ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Государственное образовательное учреждение
высшего профессионального образования
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»

Б.С. Гольдштейн, В.Ю. Гойхман
Н.Г. Сибирякова, Ю.В. Столповская

СЕТИ NGN. ОБОРУДОВАНИЕ IMS

Рекомендовано УМО по образованию в области телекоммуникаций
в качестве учебного пособия для подготовки бакалавров
и магистров техники и технологии и дипломированных специалистов
по направлению 210400 «Телекоммуникации»:
210406 «Сети связи и системы коммутации»,
210404 «Многоканальные телекоммуникационные системы»,
210402 «Средства связи с подвижными объектами»,
210407 «Эксплуатация средств связи»
и подготовки дипломированных специалистов
по направлению 230100 «Информатика и вычислительная техника»:
230101 «Вычислительные машины, комплексы, системы и сети»,
230102 «Автоматизированные системы обработки информации
и управления», 230105 «Программное обеспечение
вычислительной техники и автоматизированных систем»

СПб ГУТ)))

САНКТ-ПЕТЕРБУРГ
2010

УДК 004.032.6(076.5)
ББК З 973.23я73
С33

Утверждено
редакционно-издательским советом университета
в качестве учебного пособия

Рецензенты:
доктор технических наук, профессор, зав. кафедрой АЭС ПГУТИ
А. В. Росляков
кандидат технических наук,
Ведущий научный сотрудник ФГУП ЛО ЦНИИС,
Л. В. Голомшток

С33 Сети NGN. Оборудование IMS : учебное пособие / *Б. С. Гольдштейн, В. Ю. Гойхман, Н. Г. Сибирякова, Ю. В Столповская*. – СПб. : Изд-во «Теледом» ГОУВПО СПбГУТ, 2010. – 56 с.

Содержит учебный материал о подсистеме мультимедийной связи IMS для сетей связи следующего поколения. Процесс обучения строится на основе исследовательского полигона технологий и протоколов СОТСБИ-У. Материал учебного пособия представлен в виде теоретической и практической частей, содержит рекомендации для проведения практических и лабораторных занятий, а также необходимую литературу.

УДК 004.032.6(076.5)
ББК З 973.23я73

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

3GPP	3rdGeneration Partnership Project. Проект сотрудничества по созданию систем третьего поколения
AS	Application Server. Сервер приложений
BGCF	Breakout Gateway Control Function. Сервер, выполняющий функции управления пограничным шлюзом (IMS)
CSCF	Call/Session Control Function. Функция управления сессиями.
DSLAM	Digital Subscriber Line Access Multiplexer. Мультиплексор доступа цифровых абонентских линий xDSL
ETSI	European Telecommunications Standards Institute. Европейский институт телекоммуникационных стандартов
GGSN	Gateway GPRS Support Node. Узел шлюзовой поддержки пакетной передачи данных
GPRS	Служба пакетной передачи данных через радиоинтерфейс
HSS	Home Subscriber Server. Сервер абонентских данных
IBCF	Interconnect Border Control Function. Функция управления на границе между сетями различных провайдеров
IETF	Internet Engineering Task Force. Комитет инженерных задач интернет
IMS	IP Multimedia Subsystem. Подсистема мультимедийной связи на базе протокола IP
IM-MGW	IP Multimedia Media GateWay. Мультимедийный шлюз
IP	Internet Protocol. Протокол сетевого уровня сети Интернет
ISIM	IP Multimedia Services Identity Module. Модуль идентификации мобильных абонентов IMS (3GPP)
ISDN	Integrated Services Digital Network. Цифровая сеть интегрального обслуживания
MGCF	Media Gateway Controller Function. Функциональный объект управления медиашлюзом
MRF	Media Resource Function. Функция медиаресурсов
NGN	Next Generation Network. Сеть следующего поколения
NASS	Network Attachment Subsystem. Подсистема присоединения сетей не 3GPP доступа
PDG	Packet Data Gateway. Пакетный шлюз
QoS	Quality of Service. Качество обслуживания
RACS	Resource and Admission Control Subsystem (ETSI). Подсистема управления доступом и ресурсами
RTCP	Real-Time Transport Control Protocol. Протокол контроля транспортировки информации в реальном времени (IETF)
RTP	Real-Time Transport Protocol. Протокол транспортировки информации в реальном времени (IETF RFC 1889)
SDP	Session Description Protocol. Протокол описания сеансов связи
SIM	Subscriber Identification Module. Модуль идентификации абонента
SIP	Session Initiation Protocol. Протокол инициирования сеансов

	связи
SGSN	Serving GPRS Support Node. Шлюз текущей поддержки пакетной передачи данных
SGW	Signaling Gateway. Функциональный объект шлюза сигнализации (ISC)
TCP	Transmission Control Protocol. Протокол управления передачей
TISPAN-ETSI	Telecommunications and Internet converged Services and Protocols for Advanced Networking. Рабочая группа ETSI по стандартизации сетей NGN построенных на базе IMS
TrGW	Transition Gateway. Шлюз сопряжения
UDP	User Datagram Protocol. Протокол передачи дейтаграмм пользователя
UICC	Universal Integrated Circuit Card. Универсальная идентификационная карта
UMTS	Universal Mobile Telecommunications System. Универсальная мобильная телекоммуникационная система
USIM	Universal Subscriber Identity Module. Модуль универсальной идентификации абонента
WAG	Wireless Access Gateway. Шлюз беспроводного доступа
МСЭ	Международный союз электросвязи
СОТСБИ	Сертифицированное оборудование телекоммуникационных сетей – банк информации

1. ПОДСИСТЕМА МУЛЬТИМЕДИЙНОЙ СВЯЗИ IMS

1.1. Общие сведения

Концепция IP Multimedia Subsystem (IMS) описывает новую сетевую архитектуру, основным элементом которой является пакетная транспортная сеть, поддерживающая все технологии доступа и обеспечивающая реализацию большого числа инфокоммуникационных услуг. Ее авторство принадлежит международному партнерству Third Generation Partnership Project (3GPP), объединившему European Telecommunications Standartization Institute (ETSI) и несколько национальных организаций стандартизации.

Исторически к появлению IMS привело развитие двух технологий: эволюция интеллектуальных платформ и развитие технологии Softswitch.

Концепция IMS возникла в результате эволюции базовой сети сотовой подвижной связи третьего поколения UMTS, когда к сети на базе технологии Softswitch была добавлена область управления мультимедийными сеансами на базе протокола SIP. В дальнейшем эта концепция была взята за основу Комитетом ETSI-TISPAN для использования на сетях с различными технологиями доступа (WLAN/Wi-Fi, xDSL, LTE).

Концепции Softswitch и IMS имеют много общего: и та и другая делятся на уровни (плоскости), предоставление всех услуг осуществляется на базе IP-сети, существует разделение функций управления вызовом и коммутации. Но в концепции IMS появляется новая функция - сервер пользовательских данных HSS. Данные, хранящиеся в HSS, используются для регистрации пользователя в IMS, аутентификации пользователя, взаимодействия с функциями учета стоимости, определения профилей и параметров услуг для данного пользователя.

Концепция IMS может рассматриваться как возможное решение для построения сетей следующего поколения и как основа конвергенции мобильных и стационарных сетей на платформе IP.

1.2. Функциональные возможности IMS

Мультимедийные IP-сеансы

IMS предоставляет широкий спектр мультимедийных услуг, но основная услуга IMS – двусторонняя аудио/видео связь. Для этого архитектура IMS должна поддерживать сеансы мультимедийной связи в IP-сетях, должна обеспечивать доступ к услуге пользователям, находящимся как в домашней, так и в гостевой сети. Также пользователи IMS должны иметь возможность комбинировать различные IMS сервисы во время одного мультимедийного сеанса.

Качество обслуживания

Поддержка качества обслуживания QoS является фундаментальным требованием к IMS. При организации сеанса пользовательское оборудование извещает IMS о своих возможностях и своих требованиях к QoS. Протокол SIP, который является основным протоколом, позволяет учесть такие параметры, как тип и направление передачи данных, битовая скорость, размер пакетов, требуемая ширина полосы пропускания. IMS позволяет управлять качеством связи для различных пользователей, и таким образом дифференцировать пользователей и услуги.

Взаимодействие с другими сетями

Функция поддержки взаимодействия с сетью Интернет обеспечивает пользователям IMS установление мультимедийных сеансов связи с разными службами глобальной сети. IMS должна также иметь возможность взаимодействия с сетями предыдущих поколений – телефонными сетями с коммутацией каналов (стационарными и мобильными).

Инвариантность доступа

Инвариантность доступа к IMS, получившая название IP connectivity access, предполагает применение любой технологии доступа, которая может обеспечить транспортировку IP-трафика между пользовательским оборудованием и объектами IMS. Таким образом, функциональные возможности IMS инвариантны относительно разных технологий доступа, например, использующих WLAN, xDSL и т.п.

Создание услуг и управление услугами

В IMS применен новый подход к предоставлению услуг, позволяющий Оператору внедрять услуги, созданные сторонними разработчиками или даже самим Оператором, а не производителями телекоммуникационного оборудования. Это позволяет интегрировать различные услуги и предоставляет широкие возможности персонализации и увеличения количества услуг.

До внедрения IMS в сетях использовались так называемые «вертикальные сервисные платформы» (рис. 1.1), которые успешно справляются с предоставлением небольшого числа ключевых услуг.

