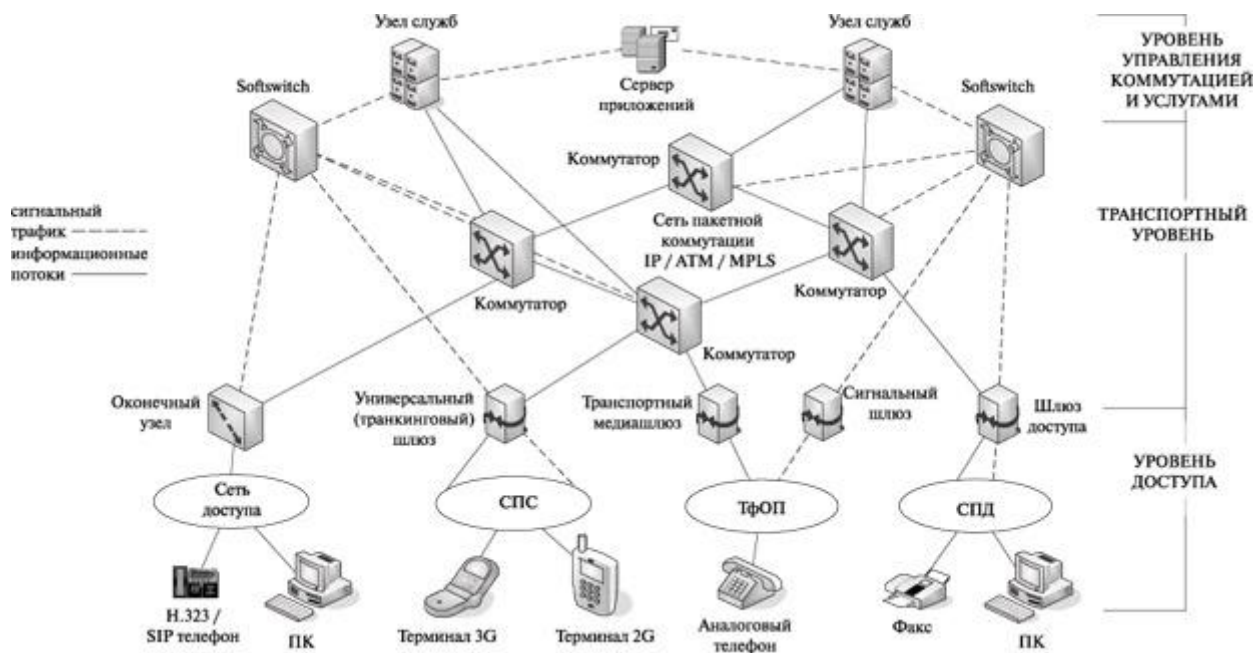


Рисунок 10.4 – Структура NGN

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-T 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.

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

Общая инфраструктура NGN, используемая для предоставления различных услуг, реализуется на транспортном уровне, основанном на пакетной технологии. Обмен информацией между источником и пунктом назначения осуществляется по одному и тому же принципу вне зависимости от вида соединения (телефонный вызов, сеанс работы в интернет, передача видео, сетевая игра с несколькими игроками или трансляция фильма).

Прикладной уровень логически и физически отделен от транспортного уровня, что позволяет независимо развивать различные сегменты сети. За различные услуги (телефонную связь, электронную коммерцию, передачу видео по запросу и т.д.) отвечают различные серверы, отделенные от транспортного уровня. Для внедрения новой услуги необходимо всего лишь добавить новый сервер, который благодаря транспортному уровню становится доступным для всех подключенных к сети пользователей.

Подключение пользователей к NGN производится через интерфейсы с различными полосами частот и пропускной способностью, основанные на различных технологиях. Несмотря на то, что наиболее пригодными для подключения к NGN являются широкополосные интерфейсы (>0,5 Мбит/с), всем пользователям предоставляется универсальный доступ к услугам независимо от используемого ими оборудования.

## Лекция 11.

### Услуги NGN. Классификация услуг для сетей NGN

В рамках концепции, когда сеть NGN предлагается рассматривать не как отдельную категорию сетей связи, а как инструмент построения и развития существующих сетей, услуги, предоставляемые в рамках фрагмента NGN, можно классифицировать следующим образом:

- 1) базовые: услуги, ориентированные на установление соединения с использованием фрагмента NGN между двумя оконечными терминалами;
- 2) дополнительные виды обслуживания: услуги, предоставляемые наряду с базовыми и ориентированные на поддержку дополнительных списков возможностей;
- 3) услуги доступа, ориентированные на организацию доступа к ресурсам, и точек присутствия интеллектуальных сетей и сетей передачи данных;
- 4) информационно-справочные услуги: услуги, ориентированные на предоставление информации из баз данных, входящих в структуру NGN ;
- 5) услуги виртуальных частных сетей: услуги, ориентированные на организацию и поддержание функционирования VPN со стороны элементов фрагмента NGN;
- 6) услуги мультимедиа: услуги, ориентированные на обеспечение и поддержку функционирования мультимедийных приложений со стороны фрагмента NGN.

#### 11.1 Базовые услуги

Под базовыми видами понимаются следующие услуги:

- услуги местной, междугородной, международной телефонной связи, предоставляемые с использованием (полным или частичным) фрагмента сети на основе NGN-технологий. Базовые услуги телефонии в сетях NGN 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 NGN при предоставлении базовых услуг является установление и поддержание соединения с требуемыми параметрами.

#### 11.2 Дополнительные виды обслуживания (ДВО)

Предоставление базовых услуг может сопровождаться дополнительными видами обслуживания, которые расширяют возможности пользователя по получению информации о соединении, тональных уведомлений, а также позволяют изменять конфигурацию соединения. В сетевом фрагменте NGN пользователям могут быть доступны следующие дополнительные виды обслуживания:

- идентификации вызывающей линии (CLIP);
- запрет идентификации вызывающей линии (CLIR);
- предоставление идентификации подключенной линии (COLP);
- безусловная переадресация вызова (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 дополнительные услуги.

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 NGN для проходящих через него вызовов должен обеспечивать поддержку ДВО, инициированных в других сетях.

### **11.3 Услуги доступа**

Услугами доступа, поддерживаемыми со стороны сетевого фрагмента NGN, 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 IN с реализацией функции SSP в сетевом фрагменте NGN. Реализованный SSP на ЕСЭ РФ должен как минимум обеспечивать поддержку следующих видов интеллектуальных услуг:
  - "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).

### **11.4 Информационно-справочные услуги**

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

### **11.5 Услуги VPN**

Фрагментом NGN 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 NGN 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.

## 11.6 Услуги мультимедиа

Мультимедийные услуги можно рассматривать с двух позиций:

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

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

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

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

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

Классификацию мультимедийных услуг связи и предложений 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.

Одной из основных целей построения NGN является расширение спектра предоставляемых услуг:

- услуги службы телефонной связи (предоставление местного телефонного соединения, междугородного 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, NGN будут поддерживать как уже существующее, так и новое окончательное 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 NGN используют различные способы кодирования и передачи и включают в себя: многоадресную и ширококвещательную передачу сообщений, передачу чувствительного и нечувствительного к задержкам трафика, услуги обычной передачи данных, услуги реального масштаба времени, диалоговые услуги.

### **11.7 Передача речи по сетям передачи данных**

Главной среди расширенного спектра услуг является доставка речи по сетям передачи данных. IP позволяет делать это экономичнее и более гибко, чем оказание таких услуг по современной телефонной сети общего пользования (ТфОП).

Всё большую популярность приобретают голосовые услуги, к организации сеансов связи в которых операторы связи не имеют прямого отношения. Самым известным, но отнюдь не единственным примером является служба skip. В таких службах функция организации сеанса голосовой связи обеспечивается программным обеспечением компьютера пользователя при помощи сервера, аналогичного серверу службы доменных имен (DNS).

Голосовые соединения в таких службах чаще всего являются бесплатными, пользователь оплачивает только услуги доступа в Интернет. Появление и широкое распространение таких приложений, с одной стороны, приближает давние мечты о персональном сетевом адресе, по которому люди могут связываться независимо от своего местонахождения и типа сообщения. С другой стороны, оно предвещает, закат традиционных бизнес-моделей оказания голосовых услуг.