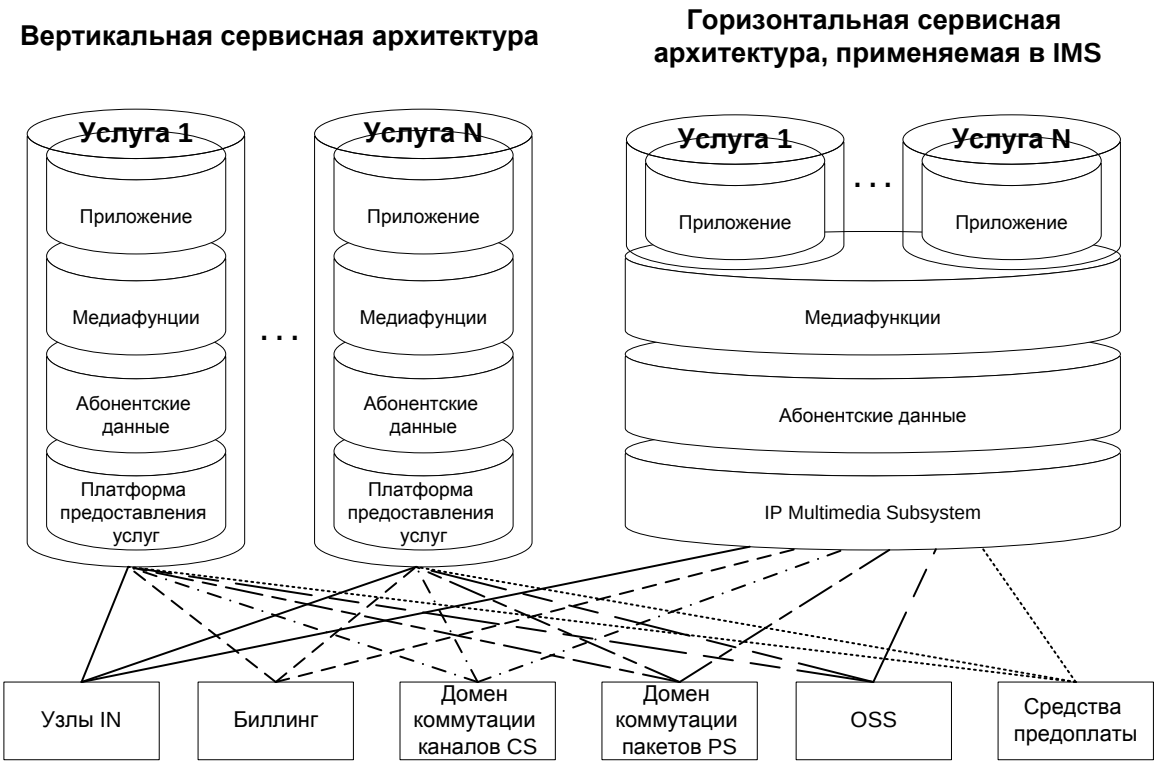

Рис. 1.1. Вертикальная и горизонтальная сервисная архитектура

Подход IMS предполагает горизонтальную архитектуру (рис. 1.1), в которой ресурсы для предоставления услуг являются общими для всех реализованных на сети услуг. Горизонтальная архитектура организации приложений дает новые возможности при создании услуг: интеграция мультимедийных приложений реального и нереального времени; взаимодействие различных видов услуг; поддержка нескольких приложений в одном сеансе.

Роуминг

С точки зрения пользователя очень важно получать доступ к сервисам независимо от географического местоположения. Функция роуминга дает возможность пользователю использовать различные сервисы даже в том случае, если пользователь находиться вне зоны обслуживания домашней сети.

Безопасность

Функции обеспечения безопасности необходимы каждой телекоммуникационной системе, и IMS предоставляет уровень безопасности, по крайней мере, не меньший, чем сети коммутации каналов. IMS производит аутентификацию пользователей перед началом предоставления услуги, предоставляет пользователю возможность запросить обеспечение конфиденциальности информации.

Начисление платы

IMS позволяет Оператору или провайдеру услуг гибко назначать тарифы для мультимедийных сеансов. IMS сохраняет возможность начислять плату за сеанс наиболее простым способом – в зависимости от длительности сеанса или от объема трафика, но может также использовать более сложные схемы, учитывающие предоставляемые услуги QoS и т.п. IMS поддерживает начисление платы в режимах online и offline.

1.3. Стандартизация IMS

Концепция IMS является 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), являющихся следующим этапом развития сетей GSM/GPRS.

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-совместимых протоколов, стандартизованных Комитетом IETF, и используя основные идеи архитектуры сетей связи следующего поколения.

Впервые концепция IMS была представлена в документах 3GPP Release 5 (март 2002). В них была сформулирована основная на то время задача IMS – поддержка мультимедийных услуг в мобильных сетях на базе протокола IP, и специфицировано взаимодействие абонентов сетей GSM/GPRS (2.5 G) и UMTS (3G), а так же механизмы взаимодействия мобильных сетей 3G на базе архитектуры IMS с беспроводными сетями с коммутацией каналов.

В документах 3GPP Release 6 (декабрь 2003) ряд положений концепции IMS был уточнен, добавлены вопросы взаимодействия с беспроводными локальными сетями и защиты информации (использование ключей, абонентских сертификатов).

В документах 3GPP Release 7 рассматривается взаимодействие мобильных и стационарных сетей, т. е. сделан первый реальный шаг в направлении конвергенции стационарных и мобильных сетей.

Спецификация Release 7 добавляет две основные функции, которые являются ключевыми в стационарных сетях:

- Network Attachment, которая обеспечивает механизм аутентификации пользователей и необходима в стационарных сетях, поскольку в них отсутствуют SIM - карты идентификации пользователя;
- Resource Admission, резервирующая сетевые ресурсы в стационарных сетях для обеспечения сеансов связи.

Работы, направленные на расширение концепции IMS на стационарные сети, проводятся Комитетом TISPAN. Интерес к архитектуре IMS со стороны ETSI привел к созданию новой рабочей группы (2003 г.), объединившей известную группу TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) и Технический комитет SPAN (Services and Protocols for Advanced Networks), который отвечает за стандартизацию стационарных сетей. С момента своего создания в 2003 году, организация ETSI TISPAN является ключевым органом стандартизации по созданию технических требований к сетям NGN.

В TISPAN стандартизация делится на этапы, результатом каждого из которых является очередной Release. В декабре 2005 года был окончательно завершен Release 1 NGN, который утверждает стандарт 3GPP IMS (IP Multimedia Subsystem) для SIP-приложений, а также добавляет дополнительные функциональные блоки и подсистемы для поддержки не SIP-приложений.

В начале 2008 года был закончен NGN Release 2, который вводит новое ключевой понятие в NGN - IPTV и IPTV на базе IMS.

TISPAN выделяет два варианта реализации IPTV:

- специализированная подсистема IPTV, ориентированная на внедрение существующих на рынке решений в NGN среду;
- решение IPTV на базе IMS, позволяющее объединять телевизионные услуги с различными телекоммуникационными услугами (голосовые услуги, услуги передачи данных и услуга присутствия в сети).

С начала 2008 года TISPAN начал работу над требованиями NGN Release3, уделяя особое внимание усовершенствованию IPTV, взаимодействию IP сетей, повышению безопасности NGN, качеству обслуживания QoS.

1.4. Идентификация пользователей и услуг

В любой сети связи необходима идентификация пользователей или пользовательских терминалов, а так же предоставляемых услуг.

Основным идентификатором, присваиваемым пользователю провайдером услуг (оператором домашней сети), является идентификатор Private User Identity (PrUI), имеющий формат NAI (Network Access Identifier), оп-

ределенный в RFC 2486. PrUI выглядит следующим образом: *username@operator.com*

Для абонентов UMTS PrUI хранится в логическом модуле идентификации мобильных абонентов IMS ISIM (IP Multimedia Services Identity Module), а так же в HSS, и используется для аутентификации и регистрации пользователя в IMS. PrUI не может быть изменен в терминале пользователя, действителен на все время подписки пользователя на услуги IMS, не используется для маршрутизации сообщений SIP. После регистрации и аутентификации пользователя PrUI должен храниться так же в S-CSCF.

3GPP Release 5 предписывал каждому пользователю иметь один PrUI, но в Release 6 это ограничение убрано, и теперь пользователь может иметь несколько PrUI.

Каждому идентификатору PrUI оператор ставит в соответствие, по меньшей мере, один идентификатор PuUI в формате SIP URI (RFC 3261) и не более чем один в формате tel URL (RFC 3966). В IMS идентификатор PuUI используется для маршрутизации сигнальных SIP-сообщений и в качестве контактной информации для других пользователей.

Формат PuUI:

- sip:alexander@operator.com
- sip:+7_812_960_6293@operator.com;user=phone

Пользователю обычно требуется два разных PuUI – один для сети передачи данных, другой для телефонной сети общего пользования.

Другая причина иметь несколько PuUI – возможность использовать различные номера для разных контактов или услуг. Идентификационная карта IMS-терминала ISIM хранит один PrUI и, как минимум, один PuUI. Перед началом установления или в ходе сессии PuUI должен быть зарегистрирован в процессе регистрации.

Полная структура взаимосвязи нескольких PrUI и PuUI хранится в пользовательском профиле HSS (рис. 1.2). Пользовательский профиль обычно состоит из информации необходимой для подписки на услуги IMS, такой как идентификатор PrUI. Подписка на услуги IMS содержит один или несколько профилей обслуживания Service Profile (набор услуг и соответствующих данных пользователя). Каждому идентификатору PuUI оператор ставит в соответствие только один профиль обслуживания Service Profile.

UICC (Universal Integrated Circuit Card) – термин, означающий сменную идентификационную карту, имеющую стандартизованный интерфейс с терминалом. Карта UICC может содержать несколько логических приложений, таких как SIM (GSM), USIM (UMTS) и ISIM – наиболее важное приложение, поскольку служит для идентификации, авторизации и конфигурации терминала при работе в IMS-сети.

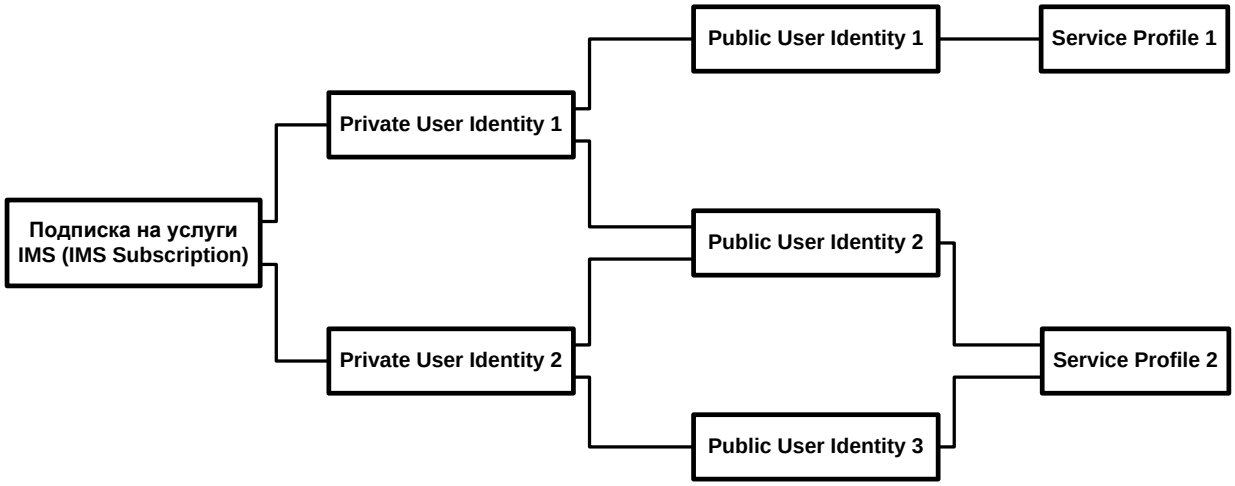

Рис. 1.2. Идентификация IMS пользователей

В 3GPP Release 6 появился идентификатор Public Service Identity (PSI), В отличие от описанных выше идентификаторов, PSI присваивается не пользователям, а услугам, размещенным на серверах приложений. Так же, как и PuUI, идентификаторы PSI могут иметь формат sip url или tel url.

1.5. Архитектура IMS

Подсистема IMS специфицируется как многоуровневая архитектура с разделением на три уровня (плоскости):

- User Plane – транспортную плоскость;
- Control Plane – плоскость управления;
- Application Plane – плоскость приложений.

Партнерство 3GPP специфицирует не оборудование сети, а функции, которые должны выполняться элементами сети. Таким образом, IMS архитектура (рис. 1.3) представляет собой набор логических функций, взаимодействующих с использованием стандартных протоколов.

Разработчики вправе комбинировать несколько функций в одном физическом объекте или, наоборот, реализовать одну функцию распределенно, однако чаще всего физическую архитектуру ставят в соответствие функциональной и реализуют каждую функцию в отдельном элементе.

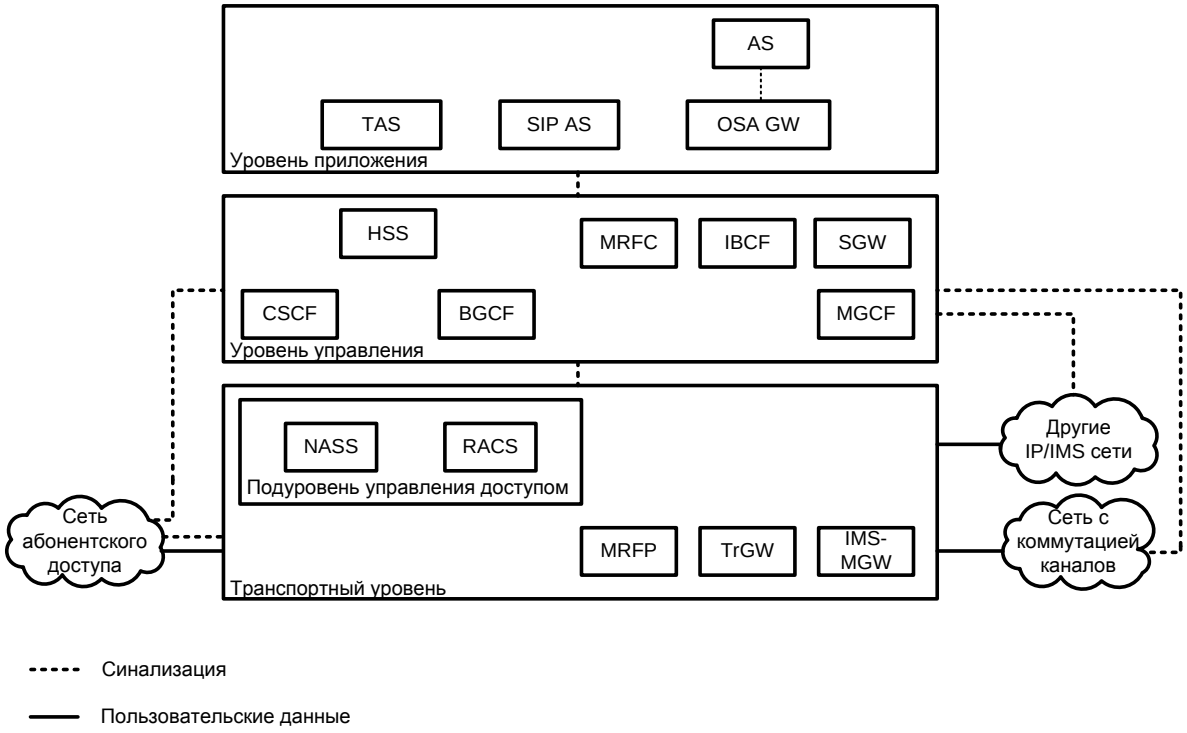

Рис. 1.3. Архитектура IMS

Транспортный уровень

Транспортный уровень отвечает за процедуру подключения пользователей к сети IMS (подуровень управления) и транспортировку данных пользователя (функции передачи). Функциональными элементами транспортного уровня являются:

- подсистема присоединения сети NASS (network attachment subsystem) используется для пользователей не 3GPP доступа, относится к подуровню управления транспортного уровня. NASS обеспечивает динамическое назначение IP-адресов и других параметров конфигурации оборудования пользователя, аутентификацию пользователя до или в течение процедуры назначения IP-адреса, авторизацию и конфигурацию доступа к сети на основе профиля пользователя, управление местоположением;
- подсистема управления доступом и ресурсами RACS (resource and admission control subsystem) используется для пользователей не 3GPP доступа, относится к подуровню управления транспортного уровня. RACS обеспечивает управление доступом, резервирование ресурсов, обеспечивает доступ к услугам, предоставляемым пограничным шлюзом, включая управление шлюзом и преобразование сетевых адресов;
- мультимедийный шлюз IM–MGW (IP Multimedia Media GateWay) осуществляет преобразование пользовательской информации сети с коммутацией каналов TDM в пакеты IP-сети и обратно и коммутацию пользовательской информации между портами шлюза;
- шлюз сопряжения TrGW (Transition Gateway) вместе с функцией пограничного взаимодействия IBCF (Interconnection Border Control

Function) отвечает за взаимодействие между IP-сетями различных версий IP и операторов. Шлюз сопряжения TrGW осуществляет согласование сетей на уровне передачи пользовательской информации;

- функция процессора ресурсов мультимедиа MRFP (Media Resource Function Processor) обеспечивает под управлением контроллера ресурсов мультимедиа MRFC широкий набор функций для поддержки мультимедийных сеансов, в том числе конфигурирование ресурсов, смешивание различных медиапотоков от нескольких источников, генерацию мультимедийных объявлений, обработку мультимедийных потоков (транскодирование), управление правом доступа к медиаресурсам при организации конференции.

Уровень управления

Уровень управления – это совокупность функций IMS, которые осуществляют все действия по управлению сеансами связи и регистрации пользователя в сети IMS.

Основные логические элементы уровня управления.

- Функциональный объект управления сессиями CSCF (Call/Session Control Function) является центральной частью системы IMS, используя протокол SIP, выполняет функции, обеспечивающие предоставление различных услуг реального времени посредством транспорта IP. CSCF включает три основных функции:

– Proxy CSCF (P-CSCF) – выполняет функцию посредника (на сигнальном уровне) для взаимодействия IMS сети и пользовательского IMS терминала. Весь сигнальный трафик протокола SIP направляется от пользовательского терминала к P-CSCF и далее к точке входа в домашнюю сеть (I-CSCF), если пользователь находится в гостевой IMS, или к S-CSCF, если пользователь находится в домашней сети. Адрес S-CSCF определяется в процессе регистрации пользователя. Можно сказать, что P-CSCF реализует функции логического объекта SIP-агента пользователя UA (User Agent). P-CSCF участвует в регистрации пользователя, определяет адрес I-CSCF, находящейся в домашней сети, формирует учетные записи и передает их в сервер начисления платы, а также осуществляет проверку правильности построения сообщений SIP, передаваемых IMS терминалом. Обслуживаемый терминал пользователя закрепляется за функциональным объектом P-CSCF при регистрации в сети на все время регистрации. Адрес P-CSCF на все время сеанса хранится в S-CSCF для трансляции данных к пользователю;

– Interrogating CSCF (I-CSCF) – выполняет функцию посредника для взаимодействия с внешними сетями. Функциональный объект I-CSCF создает первую контактную точку домашней сети IMS на сигнальном уровне в процессе регистрации пользователей, находящихся в гостевой сети, при установлении соединений между пользователями, находящимися в

различных домашних сетях, для всех внешних соединений с пользователями данной сети или гостевыми пользователями, временно находящимися в данной сети. Кроме выполнения функций SIP-прокси I-CSCF взаимодействует по протоколу Diameter с пользовательской базой данных HSS для:

- определения наличия или возможности регистрации пользователя в данной сети,
- получения информации о функциональном объекте S-CSCF,
- если S-CSCF еще не назначен, I-CSCF производит его выбор в процессе регистрации пользователя,
- определение возможностей пользователя по доступу к услугам.