К голосовым услугам предъявляются следующие основные требования:

- гибкость управления услугами;
- короткое время введения новых услуг;
- независимость от платформы;
- простота пользования услугами для конечного пользователя;
- возможность интеграции голосовых услуг с другими современными услугами (например, приобретение транспортных билетов, билетов в театры и т.п.).

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

## **Лекция 12**

### **Оборудование NGN**

#### **12.1 Классификация оборудования NGN**

Все оборудование сети NGN можно разделить на следующие основные группы:

1. Оборудование управления вызовами и коммутацией.
2. Шлюзы.
3. Терминалы.
4. Серверы приложений.

Схема классификации оборудования сети NGN представлена на рисунке 12.1.

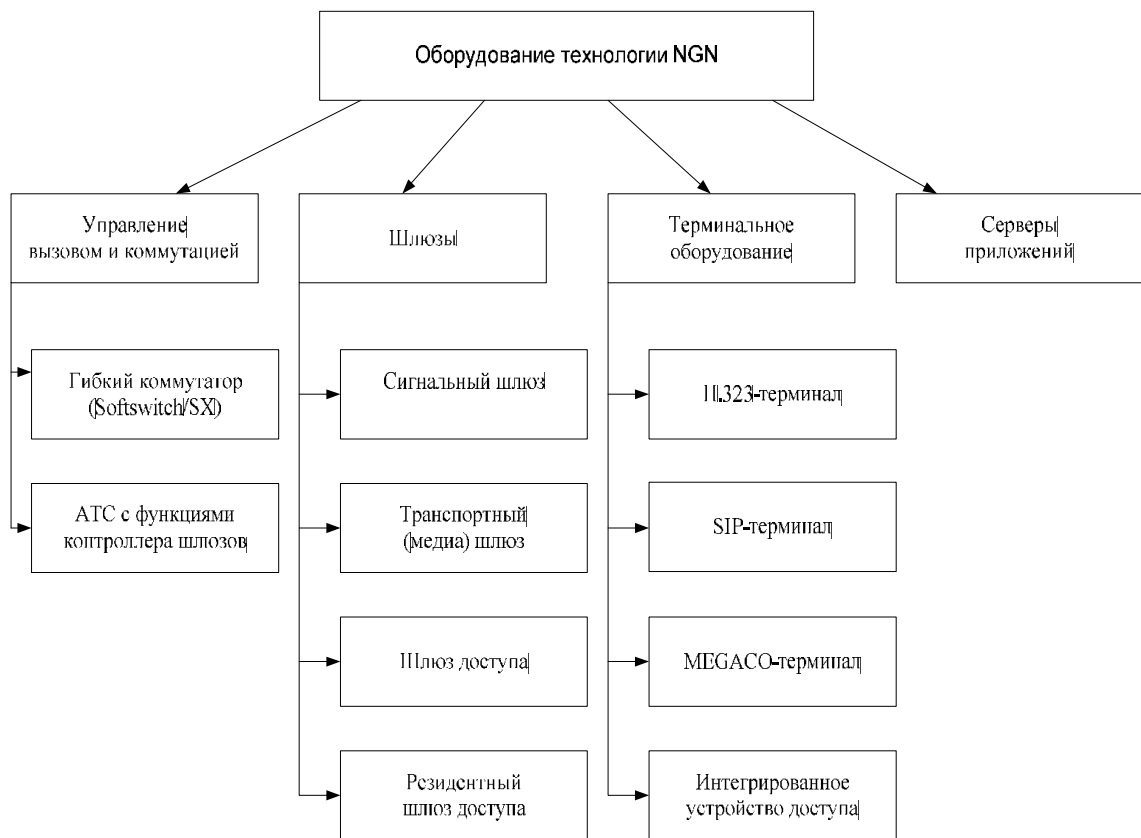


Рисунок 12.1 - Классификация оборудования NGN

## 12.2 Оборудование управления вызовами и коммутацией

К оборудованию управления вызовами и коммутацией относятся гибкий коммутатор Softswitch и АТС с функциями контроллера шлюзов.

*Гибкий коммутатор (Softswitch)* — реализует функции по логике обработки вызова, доступу к серверам приложений, доступу к ИСС (интеллектуальная сеть связи), сбору статистической информации, тарификации, сигнальному взаимодействию с сетью ТФОП и внутри пакетной сети, управлению установлением соединения и др. Гибкий коммутатор является основным устройством, реализующим функции уровня управления коммутацией и передачей информации.

В оборудовании гибкого коммутатора 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 . Реализуется в оборудовании гибкого коммутатора 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 гибкого коммутатора могут быть реализованы следующие функции:

- функция SP/STP (пункт сигнализации/транзитный пункт сигнализации) сети ОКС7 (общеканальная система сигнализации);
- функция предоставления расширенного списка ДВО. Реализуется самостоятельно или с использованием серверов приложений;
- функция взаимодействия с серверами приложений;
- функция SSP (узел коммутации услуг);
- другие функции.

К основным характеристикам гибкого коммутатора относятся следующие характеристики.

— как максимальное количество обслуживаемых базовых вызовов за единицу времени (как правило, за час). Производительность гибкого коммутатора является одной из главных характеристик, на основе которой должен проводиться выбор оборудования и проектирование сети. Следует понимать, что гибкий коммутатор обслуживает вызовы от различных источников нагрузки, каковыми являются:

- вызовы от терминалов, предназначенных для работы в сетях NGN (терминалы SIP и H.323, а также IP-УПАТС);
- вызовы от терминалов, не предназначенных для работы в сетях NGN (аналоговые и ISDN терминалы) и подключаемых через оборудование резидентных шлюзов доступа;
- вызовы от оборудования сети доступа, не предназначенного для работы в сетях NGN (концентраторы с интерфейсом V5) и подключаемого через оборудование шлюзов доступа;
- вызовы от оборудования, использующего первичный доступ (УПАТС – учрежденческо-производственные АТС) и подключаемого через оборудование шлюзов доступа;
- вызовы от сети ТфОП, обслуживаемые с использованием сигнализации ОКС7, с включением сигнальных каналов ОКС7 либо непосредственно в гибкий коммутатор, либо через оборудование сигнальных шлюзов;
- вызовы от других гибких коммутаторов, обслуживаемые с использованием сигнализации SIP-T.

Производительность оборудования гибкого коммутатора 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 NGN в части возможностей гибкого коммутатора 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 гибкого коммутатора характеризуются средней наработкой на отказ, средним временем восстановления, коэффициентом готовности, сроком службы. При проектировании сети следует понимать, что выход из строя гибкого коммутатора приведет к пропаже всех видов связи в обслуживаемом сетевом фрагменте (домене); поэтому должны быть предусмотрены меры по обеспечению дублирования и защиты оборудования.

Оборудование гибкого коммутатора может поддерживать следующие виды протоколов.

При взаимодействии с существующими фрагментами сети ТфОП:

- непосредственное взаимодействие: ОКС7 в части протоколов МТР (подсистемы передачи сообщений ОКС7), ISUP (подсистемы пользователя) и SCCP (подсистемы управления соединениями сигнализации);
- взаимодействие через сигнальные шлюзы:
  - 1) M2UA (уровень адаптации протокола канального уровня МТР - подсистемы передачи сообщений ОКС7),
  - 2) M3UA (уровень адаптации протокола сетевого уровня МТР), для передачи сигнализации ОКС7 через пакетную сеть;
  - 3) V5UA (протокол адаптации сигнализации для передачи сигнальной информации V5 через пакетную сеть);



4) IUA (протокол адаптации сигнализации пользователя ISDN) для передачи сигнальной информации первичного доступа ISDN через пакетную сеть;

5) MEGACO (H.248) (протокол управления транспортными шлюзами) 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.

При взаимодействии с терминальным оборудованием:

- непосредственное взаимодействие с терминальным оборудованием пакетных сетей: SIP (протокол инициирования сеанса связи) и H.323;

- взаимодействие с оборудованием шлюзов, обеспечивающим подключение терминального оборудования ТфОП:

1) MEGACO (H.248) для передачи сигнализации по аналоговым абонентским линиям;

2) IUA для передачи сигнальной информации базового доступа ISDN.

При взаимодействии с другими гибкими коммутаторами: SIP-T (протокол согласования традиционной телефонной сигнализации с сигнализацией SIP).

При взаимодействии с оборудованием интеллектуальных платформ (SCP): INAP (прикладной протокол интеллектуальной сети).

При взаимодействии с серверами приложений: в настоящее время взаимодействие с серверами приложений, как правило, базируется на внутрифирменных протоколах, в основе которых лежат технологии JAVA, XML (языки программирования), SIP и др.

При взаимодействии с оборудованием транспортных шлюзов:

- для шлюзов, поддерживающих транспорт IP или IP/ATM: H.248, MGCP (протоколы управления транспортными шлюзами), IPDC (протокол управления устройствами сети IP) и др.;

- для шлюзов, поддерживающих транспорт ATM: BICC (протокол управления вызовом).

Как правило, оборудование гибкого коммутатора поддерживает следующие виды интерфейсов:

- интерфейс E1 (2048 кбит/с) для подключения сигнальных каналов ОКС7, включаемых непосредственно в гибкий коммутатор;

- интерфейсы семейства Ethernet для подключения к IP сети. Через Ethernet-интерфейсы передается сигнальная информация в направлении пакетной сети.

*АТС с функциями контроллера шлюзов MGC* - это АТС, в которых помимо функций коммутации каналов реализованы функции коммутации пакетов, т. е. функции шлюзов и частично функция гибкого коммутатора. Функционально к такому оборудованию одновременно предъявляются требования, определенные как для гибкого коммутатора, так и для шлюзов.

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.

*Шлюзы (Gateways)* — это устройства доступа к сети NGN и сопряжения с существующими сетями. Оборудование шлюзов реализует функции 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 сети NGN.

Для реализации возможности подключения к сети NGN различных видов оборудования ССОП используются различные программные и аппаратные конфигурации шлюзового оборудования:

- *транспортный (медиа) шлюз (Media Gateway (MG))* реализует функции преобразования речевой информации в пакеты IP/ячейки ATM и маршрутизации пакетов IP/ячеек ATM;
- *сигнальный шлюз (Signaling Gateway (SG))* реализует функции преобразования систем межстанционной сигнализации сети ОКС №7 (квазисвязный режим) в системы сигнализации пакетной сети (SIGTRAN (MxUA));

- *транкинговый шлюз (Trunking Gateway (TGW))* выполняет совместную реализацию функций MG и SG;
- *шлюз доступа (Access Gateway (AGW))* — реализует функции MG и SG для оборудования сети доступа, подключаемого через интерфейс V5;
- *резидентный шлюз доступа (Residential Access Gateway (RAGW))* реализует функции подключения пользователей, использующих терминальное оборудование ССОП/ЦСИС к сети NGN.

Оборудование транспортного шлюза должно выполнять функции устройства, производящего обработку информационных потоков среды передачи и 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, включая процедуры использования кодеков;
- функцию обработки транспортного потока с пакетной коммутацией/коммутацией каналов: обеспечивает преобразование между каналом передачи аудио информации, 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 функцию посредника при сигнализации между пакетной сетью и сетью с коммутацией каналов и 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 характеристики.

*Емкость*, определяемая как в направлении ТфОП, так и в направлении к пакетной сети.

В направлении к ТфОП емкость определяется количеством подключаемых потоков Е1 в направлении сети ТфОП для транспортных шлюзов, а также количеством аналоговых абонентских линий и количеством U(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 10BaseT или пять интерфейсов IMA с использованием потоков Е3.

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

*Протоколы*. Оборудование шлюзов может поддерживать следующие протоколы.

Для транспортных шлюзов:

- в направлении к гибкому коммутатору: H.248, MGCP, IPDC для управления вызовами при использовании транспортной технологии IP; ВСС для управления вызовами при использовании транспортной технологии АТМ;

- в направлении к другим шлюзам или терминальному оборудованию пакетной сети: RTP/RTCP (протокол передачи реального времени/протокол управления передачей в режиме реального времени) при использовании транспортной технологии IP; PNNI (интерфейс между частными сетями АТМ) при использовании транспортной технологии АТМ.

Для сигнальных шлюзов:

- в направлении к сети ТфОП: в зависимости от реализации возможна поддержка уровня МТР2 (протокола канального уровня подсистемы МТР) или МТР3 (протокола сетевого уровня подсистемы МТР) системы сигнализации ОКС7. В первом случае сигнальный шлюз должен терминировать уровень МТР2 и передавать всю «вышестоящую» информацию в направлении гибкого коммутатора с использованием протокола М2UA. Во втором случае сигнальный шлюз должен терминировать уровень МТР3 и передавать «вышестоящую» информацию в направлении гибкого коммутатора с использованием протокола М3UA;

- в направлении к гибкому коммутатору: в зависимости от используемых механизмов обработки ОКС7 могут поддерживаться М2UA или М3UA.

Для шлюзов доступа:

- в направлении к гибкому коммутатору: 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 - протокол доступа к каналу D), сигнализацию по интерфейсу V5 в части протоколов уровня 2 (LAP-V5 - протокол доступа к каналу V5).

*Поддерживаемые интерфейсы*. Как правило, оборудование шлюзов поддерживает следующие интерфейсы:

- транспортные шлюзы: в направлении к ТфОП поддерживаются интерфейсы PDH (Е1) и/или SDH (STM1/4 – синхронный транспортный модуль). В направлении пакетной сети на основе IP технологий: интерфейсы семейства Ethernet от 10Base до GigabitEthernet (1000Base), причем используемая среда передачи специфицируется отдельно.

- сигнальные шлюзы в направлении ТфОП в основном поддерживают интерфейс PDH (Е1), а в направлении пакетной сети — интерфейс 10Base Ethernet;

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

### 12.3 Терминальное оборудование

*Терминальное оборудование* — это терминальные устройства, используемые для предоставления голосовых и мультимедийных услуг 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, так и программное исполнение.

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 ССОП (аналоговые ТА и терминалы ISDN) и терминального оборудования сетей передачи данных (СПД). В IAD реализуются функции по преобразованию протоколов сигнализации ССОП в протоколы пакетных сетей (SIP/H.323) и преобразованию потоков пользовательской информации между сетями с коммутацией каналов и пакетными сетями. Ближайшей аналогией IAD в сетях ССОП является оборудование малых УПАТС.