I-CSCF также формирует учетные записи для начисления платы;

– Serving CSCF (S-CSCF) – обслуживающая функция, обеспечивает управление мультимедийными сеансами. Помимо функции SIP-сервера, S-CSCF выполняет функцию регистрирующего сервера сети SIP (SIP-registrar), то есть хранит всю информацию о пользователе, полученную от I-CSCF и HSS: IP-адреса терминала, с которого пользователь получил доступ в сеть, PuUI, PrUI, возможности пользователя по доступу к услугам, адреса P-CSCF, I-CSCF. В свою очередь, S-CSCF информирует сервер пользовательских данных HSS о том, что пользователь прикреплен к ней на срок своей регистрации, и о срабатывании таймера регистрации. Вся сигнальная информация SIP, передаваемая и принимаемая IMS-терминалом, проходит через функциональный объект S-CSCF, к которому прикреплен пользователь. S-CSCF поддерживает сеанс в течение всего времени его продолжения и, по мере надобности, взаимодействует с сервисными платформами и с функциями начисления платы. S-CSCF всегда находится в домашней сети пользователя.

- Пользовательская база данных HSS (Home Subscriber Server) представляет собой централизованное хранилище информации о пользователях и услугах сети IMS и является эволюционным развитием HLR (Home Location Register) из архитектуры сетей GSM/UMTS. В HSS хранится информация о публичном PuUI и закрытом PrUI идентификаторах пользователя IMS, имя обслуживающей функции управления сеансом связи S-CSCF, параметры аутентификации и шифрования, информация о сервере приложений, об услугах, на которые подписан пользователь, имя функции учета стоимости.

HSS взаимодействует с CSCF и серверами приложений, используя протокол Diameter. Если количество пользователей слишком велико, чтобы данные о них хранились в одном HSS, сеть может содержать более одного HSS. Такая сеть наряду с несколькими HSS имеет в своем составе функциональный объект SLF (Subscriber Location Function), который хранит данные и соответствие адресов HSS адресам пользователей. Узел, передавший к SLF запрос с адресом пользователя, получает от него сведения о

HSS, содержащем информацию о данном пользователе. Как HSS, так и SLF используют для взаимодействия с элементами сети IMS протокол Diameter.

- Функциональный объект управления медиашлюзом MGCF (Media Gateways Control Function), его основной задачей является управление медиашлюзами (IM-MGW), а также прямое и обратное преобразование сигнализации сетей ОКС 7 (протокол ISUP) в сигнализацию сети IMS (протокол SIP).
- Сигнальный шлюз SGW (Signaling Gateway) осуществляет преобразование протоколов нижних уровней для обеспечения двустороннего сигнального обмена между сетью IP и сетью TDM, заменяя подсистемы MTP протоколом SIGTRAN. При этом протоколы прикладного уровня (ISUP, MAP, CAP и другие) через SGW транслируются без анализа.
- Контроллер ресурсов мультимедиа MRFC (Media Resource Function Controller). Контроллер ресурсов мультимедиа MRFC взаимодействует с S-CSCF по протоколу SIP и, используя информацию, полученную от S-CSCF, управляет MRFP с помощью протокола MEGACO (H.248). Например, трансляцией акустических сигналов и объявлений, транскодированием и перекодированием, объединением медиапотоков при управлении конференциями.
- Функциональный объект управления пограничными шлюзами BGCF (Breakout Gateway Control Function) реализует функции управления выбором сети, осуществляет маршрутизацию на основе информации о телефонных номерах, получаемой из сообщений протокола SIP, административной информации и/или с помощью доступа к базам данных. BGCF используется только при установлении сеанса между пользователями сети IMS и абонентом сети с коммутацией каналов. BGCF выбирает сеть IMS, в которой будет происходить взаимодействие с сетью с коммутацией каналов, или MGCF, если BGCF находится в сети IMS, которая будет взаимодействовать с сетью с коммутацией каналов. Оборудование BGCF также маршрутизирует транзитный сигнальный трафик.
- Функциональный объект граничного взаимодействия IBCF (Interconnection Border Control Function) обеспечивает взаимодействие с IP-сетями. IBCF, обеспечивает реализацию стека протоколов SIP/SDP для установления взаимосвязи между приложениями SIP на основе IPv6 и приложениями SIP на основе IPv4, сокрытие сетевой топологии, управление с помощью протокола MEGACO шлюзами сопряжения TrGW при установлении соединений с другими IMS или другими сетями, функционирующими на основе протокола IP. IBCF также выполняет функции маршрутизации при транзите.

Уровень приложений

Уровень приложений относится к верхнему уровню сетевой архитектуры IMS. На данном уровне расположены серверы приложений AS, пре-

доставляющие доступ как к приложениям IMS, так и приложениям на основе других платформ (таких как OSA и CAMEL).

На этом уровне сервера приложений отвечают за обслуживание конечных пользователей.

Архитектура IMS и сигнализация SIP обеспечивают достаточную гибкость для поддержки разнообразных телефонных и других приложений:

- 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 (OSA). Его задачей является обеспечение возможности доступа услуг к сетевым функциям посредством стандартного программного интерфейса приложений;
- IM-SSF (IP Multimedia – Service Switching Function) – сервер коммутации услуги, служит для возможности использования в IMS услуг CAMEL (Customized Applications for Mobile network Enhanced Logic) разработанных для мобильных сетей;
- 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.

1.6. Технологии доступа к сети IMS

Благодаря концепции инвариантности доступа даже не предназначенные для взаимодействия с подсистемой IMS пользовательские устройства могут осуществлять доступ к опорной сети и сервисам на базе IMS.

Изначально (в спецификациях 3GPP Release 5) IMS была ориентирована на работу с мобильными сетями поколения 2,5G (GSM/GPRS), имеющими технологию радиодоступа GERAN, и 3G (UMTS) – технология радиодоступа UTRAN. В стандартах консорциума 3GPP2 описана возможность доступа к IMS сети радиодоступа CDMA2000.

В последующих версиях 3GPP Release 6, 7 и ETSI TISPAN рассмотрены вопросы взаимодействия IMS с сетями, имеющими технологии доступа WLAN/Wi-Fi, xDSL (рис. 1.4). А в версиях 8 и 10 спецификаций 3GPP была добавлена поддержка инфраструктур HSPA и LTE.

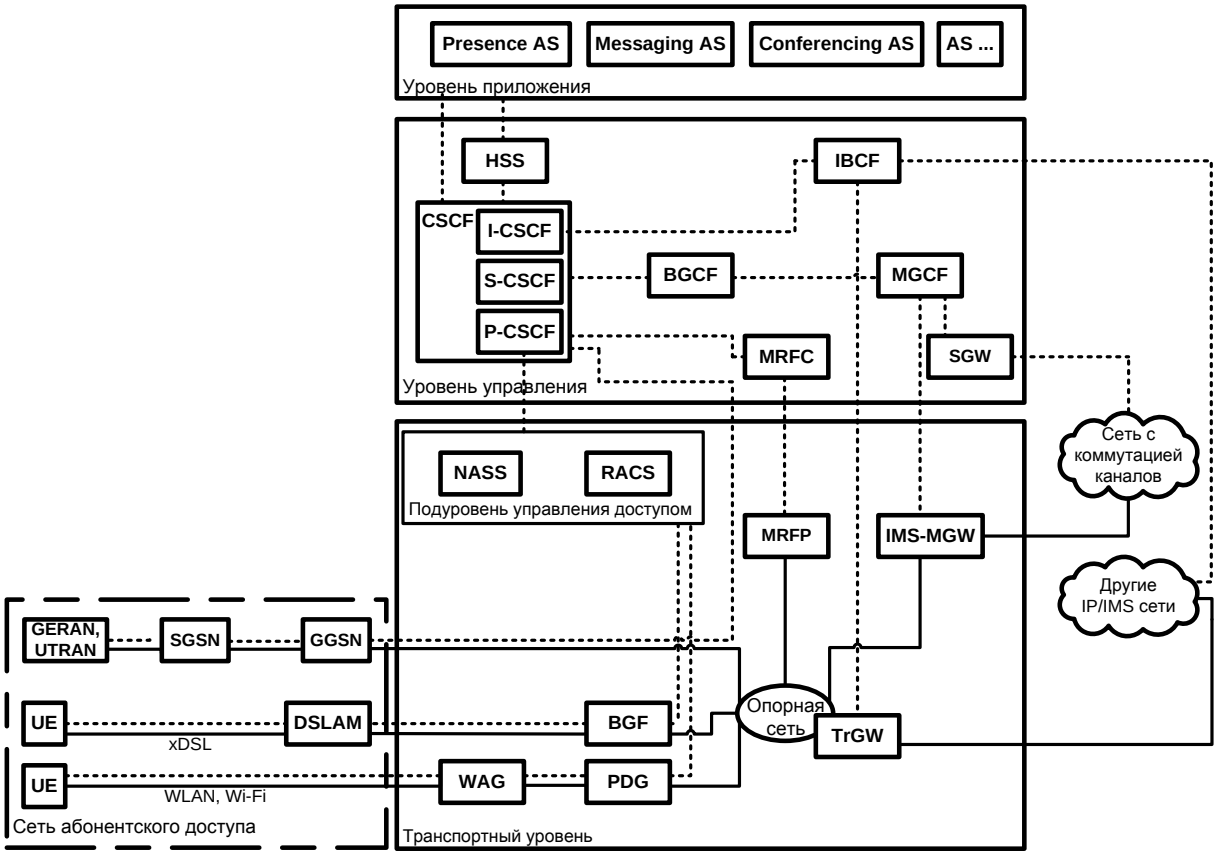

Рис. 1.4. Организация доступа к сети IMS

Для доступа к IMS пользователей сетей радиодоступа GERAN/UTRAN используются узлы GPRS (SGSN, GGSN) (рис. 1.4).

За доступ пользовательского оборудования WLAN к сети IMS отвечает пакетный шлюз PDG (Packet Data Gateway) и шлюз беспроводного доступа WAG (Wireless Access Gateway).

Мультиплексор DSLAM (Digital Subscriber Line Access Multiplexer) и граничный шлюз A-BGF/BAS (Access Border Gateway Function/Broadband Access Switch), обеспечивает широкополосный доступ фиксированных пользователей к сети IMS.

1.7. Основные протоколы IMS

Как уже говорилось ранее, архитектура IMS представляет собой набор функциональных объектов, соединенных стандартными интерфейсами (рис. 1.5). Взаимодействие функциональных объектов IMS осуществляется с использованием протоколов сети Интернет, определенных организацией IETF.

Протоколы подсистемы IMS обеспечивают управление мультимедийными сессиями (SIP, SDP), передачу пользовательского трафика (RTP и RTCP), регистрацию, аутентификацию, авторизацию, поддержку мобильности пользователя (Diameter). Протокол MEGACO/H.248 используется для

управления зависимыми объектами транспортной плоскости. Для транспортировки сигнальной информации ОКС7в сетях IP и взаимодействия с другими сетями, в частности с ТфОП, используется протокол SIGTRAN.

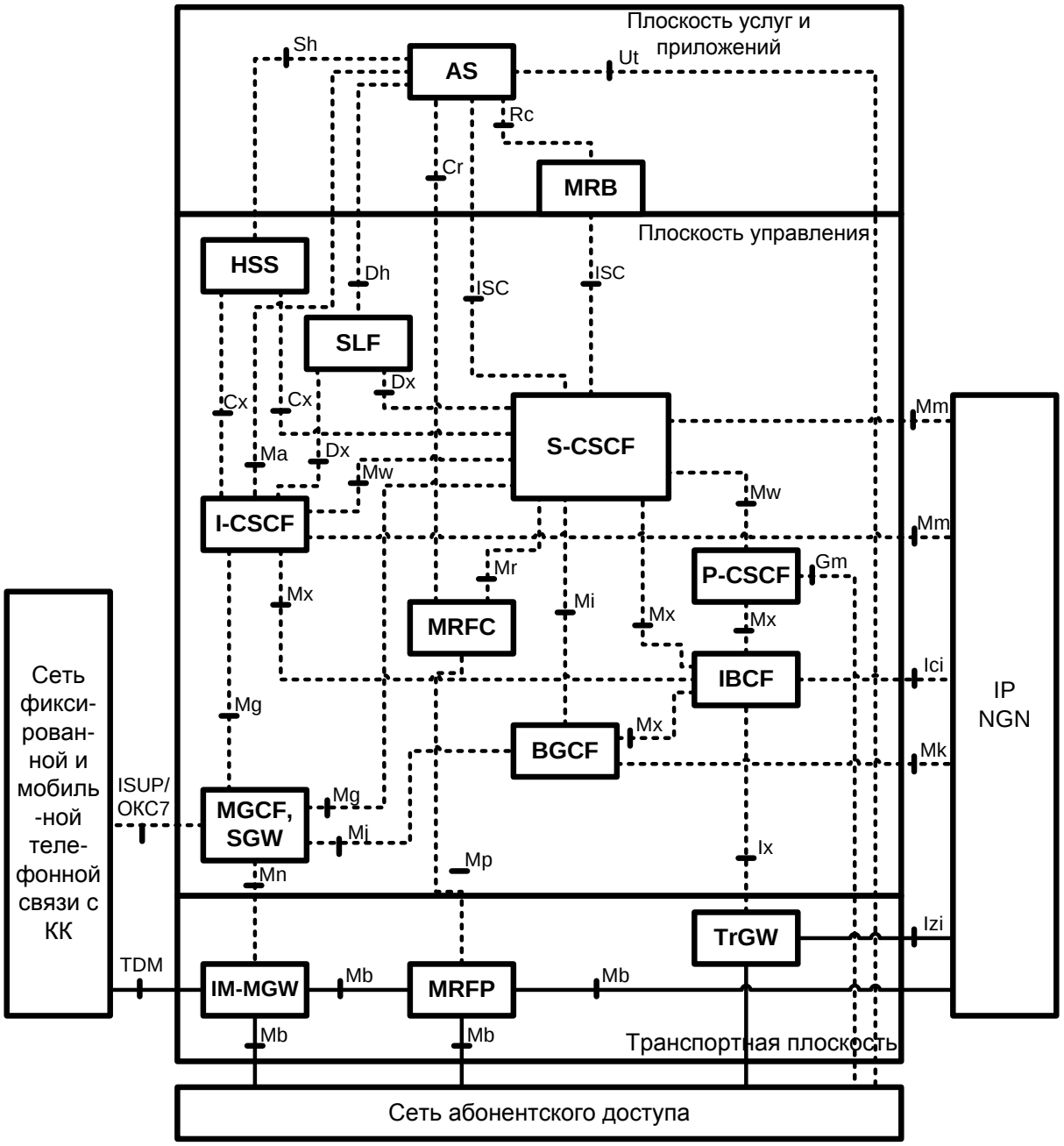

Рис. 1.5. Функциональные элементы и интерфейсы архитектуры IMS

Перечень возможных интерфейсов (внешних и внутренних) и протоколов взаимодействия, реализованных в архитектуре IMS, представлен в табл. 1.1.

Таблица 1.1

Наименование интерфейса (рис. 1.6)	Протоколы взаимодействия	Описание
Cr	SIP	Обмен сообщениями между сервером приложения AS и функцией MRFC
Cx	Diameter	Взаимодействие между I-CSCF/S-CSCF и HSS
Dh	Diameter	Обнаружение сервером приложений AS, необходимого HSS, в сети с несколькими HSS
Dx	Diameter	Обнаружение функциями I-CSCF/S-CSCF, необходимого HSS, в сети с несколькими HSS
Gm	SIP	Обмен сообщениями между оборудованием пользователя и функциями CSCF
Ici	SIP	Взаимодействие между блоками IBCF различных мультимедийных сетей
ISC	SIP	Обмен сообщениями между функциями CSCF и серверами приложений AS
Ix	MEGACO	Взаимодействие между элементами IBCF и TrGW
Izi	RTP/RTCP	Взаимодействие между TrGW и пограничными шлюзами различных мультимедийных сетей
Ma	SIP	Взаимодействие между блоками I-CSCF и сервером приложений AS

Окончание табл. 1.1

Наименование интерфейса (рис. 1.6)	Протоколы взаимодействия	Описание
Mg	SIP	MGCF преобразует сигнализацию ISUP в SIP (и обратно) и передает сигнальную информацию SIP к I-CSCF
Mg	SIP	Взаимодействие между элементами MGCF и CSCF
Mi	SIP	Обмен сообщениями между S-CSCF и BGCF
Mj	SIP	Обмен сообщениями между BGCF и MGCF в одной IMS сети
Mk	SIP	Обмен сообщениями между BGCF и другими сетями
Mn	MEGACO/H.248	MGCF управляет оборудованием медиашлюза IM-MGW
Mp	MEGACO/H.248	MRFC управляет функцией IM-MRFP
Mr	SIP	Обмен сообщениями между S-CSCF и MRFC
Mr	SIP	Взаимодействие между элементами S-CSCF и MRFC
Mw	SIP	Обмен сообщениями между функциями CSCF
Mx	SIP	Обмен сообщениями между I- CSCF/BGCF и IBCF
Ut	HTTP(s), XCAP	Взаимодействие между пользовательским терминалом IMS и сервером приложений AS

Протокол SIP

SIP (Session Initiation Protocol) является текст-ориентированным протоколом прикладного уровня и предназначен для организации, модификации и завершения различных сеансов связи, в том числе мультимедийных конференций, телефонных соединений, широковещательной рассылки мультимедийной информации и соединений пользователей с разными инфокоммуникационными приложениями.

В ноябре 2000 года SIP был принят в качестве сигнального протокола 3GPP, позднее он был выбран в качестве протокола управления сессиями для сети IMS.

SIP является основным протоколом IMS, позволяет устанавливать мультимедийные сеансы и управлять ими. Почти все элементы сети IMS взаимодействуют друг с другом по протоколу SIP (табл. 1.1). Более подробно протокол SIP описан в [2].

Протокол SDP

Протокол описания сессии (SDP), описанный в рекомендации IETF RFC 4566, определяет формат и синтаксис описания мультимедийной сессии и ее начальных параметров с целью инициирования сеансов, оповещения о них и приглашения к ним.

В описание сессии входит следующая информация:

- тип передаваемых данных (видео, аудио);
- транспортный протокол (TCP,UDP);
- формат данных (H.261, MPEG);
- IP адрес устройства, адрес порта RTP;
- используемые кодеки.

Протокол MEGACO/H.248

MEGACO/H.248 является официальным стандартным протоколом взаимодействия контроллеров транспортного шлюза (MGC) и мультимедийных шлюзов (MG). Этот стандарт является результатом совместных усилий организаций по стандартизации IETF и ITU. Протокол MEGACO/H.248 также был выбран организациями 3GPP и TISPAN для всех операций управления пользовательскими данными в IMS: между MGCF и IM-MGW, MRFC и MRFP, IBCF и TrGW.

Более подробно протокол MEGACO/H.248 описан в [3].

Протокол DIAMETER

Протокол DIAMETER, описанный организацией IETF в RFC 3588, является протоколом аутентификации, авторизации и учета (протоколом AAA) в IMS и NGN.

В HSS хранятся данные, необходимые для регистрации пользователя в сети IMS, аутентификации пользователя, взаимодействия с функциями уче-

та стоимости, определения обслуживающего функционального объекта CSCF (S-CSCF) и профилей и параметров услуг для данного пользователя. CSCF и серверы приложений AS взаимодействуют с HSS по протоколу DIAMETER при обмене этими данными.