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

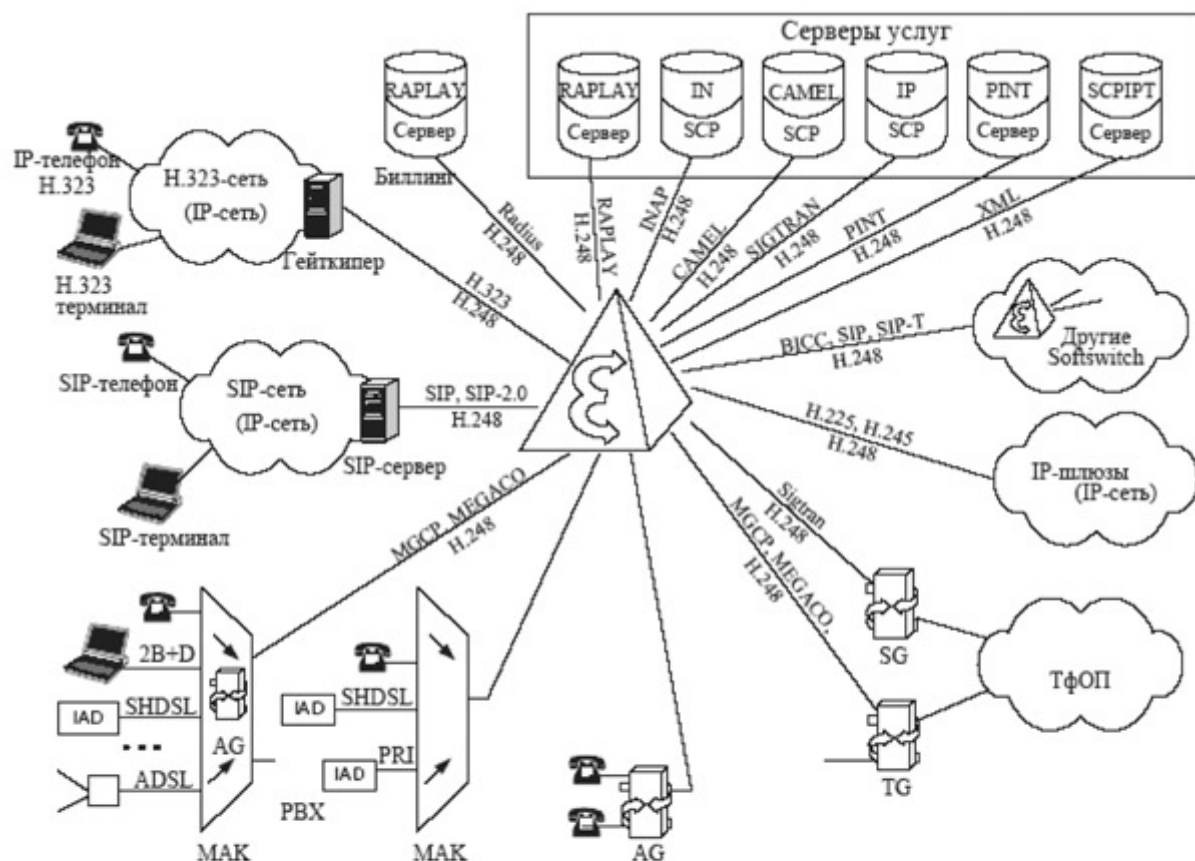
### 12.4 Сервер приложений

*Сервер приложений* - используется для предоставления расширенного списка дополнительных услуг абонентам пакетных сетей или абонентам, получающим доступ в пакетные сети. Серверы приложений предназначены для выполнения функции 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 гибкого коммутатора с использованием технологий JAVA, XML, OSP. Подключение производится в основном с использованием интерфейсов, базирующихся на Ethernet.

## Лекция 13.

### Протоколы NGN

Коммутатор Softswitch управляет обслуживанием вызовов, т.е. установлением и разъединением 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 (рисунок 13.1).



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

Рисунок 13.1 – Схема взаимодействия Softswitch с оборудованием NGN

Основные типы сигнализации, которые использует Softswitch:

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

Основными протоколами сигнализации для управления соединениями являются SIP, ОКС-7, H.323.

Также используются:

- абонентская сигнализация EDDS-1 первичного доступа ISDN;
- протокол абонентского доступа через интерфейс V5;
- российская версия сигнализаций R1, R2 – R 1.5.

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

В таблице 13.1 приведены функциональные назначения протоколов в архитектуре Softswitch.

Таблица 13.1

Протокол	Функция в архитектуре Softswitch	Примечание
SIP	Управление и установление сеанса	Применяется для установления голосовых и мультимедийных вызовов по IP-сетям.

	связи	Использует механизмы, принятые в Интернете, более простой чем протокол H.248. Терминалы содержат ПО SIP-агента. Интеллектуальность ПО смещается от опорной сети к абонентским устройствам.
SIP-T	Передача сигнализации ССОП ISUP через SIP-сеть.	Специальная разновидность протокола SIP, обеспечивающая прозрачную передачу сообщений ISUP по сети SIP. При этом SIP-сеть выполняет функции транзитной станции. Разработка протокола продолжается для обеспечения всех функций ССОП.
H.323	Управление и установление сеанса связи.	Наиболее распространенный протокол в сетях передачи голоса по IP. Считается трудно масштабируемым и менее перспективным, чем SIP-протокол.
H.248/MEGACO	Управление шлюзами доступа в пакетную сеть.	Наиболее перспективный разрабатываемый стандарт. Потенциально должен обеспечить значительно большие возможности по совместимости различного оборудования.
MGCP	Управление шлюзами доступа в пакетную сеть.	Существуют сети с использованием данного протокола. Его усовершенствование затруднено из-за его особенностей.
BICC	Управление вызовом в сетях с разделенными уровнями управления и переноса информации	Протокол установления соединения, не зависящий от типа используемой сети переноса (IP, ATM). Реализует полный набор услуг сети ССОП/ЦСИО. Содержит комплект стандартов, описывающих не только сигнальные процедуры, но и сетевую архитектуру. Основная идея протокола заключается в обеспечении полной реализации всех принятых голосовых услуг классической телефонии при использовании пакетных сетей. Протокол принят организацией 3GPP для сетей мобильной связи третьего поколения.
SIGTRAN	Передача протоколов управления и сигнализации по IP-сети	Набор стандартов, предлагаемый организацией IETF для обеспечения надежной передачи по IP-сети.

### 13.1 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 (рисунок 13.2).

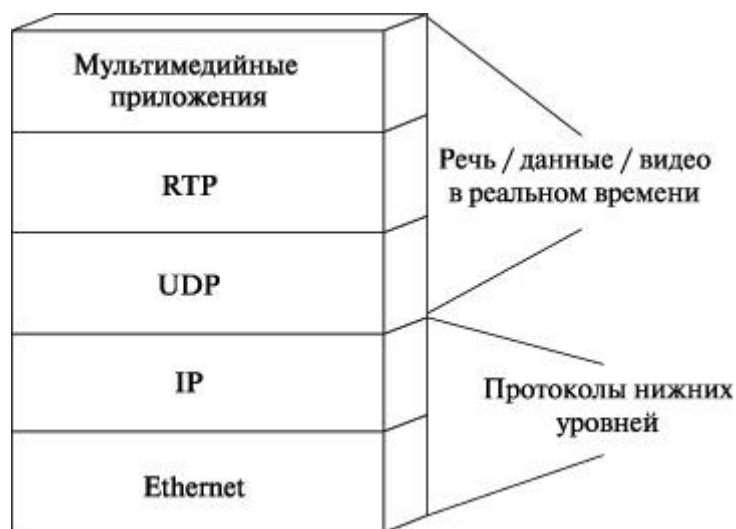


Рисунок 13.2 - Уровни протоколов RTP/UDP/IP

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

Протокол RTP позволяет компенсировать негативное влияние джиттера на качество речевой и видеoinформации, но в то же время он не имеет собственных механизмов, гарантирующих своевременную доставку пакетов или другие параметры качества услуг, – это осуществляют нижележащие протоколы. Он даже не обеспечивает все те функции, которые обычно предоставляют транспортные протоколы, в частности функции исправления ошибок и управления потоком. Обычно протокол RTP базируется на протоколе UDP и использует его функции, но может работать и поверх других транспортных протоколов.

Протокол TCP плохо подходит для передачи чувствительной к задержкам информации. Во-первых, это алгоритм надежной доставки пакетов. Пока отправитель повторно передаст пропавший пакет, получатель будет ждать, результатом чего может быть недопустимое увеличение задержки. Во-вторых, алгоритм управления при перегрузке в протоколе TCP не оптимален для передачи речи и видеoinформации. 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.

### 13.2 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 (рисунок 13.3).

Сети, построенные на базе протоколов H.323, ориентированы на интеграцию с телефонными сетями и могут рассматриваться как сети ЦСИС (цифровая служба 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.

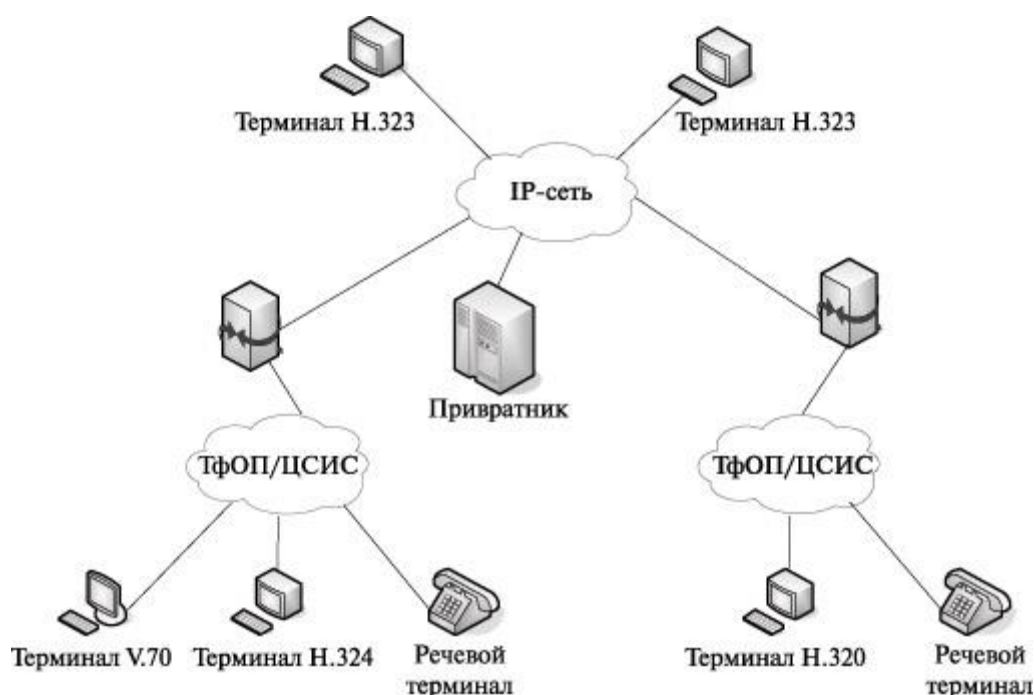


Рисунок 13.3 - Структура сети H.323

Основными устройствами сети H.323 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 – окончательное 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



Н.323 могут быть территориально разнесены, но соединяться друг с другом через маршрутизаторы (рисунок 13.4).



Рисунок 13.4 - Зоновая архитектура сети Н.323

В число наиболее важных функций, выполняемых привратником, входят:

- 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);
- контроль доступа пользователей системы к услугам IP-телефонии при помощи сигнализации RAS (Registration, Admission and Status);
- контроль, управление и резервирование пропускной способности сети;
- 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.

### 13.3 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:

1) персональная мобильность пользователей. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится;

2) масштабируемость сети (характеризуется в первую очередь возможностью увеличения количества элементов сети при ее расширении);

3) 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 рисунке 13.5.



Рисунок 14.5 - Пример построения SIP-сети

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 (проxy 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;

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.

### 13.4 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 (рисунок 13.6):

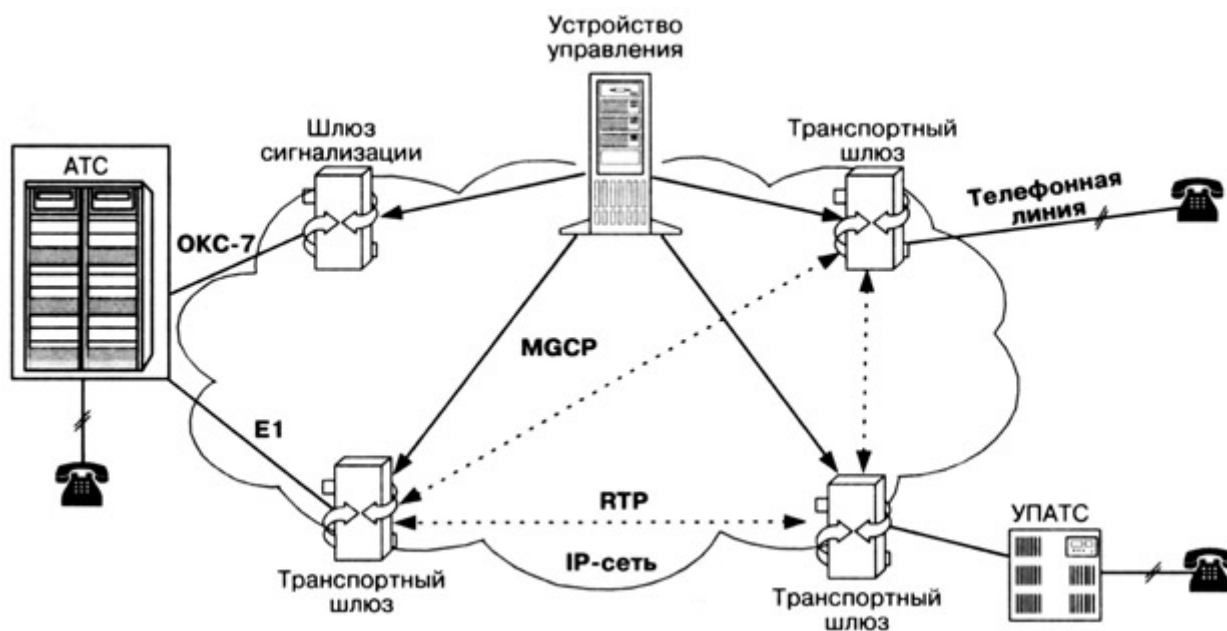


Рисунок 13.6 - Архитектура сети, базирующейся на протоколе MGCP

- транспортный шлюз MG – 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;

- устройство управления CA – Call Agent, выполняющее функции управления шлюзом;

- шлюз сигнализации SG – 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 сетью 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.

### **13.5 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 АТМ. 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 АТМ, 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 (рисунок 13.7).

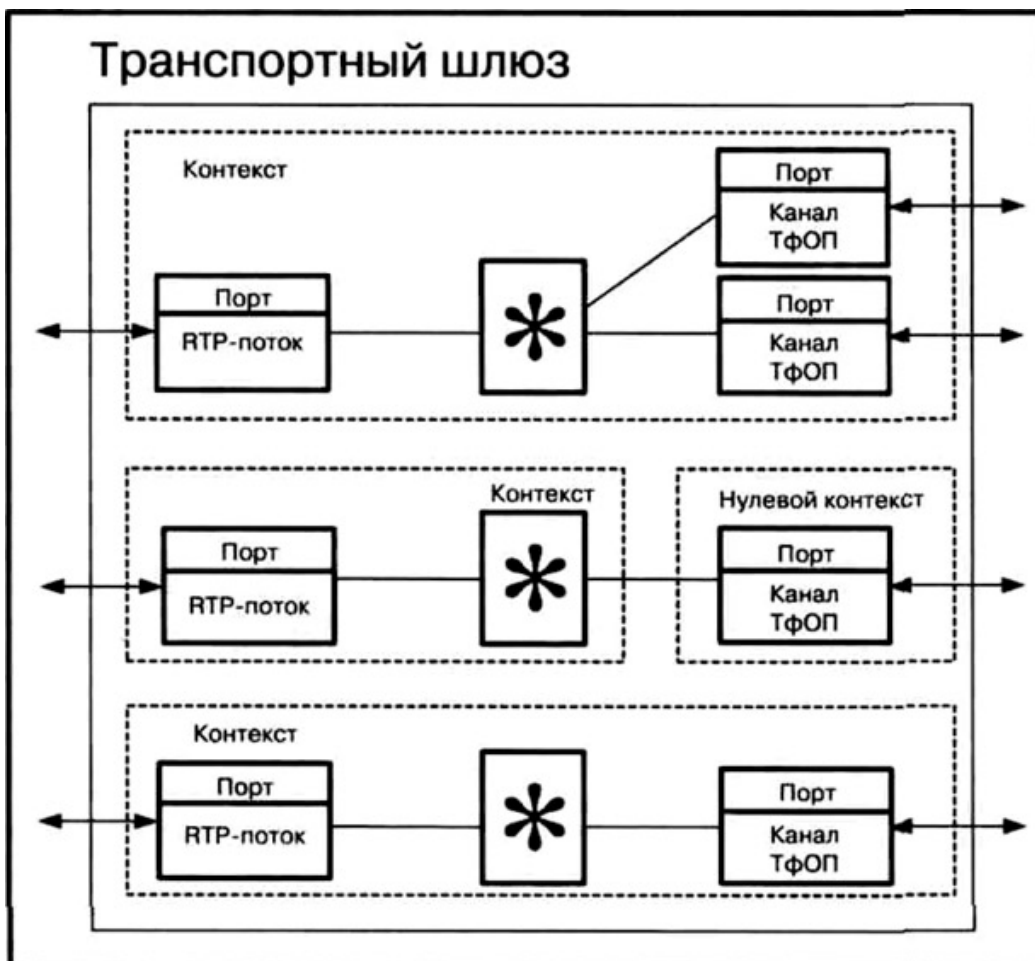


Рисунок 13.7 - Примеры модели процесса обслуживания вызова

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.

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.

## **13.6 Сравнение протоколов**

### **13.6.1 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.

### **13.6.2 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.

### **13.6.3 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.

## **13.7 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 NGN 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 узлы 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.

На рисунке 13.8 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.

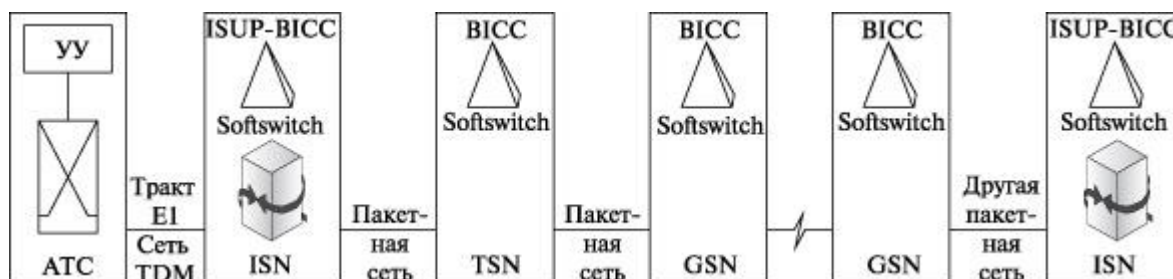


Рисунок 13.8 - Протокол BICC

### 13.8 Транспортировка информации сигнализации (SIGTRAN)

Транспортировка информации сигнализации по технологии SIGTRAN (рисунок 13.9) предназначена для передачи сообщений протокола сигнализации сети с коммутацией каналов через сеть с коммутацией пакетов.