Более подробно протокол DIAMETER описан в [4].

Протоколы RTP/RTCP

Для передачи мультимедийных данных применяется протокол реального времени RTP и протокол управления передачей RTCP.

Протокол RTP был разработан IETF (RFC 1889) для переноса в реальном времени речевой и видеоинформации по сети с коммутацией пакетов. Совместно с протоколом UDP, RTP реализует функции транспортного уровня.

Протокол управления передачей информации в реальном времени RTCP формирует отчеты, содержащие информацию о сеансах связи RTP. Предоставляет возможности повышения QoS, поддерживая связь между отправителем и получателем потока путем обмена пакетами, отчет приемника и отчет источника. RTCP использует тот же стек транспортных протоколов, что и RTP (UDP/IP).

Протокол SIGTRAN

В рамках IETF была создана рабочая группа Sigtran (IETF SigTran Working Group), предназначенная для исследования транспортировки сигнальной информации ОКС7 в сетях IP и взаимодействия с другими сетями, в частности, ТфОП. С момента первого своего заседания в Орландо в 1998 году этой рабочей группе удалось создать достаточно полную архитектуру ОКС7 (и не только ОКС7) поверх IP, которая описана в RFC 2719.

1.8. Регистрация пользователя в сети IMS

Регистрация является необходимой процедурой при работе в сети IMS. Незарегистрированные пользователи не могут получить доступ к сервисам сети. Сценарий (рис. 1.6) отображает процедуру регистрации пользователя в сети IMS при условии, что пользователь находиться в гостевой сети.

Возможны два варианта процедуры регистрации: с аутентификацией и без аутентификации. В случае если пользователь впервые регистрируется в сети IMS, ему необходимо пройти аутентификацию (рис. 1.6, а).

При повторной регистрации аутентификация пользователя не требуется (рис. 1.6, б).

Прежде чем начать регистрацию оборудование пользователя (UE) осуществляет поиск точки доступа в сеть IMS (P-CSCF).

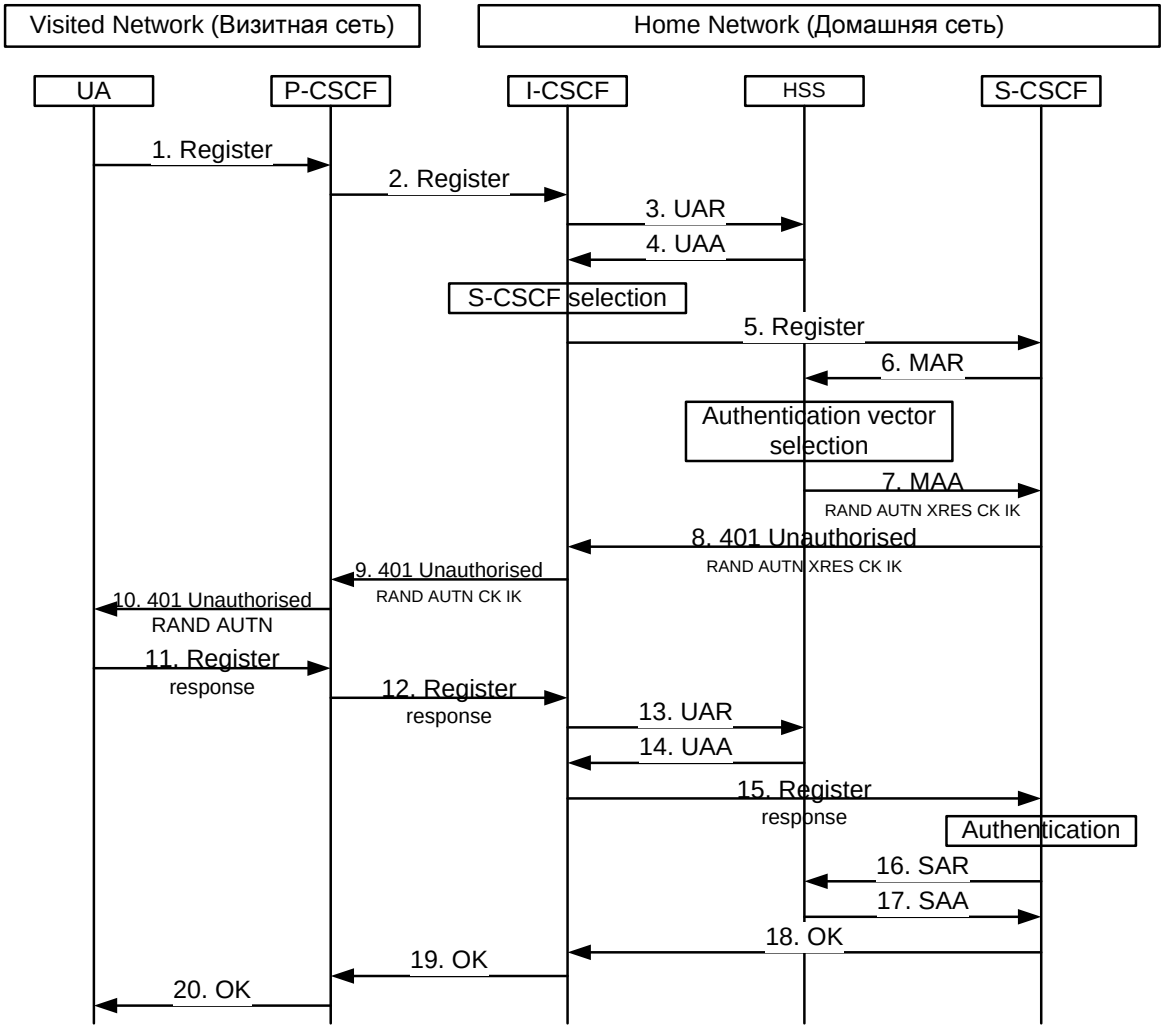

Рис. 1.6, а. Процедура регистрации пользователя в сети IMS

1. После получения адреса P-CSCF UE начинает процедуру регистрации, для чего UE отправляет запрос протокола SIP Register к обнаруженной P-CSCF. Он содержит идентификаторы пользователя PrUI (заголовок To сообщения Register) и PuUI (заголовок Contact), который необходимо зарегистрировать, а также доменное имя домашней сети (заголовок Request URI) и IP-адрес терминала пользователя.

2. Функциональный объект P-CSCF обрабатывает запрос Register, анализирует доменное имя домашней сети для выявления точки входа в домашнюю сеть (I-CSCF), затем передает запрос Register к I-CSCF (адрес P-CSCF, PrUI (To) PuUI (Contact), идентификатор гостевой сети, где находится P-CSCF, IP-адрес терминала пользователя). Для определения адреса домашней сети на основании ее доменного имени используется механизм преобразования имен в адреса. Идентификатор гостевой сети представляет собой последовательность символов, которая идентифицирует в домашней сети, сеть, в которой находится P-CSCF (например, идентификатором сети P-CSCF может быть доменное имя сети P-CSCF).

3. I-CSCF обращается к HSS домашней сети для выбора функционального объекта S-CSCF, который будет обслуживать данного пользователя. Это осуществляется с помощью обмена сообщениями протокола Diameter: User-Authorization-Request (UAR) и User-Authorization-Answer (UAA). UAR содержит PrUI, PuUI, идентификатор гостевой сети, где находится P-CSCF. HSS должен проверить, не зарегистрирован ли уже пользователь, разрешено ли пользователю зарегистрироваться в этой гостевой сети, в зависимости от оформленной пользователем подписки, а также налагаемых оператором ограничений или запретов, если таковые имеются

4. От HSS к I-CSCF посылается ответ User-Authorization-Answer, который должен содержать имя S-CSCF, если оно известно серверу HSS, или функциональные возможности S-CSCF, если выбор новой S-CSCF осуществляет I-CSCF. После получения информации о функциональных возможностях I-CSCF должен выполнить на их основе выбор нового S-CSCF. Если проверка в HSS была неуспешной, отправкой ответа UAA отменяется попытка регистрации.

5. I-CSCF, используя имя S-CSCF, должен определить адрес S-CSCF посредством механизма преобразования имен в адреса. Затем I-CSCF должен послать запрос Register (адрес/имя P-CSCF, PrUI, PuUI, идентификатор сети P-CSCF, IP-адрес UE) к выбранному S-CSCF, который должен сохранить адрес/имя P-CSCF, предоставленный гостевой сетью. Это тот адрес/имя, по которым домашняя сеть пересылает последующую сигнализацию входящей сессии к терминалу пользователя. S-CSCF должен сохранить информацию и об идентификаторе сети P-CSCF.

6. S-CSCF обрабатывает запрос и так как пользователь не авторизован, то S-CSCF должен получить данные от HSS необходимые для аутентификации путем обмена сообщениями протокола Diameter: Multimedia-Auth-Request (MAR) и Multimedia-Auth-Answer (MAA). MAR содержит PrUI, PuUI, имя S-CSCF.

7. HSS должен сохранить имя S-CSCF для данного пользователя, и послать в S-CSCF ответ MAA (информацию о пользователе). Информация о пользователе, передаваемая от HSS к S-CSCF, должна включать одно или более имен/адресов, которые могут использоваться для доступа к платформе (платформам) управления услугами, в то время пока пользователь регистрируется на этой S-CSCF. S-CSCF должна сохранить информацию для зарегистрированного пользователя. В дополнение к информации об именах/адресах, может также посылаться информация безопасности, которая может использоваться в S-CSCF. Также сообщение MAA содержит параметры аутентификации и шифрования (произвольный номер (RAND), ожидаемый ответ (XRES), ключ шифрования (CK), ключ целостности (IK) и символ аутентификации (AUTN).