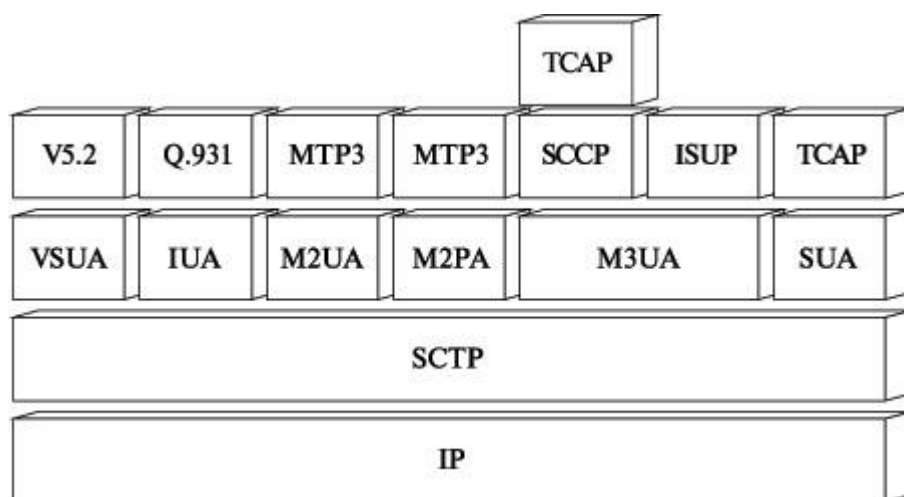


Рисунок 13.9 - Архитектура протоколов SIGTRAN

Она должна обеспечивать:

- 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);

- средства идентификации конкретного транспортируемого протокола сигнализации сети с коммутацией каналов;

- 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;

- функциональные возможности (с участием нижележащего сетевого протокола, например IP), соответствующие нижнему уровню конкретной сети с коммутацией каналов.

### **13.9 Протокол передачи информации управления потоком (SCTP)**

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) 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 адапционные 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.

### **13.10 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 (PRA и BRA) как для режима "точка-точка", так и для разветвленного режима "точка – несколько точек". Процедуры уровня адаптации QSIG не отличаются от аналогичных процедур Q.931.

### **13.11 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.



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 (рисунок 13.10).

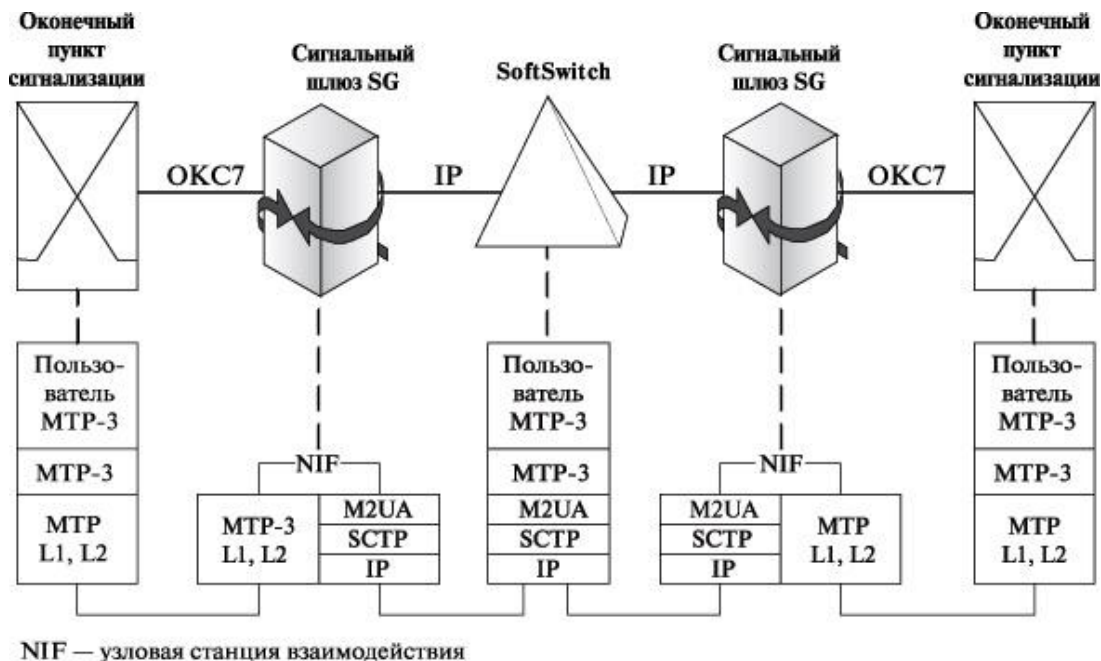


Рисунок 13.10 - Функции M2UA в Softswitch

### 13.12 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.

### 13.13 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 (рисунок 13.11).

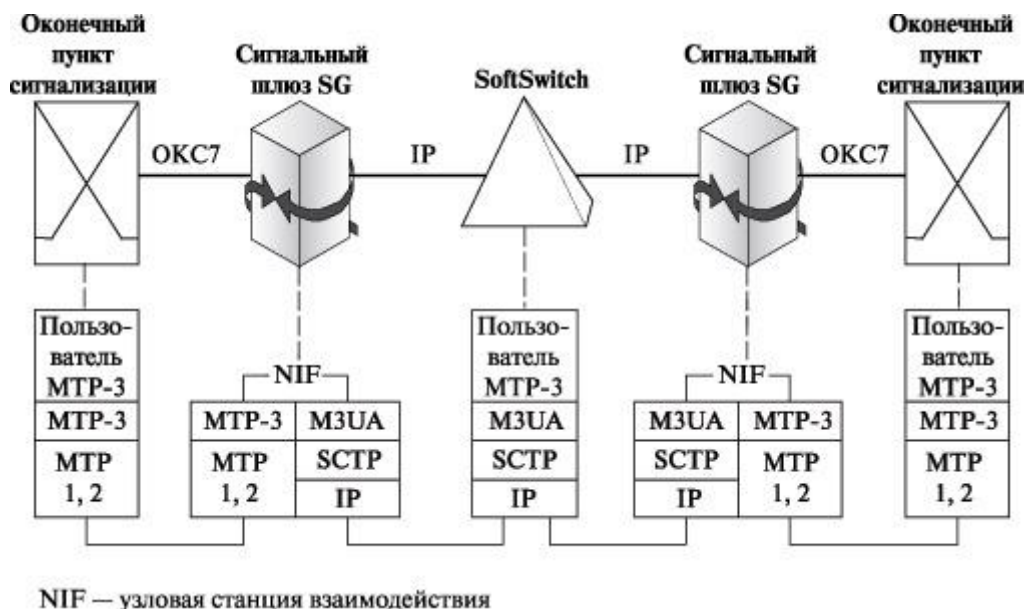


Рисунок 13.11 - Протокол M3UA

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 OKC7).

### 13.14 Пользовательский уровень адаптации SCCP (SUA)

Средствами сети IP возможна доставка сообщений подсистем пользователей SCCP. Архитектура такой доставки может представлять собой связь от SG OKC7 к сигнальному узлу IP (например, резидентной базе данных IP) или связь между двумя оконечными точками, расположенными в пределах сети IP. (рисунок 13.12). 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;
- выдачу отчетов об изменении состояний конфигурации в асинхронном режиме (в целях управления).

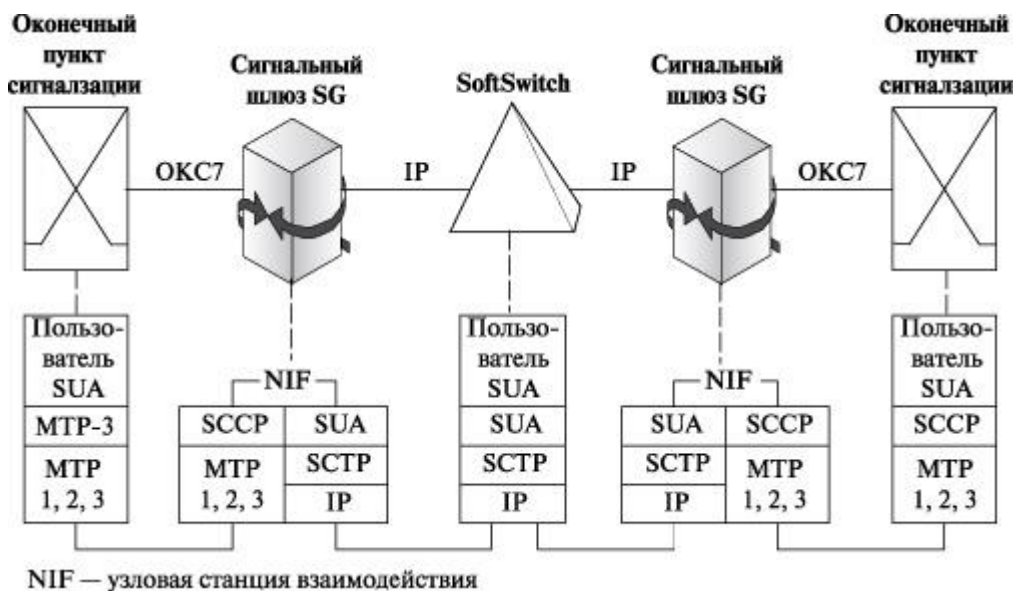


Рисунок 13.12 - Протокол SUA

### 13.15 Протокол SCTP для MEGACO

Реализации протокола MEGACO направлены на достижение высокой пропускной способности и доступности. Они 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 14

### Гибкий коммутатор Softswitch

#### 14.1 Архитектура Softswitch

Softswitch – это совокупность сетевых элементов, взаимодействующих по стандартизированным интерфейсам, и образующих распределённую архитектуру управления вызовами, обеспечивающую управление коммутацией информации различного вида, а также интеграцию с ССОП, СПС и СПД в процессе предоставления услуг связи.

Softswitch (контроллер медиашлюзов MGC) на базе фирменных или промышленных серверов обеспечивает управление распределёнными по сети элементами оборудования NGN.

Softswitch управляет обслуживанием вызовов, выполняя функции Call Agent. В число функций управления обслуживанием вызова Call Agent входят распознавание и обработка цифр номера для определения пункта назначения вызова, распознавание момента ответа вызываемой стороны, момента отбоя, когда один из абонентов кладет трубку, и регистрация этих действий для начисления платы.

Таким образом, Softswitch фактически остается коммутационным узлом, только без цифрового коммутационного поля и кросса и т.п.

Softswitch координирует обмен сигнальными сообщениями между сетями, т.е. поддерживает функции пункта сигнализации Signaling Gateway (SG). Softswitch координирует действия, обеспечивающие соединение с логическими объектами в разных сетях и преобразует информацию в сообщениях с тем, чтобы они были понятны на обеих сторонах несхожих сетей.

Основные типы сигнализации, которые использует Softswitch:

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

Основными протоколами сигнализации управления соединениями сегодня являются SIP-T, OKC7 и H.323. В качестве опций используются протокол E-DSS1 первичного доступа ISDN, протокол абонентского доступа через интерфейс V5 (или его Sigtran-версии V5U), а также сигнализация по выделенным сигнальным каналам R1.5.

Основными протоколами сигнализации управления транспортными шлюзами являются MGCP и Megaco/H.248, а основными протоколами сигнализации взаимодействия между коммутаторами Softswitch являются SIP-T и BICC.

Для взаимодействия Softswitch между собой могут применяться два протокола – SIP (SIP-T), разработанный комитетом IETF и BICC, специфицированный ITU-T. Сегодня на роль основного протокола взаимодействия более претендует протокол SIP-T, хотя BICC обладает возможностью работы и с сигнализацией DSS1, а не только с OKC7.

Использование IP-телефонов в сочетании со Softswitch может иметь для традиционных операторов разрушительные последствия, поскольку при этом требуется лишь, чтобы у абонента имелся IP-телефон и чтобы в установлении соединения могли участвовать разные провайдеры услуг.

Ускорить реализацию этого сценария может повсеместное доведение широкополосных каналов связи до жилых домов и предприятий. Мультисервисный абонентский доступ и технологии беспроводной связи, такие как WiMAX, наряду с интенсивным развитием Softswitch сделают возможным быстрое развёртывание сетей доступа к NGN.

Согласно эталонной архитектуре Softswitch, разработанной консорциумом IPCC, в ней предусматриваются четыре функциональные плоскости (рисунок 14.1.):

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

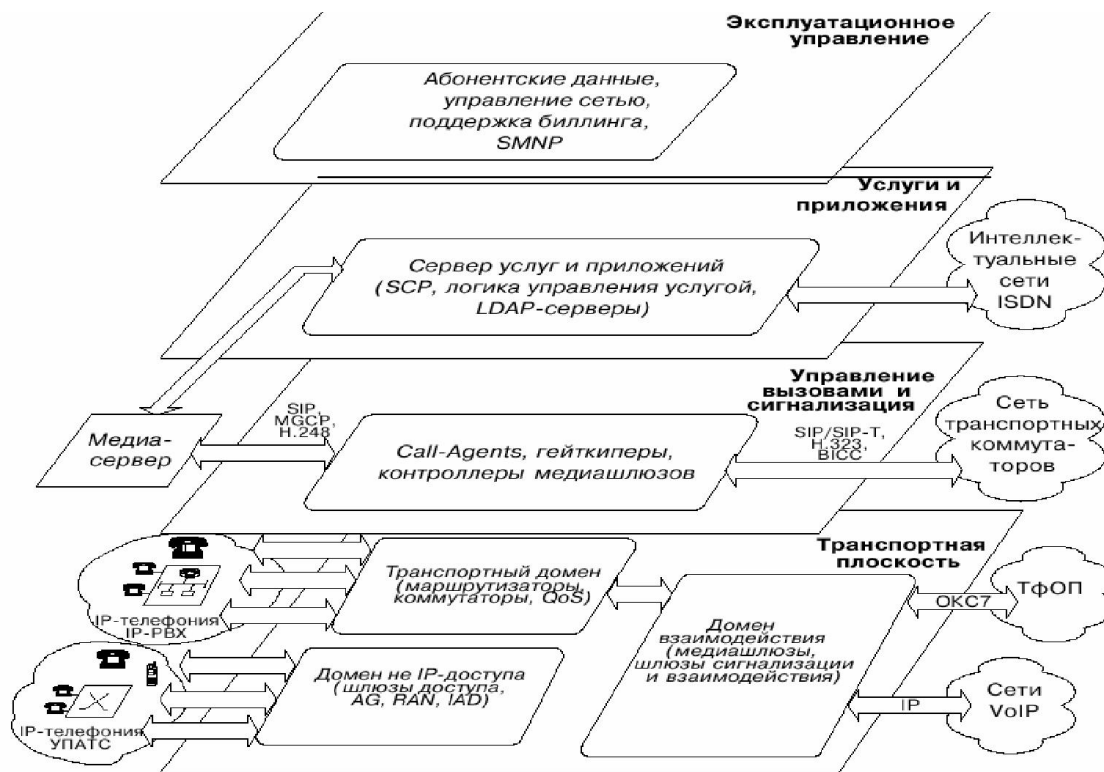


Рисунок 14.1 - Функциональные плоскости эталонной архитектуры Softswitch.

*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 этих 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 пользовательской информации, поступающей со стороны других сетей или терминалов.

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* ID (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 или медиашлюзы MG (Media

Gateways), и шлюзы взаимодействия IG (Interworking Gateways), обеспечивающие взаимодействие различных протоколов сигнализации на одном транспортном уровне.

*Домен доступа*, отличного от IP Non-IP AD (Non-IP Access Domain), предназначен для организации доступа к сети IP-телефонии различных IP-несовместимых терминалов. Он состоит из шлюзов AG (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 и других устройств доступа. IP-терминалы подключаются непосредственно к домену транспортировки по протоколу IP без участия Access Gateway.