8. S-CSCF формирует ответ 401 Unauthorized response, который в заголовке www-Authenticate содержит параметры аутентификации и шифрова-

ния, принятые из HSS, а также тип поддерживаемого алгоритма аутентификации.

9. Когда P-CSCF получает сообщение 401, она удаляет ключи (XRES, IK, CK) из сообщения и сохраняет их.

10. После сохранения ключей P-CSCF передает сообщение 401 Unauthorized response к оборудованию пользователя.

11. Далее UE обрабатывает сообщение 401, вычисляет ответ на запрос авторизации, который вставляется в заголовок Authorization нового запроса Register, и отправляет новый запрос Register к P-CSCF на порт, полученный в ответе 401 Unauthorized response. Register содержит XRES, ключ шифрования CK, ключ целостности IK, вычисленные в UE. Также в заголовке Authorization передается тип поддерживаемого алгоритма аутентификации.

12. P-CSCF опять передает запрос Register к I-CSCF.

13. I-CSCF обращается к HSS домашней сети для выбора функционального объекта S-CSCF, который будет обслуживать данного пользователя. Это осуществляется с помощью обмена сообщениями протокола Diameter: User-Authorization-Request (UAR) и User-Authorization-Answer (UAA).

14. От HSS к I-CSCF посылается ответ User-Authorization-Answer, который содержит имя S-CSCF, если оно известно серверу HSS, или функциональные возможности S-CSCF, если выбор нового S-CSCF осуществляет I-CSCF.

15. I-CSCF после обращения к HSS передает запрос Register к S-CSCF.

16. S-CSCF сравнивает данные аутентификации, полученные ранее от HSS и от UE. В случае если данные аутентификации совпадают, S-CSCF передает сообщение Service Assigment Request (SAR) к HSS для загрузки данных пользователя из HSS и хранения их в S-CSCF.

17. S-CSCF получает ответ с данными Service Assigment Answer (SAA) от HSS.

18. После получения ответа S-CSCF подтверждает регистрацию и аутентификацию UE ответом 200 OK.

19. I-CSCF принимает ответ 200 OK и передает его к P-CSCF.

20. P-CSCF передает ответ к оборудованию пользователя UE.

Когда оборудование пользователя зарегистрировано, оно может инициировать и принимать сессии. При повторной регистрации аутентификация пользователя не требуется (рис. 1.6, б).

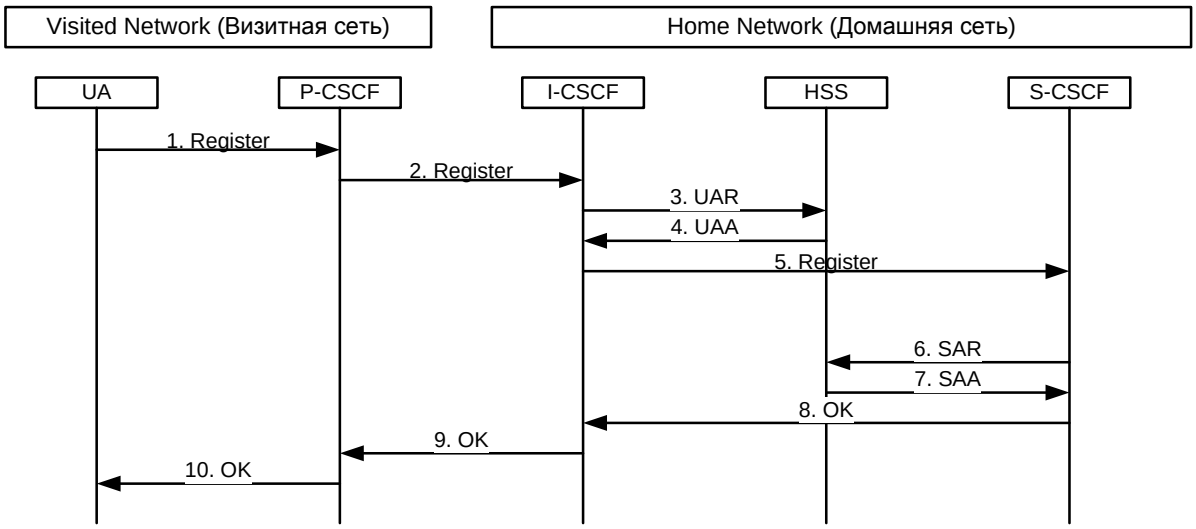

Рис. 1.6, б. Процедура регистрации пользователя в сети IMS

Информация, хранящаяся в элементах сети IMS до, во время и после процесса регистрации UE представлена в табл. 1.2.

Таблица 1.2

Элемент сети, UE	До регистрации	Во время регистрации	После регистрации
Терминал пользователя (UE) – в гостевой сети	Учетная запись с параметрами доступа пользователя, сформированными после его успешной аутентификации. Адрес домашнего домена. Имя/адрес P-CSCF	То же, что до регистрации	Учетная запись с параметрами доступа пользователя, сформированными после его успешной аутентификации. Адрес домашнего домена. Имя/адрес P-CSCF
P-CSCF – в домашней или гостевой сети	Функция маршрутизации	Начальная точка входа в домашнюю сеть. Адрес UE. PrUI, PuUI	Финальная точка входа в домашнюю сеть. Адрес UE. PrUI, PuUI
I-CSCF – в домашней сети	Адрес HSS или SLF	Адрес/имя S-CSCF. Идентификатор сети P-CSCF. Контактная информация о домашней сети	Никакой информации о состоянии
HSS	Профиль услуг пользователя	Идентификатор сети P-CSCF	Адрес/имя S-CSCF
S-CSCF – в домашней сети	Никакой информации о состоянии	Адрес/имя HSS. Профиль пользователя (ограниченный). Адрес/имя P-CSCF. Идентификатор сети P-CSCF. PrUI, PuUI. IP-адрес UE. Идентификатор GRUU для UE	Может храниться информация о состоянии сессии. То же, что во время регистрации

Отмена регистрации пользователя в сети IMS

Процедура отмены регистрации аналогична процедуре регистрации (рис. 1.7), только сообщение протокола SIP Register содержит заголовок Expires со значением времени регистрации, равным нулю, либо заголовок Contact с параметром expires равным нулю.

Регистрация множественных идентификаторов пользователя

Протокол SIP позволяет регистрировать за одну процедуру регистрации один идентификатор PuUI пользователя. Таким образом, если пользователь имеет несколько идентификаторов PuUI, он должен регистрировать каждый из них индивидуально. Для регистрации нескольких PuUI 3GPP разработан механизм множественной регистрации.

Множественная регистрация позволяет зарегистрировать группу идентификаторов PuUI с помощью одного запроса регистрации. PuUI идентификаторы объединяются в группы и, когда один из идентификаторов группы зарегистрирован, все PuUI идентификаторы, ассоциированные с ним, регистрируются в этот же момент. Когда для одного из идентификаторов отменяется регистрация, она отменяется и для всех идентификаторов группы.

1.9. Установление сессии в IMS

Сценарий (рис. 1.7) представляет процедуру установления мультимедийной сессии между зарегистрированными пользователями IMS, находящимися в домашних сетях.

Пользователь User A инициирует вызов к пользователю User B. Терминальное оборудование пользователя User A отправляет сообщение INVITE протокола SIP для запроса установления мультимедийной сессии с пользователем User B, содержащее описание сессии в формате SDP для передачи данных от User B к User A (тип передаваемых данных – видео, аудио), транспортный протокол (TCP,UDP), формат данных (H.261, MPEG), IP адрес устройства, адрес порта RTP, используемые кодеки).

P-CSCFA принимает запрос INVITE, заменяет в запросе INVITE заголовок P-Preferred-Identity на заголовок P-Asserted-Identity, содержащий зарегистрированный идентификатор PuUI вызывающего пользователя, добавляет в заголовок Route свой адрес и отправляет запрос к функциональному объекту S-CSCFA.

К оборудованию вызываемого пользователя P-CSCFA отправляет ответ с кодом 100 (Trying). Этот ответ информирует терминал о том, что запрос INVITE был получен, и прокси-сервер выполняет маршрутизацию запроса к месту назначения.

S-CSCFA на основании идентификатора пользователя User B, содержащегося в запросе INVITE, определяет входную точку в домашнюю сеть вызываемого пользователя I-CSCFB. После чего отправляет запрос INVITE к I-CSCFB, а к P-CSCFA ответ 100 (Trying). I-CSCFB обрабатывает запрос и обращается к базе пользователей HSS для получения адреса функции S-CSCF, обслуживающей пользователя User B (взаимодействие с HSS на рис. 1.8 не представлено).