*Плоскость управления обслуживанием вызова и сигнализации* (Call Control & Signaling Plane) управляет основными элементами сети IP-телефонии и, в первую очередь, теми, которые принадлежат транспортной плоскости. В этой плоскости введётся управление обслуживанием вызова на основе сигнальных сообщений, поступающих из транспортной плоскости, устанавливаются и разрушаются соединения, используемые для передачи пользовательской информации по сети. Эта плоскость включает в себя такие устройства, как контролер медиашлюзов MGC, сервер управления обслуживанием вызова Call Agent, привратник Gatekeeper и LDAP-сервер.

*Плоскость услуг и приложений* (Service & Application Plane) реализует управление услугами и/или приложениями в сети IP-телефонии, их логику и выполнение. Устройства в этой плоскости содержат логику услуг и управляют этими услугами путем взаимодействия с устройствами, находящимися в плоскости управления обслуживанием вызова и сигнализации. Эта плоскость состоит из таких устройств, как серверы приложений и серверы дополнительных услуг.

На *плоскости эксплуатационного управления* поддерживаются функции активизации абонентов и услуг, техобслуживания, биллинга и другие функции эксплуатационного управления сетью. Плоскость эксплуатационного управления может взаимодействовать с некоторыми или со всеми другими тремя плоскостями либо по стандартному протоколу, либо по внутренним протоколам и интерфейсам API.

Рассмотрим структуру программного коммутатора Softswitch (рисунок 14.2).

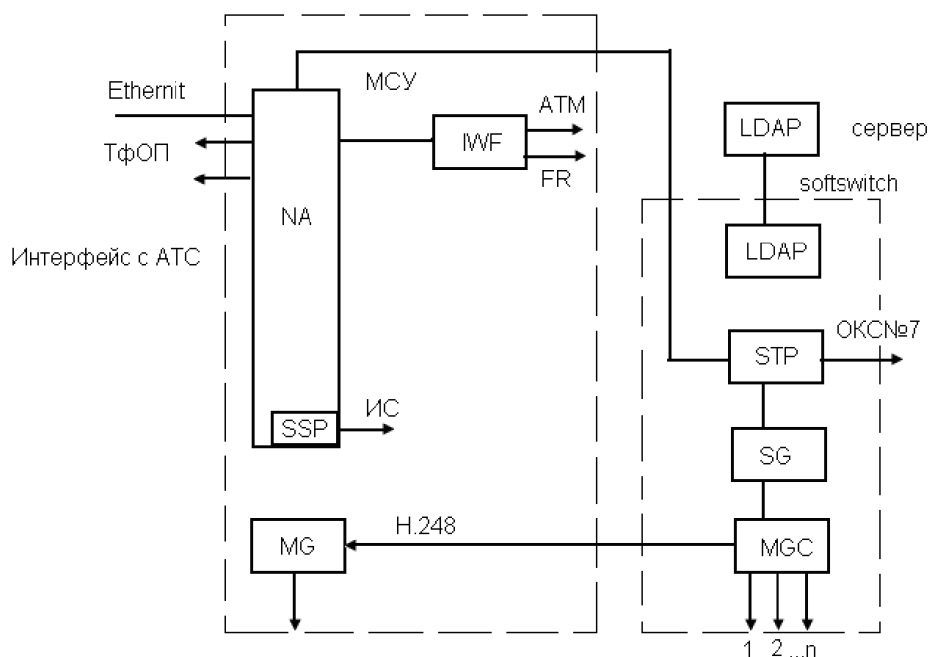


Рисунок 14.2 – Структурная схема Softswitch  
MCU – Мультисервисный сетевой узел.

NA – сетевой адаптер сигнализации, служит для преобразования любого типа сигнализации в сигнализацию ОКС №7.

SSP – коммутатор услуг.

MG – интерфейс с контроллером транспортных шлюзов MGC.

IWF – интерфейс с пакетными сетями.

FR – транспортная пакетная сеть.

MGC – контроллер транспортных шлюзов, управляет работой транспортных шлюзов, обрабатывает сигнальную информацию от пакетных сетей и ТфОП.

SG – сигнальный шлюз, выполняет функции транзитного пункта сигнализации STP и функции преобразования сигнальных сообщений ТфОП в сигнализацию IP-сети.

STP – транзитный пункт сигнализации ОКС №7.

LDAP-сервер – обеспечивает управление, тарификацию и маршрутизацию вызовов в IP-сети.

LDAP – база данных LDAP-сервера.

Таким образом, Softswitch состоит из комплекта серверов, взаимодействующих между собой. Программные серверы могут быть установлены либо на один компьютер, либо распределены. Увеличение производительности каждого модуля выполняется добавлением в стойку сервера нужных блоков.

## **Лекция 15.**

### **Концепция IMS (IP Multimedia Subsystem)**

Развитие телекоммуникационных систем проходит последовательно этапы узкополосных цифровых сетей интегрального обслуживания (сетей ISDN), широкополосных сетей ISDN (B-ISDN), сетей следующего поколения NGN, создание концепции IMS – мультимедийной IP-ориентированной подсистемы связи. Эта концепция открывает путь к построению универсальной сетевой инфраструктуры.

#### **15.1 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 Standardization 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 NGN, 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 сетей NGN 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 сетей NGN – 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 NGN, 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 NGN.

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 объединять 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.

## 15.2 Стандартизация IMS

Стандартизация архитектуры IMS является предметом внимания широкого круга международных организаций, благодаря ключевой роли IMS в эволюции сетей в направлении к NGN. 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 сетей ССП.

Впервые концепция IMS была представлена в документе 3GPP Release 5 (март 2002 г.). В нем была сформулирована основная 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 в 2003 году новой рабочей группы, 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 NGN, а также все, что связано с архитектурой IMS.

### 15.3 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 доступ 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 (рисунок 15.1).

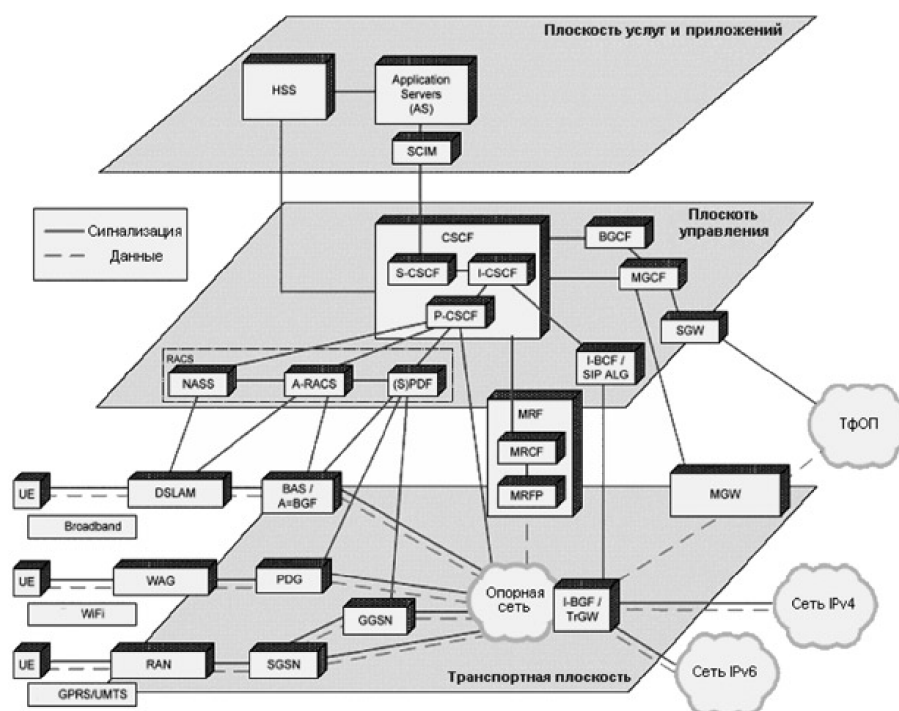


Рисунок 15.1 - Архитектура IMS

### 15.3.1 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, персональный компьютер (ПК) 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:

- 1) обслуживание потоков мультимедийных данных для служб оповещения и т. п.;

- 2) объединение входящих мультимедиапотоков;

- 3) 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 обеспечение функций безопасности (трансляцию адресов и портов NAT, 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.

### 15.3.2 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.

### **15.3.3 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.

Основные элементы:

- 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 медиасerverам 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.

## **15.4 Сравнение Softswitch и IMS**

### **15.4.1 Сходство**

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.

### **15.4.2 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 NGN. 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 IPSS 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 NGN 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.