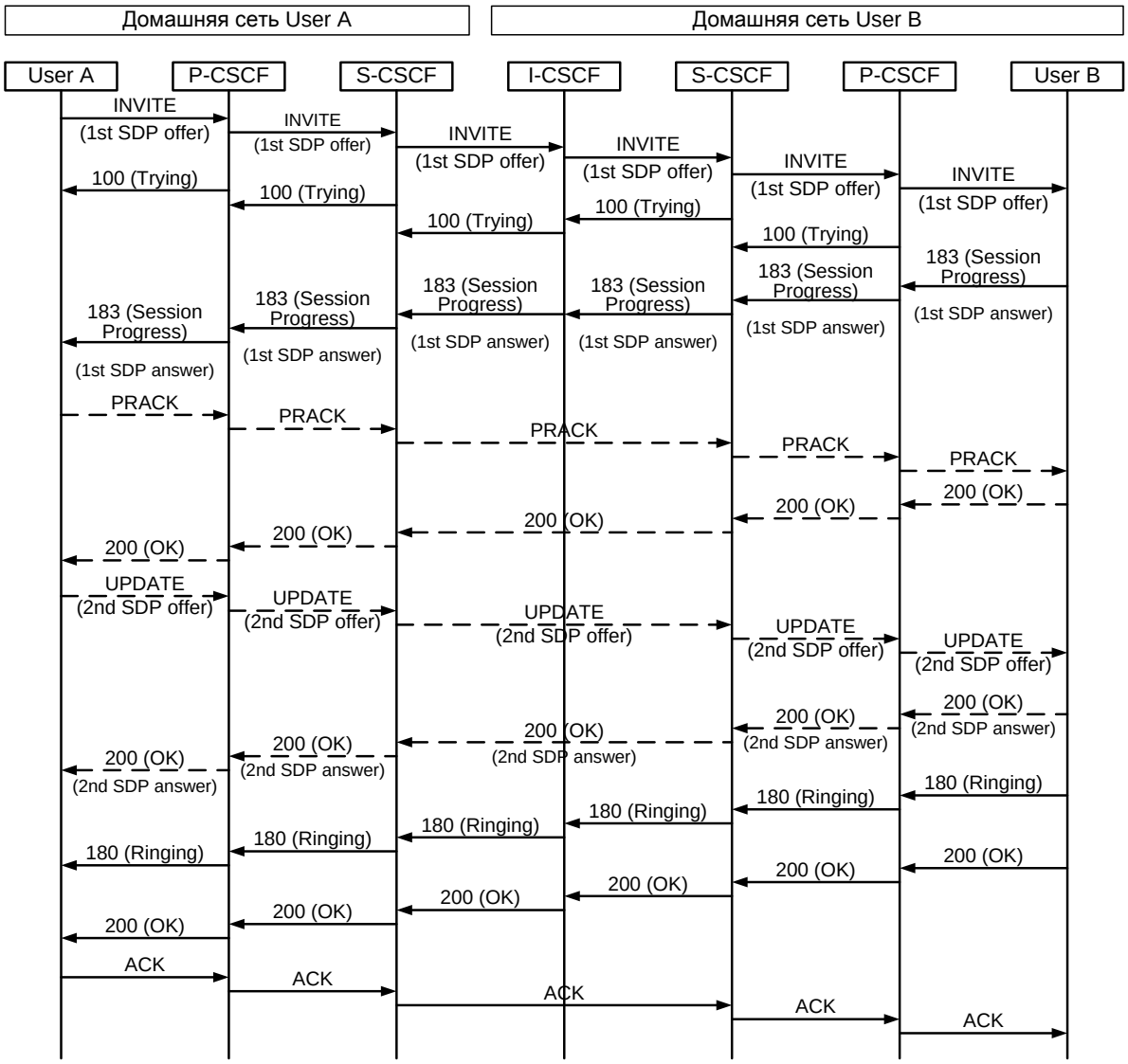

Рис. 1.7. Установление мультимедийного сеанса

После получения адреса I-CSCFB передает запрос INVITE к функции S-CSCFB, которая формирует ответ 100 (Trying) к I-CSCFB. S-CSCFB передает запрос уже к функции P-CSCFB, которая транслирует его к терминалу User B. Терминал вызываемого пользователя обрабатывает запрос INVITE и отправляет ответ 183 Session Progress, содержащий SDP-описание сессии для передачи мультимедийных данных от User A к User B.

Терминальное оборудование User A, получив ответ 183 Session Progress, анализирует предложенное SDP-описание сессии и отправляет запрос PRACK для информирования вызываемого пользователя User B о выбранных параметрах сессии (например, кодеках). Пользователь User B подтверждает принятие запроса PRACK ответом 200 OK. Затем пользователь User A отправляет запрос UPDATE для согласования параметров качества обслуживания QoS с пользователем User B и получает подтверждение – ответ 200 OK. При оповещении пользователя о входящем вызове терминал пользователя User B информирует об этом терминал пользователя User A с

помощью ответа с кодом 180 (Ringing), который маршрутизируется обратно через функциональные объекты сети IMS.

В приведённом примере User B решает ответить на вызов. Когда он поднимает трубку, его терминал отправляет ответ с кодом 200 OK, указывающий, что вызов принят. При получении ответа с кодом 200 терминал пользователя User A прекращает подачу сигнала КПВ и сообщает о том, что вызываемый пользователь принял вызов.

В итоге, терминал User A отправляет сообщение подтверждения ACK, для того чтобы подтвердить принятие окончательного ответа 200 OK. Это подтверждение завершает 3-этапную транзакцию INVITE/200/ACK, используемую для установления SIP-сессии. Медиасессия между User A и User B теперь считается установленной.

2. ИССЛЕДОВАТЕЛЬСКИЙ ПОЛИГОН ТЕХНОЛОГИЙ И ПРОТОКОЛОВ «СОТСБИ-У»

2.1. Назначение

Исследовательский полигон технологий и протоколов «СОТСБИ-У» предназначен для проведения практических и исследовательских работ по изучению сетей NGN. Исследовательский полигон позволяет организовать полноценную работу с реальным оборудованием, начиная от настройки оборудования до имитации и анализа различных ситуаций взаимодействия элементов полигона между собой.

2.2. Компоненты полигона СОТСБИ-У

Сеть NGN полигона СОТСБИ-У, используемая для проведения практических работ (рис. 2.1) по теме «Сети NGN. Оборудование IMS» состоит из следующих основных элементов:

- серверы, на которых установлено Ядро сети IMS OpenIMSCore и база пользователей HSS;
- рабочие места учащихся, оборудованные периферийными устройствами для приема и передачи мультимедийной информации (гарнитура и видеокамера).

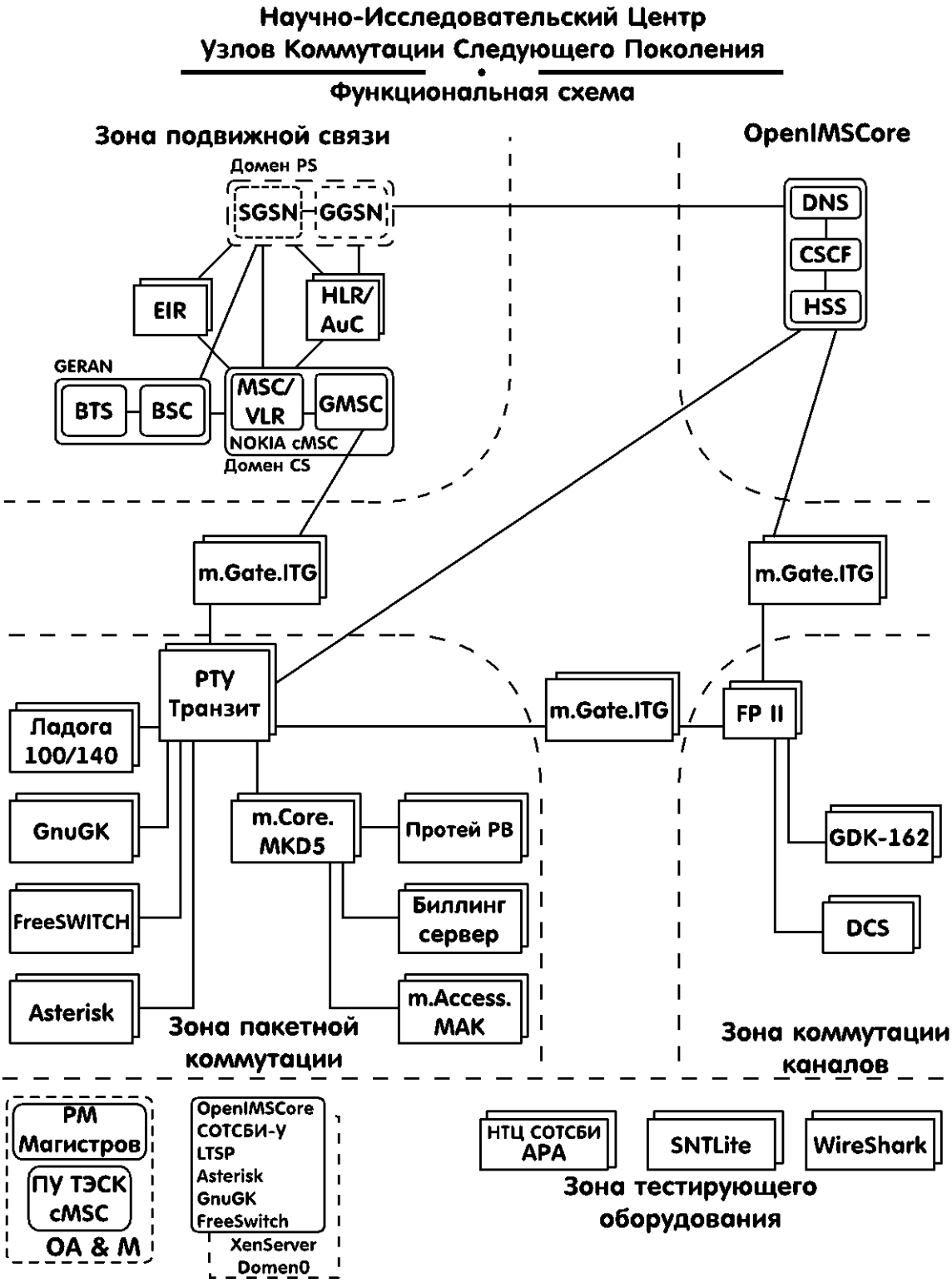

Рис. 2.1. Схема полигона СОТСБИ-У

Ядро сети IMS OpenIMSCore и база данных HSS

Мультимедийная подсистема на базе протокола IP Open Source IMS Core System разработана франкфуртским университетом FOKUS и полностью соответствует стандартам 3GPP, 3GPP2, ETSI TISPAN. Проект Open-

IMS Core был официально запущен 16 ноября 2006 года и создавался для целей проведения исследования и разработок в области технологии IMS.

OpenIMSCore состоит из функций управления сеансами CSCFs (P-CSCF, I-CSCF и S-CSCF) и базы данных пользователей HSS (рис. 2.2).

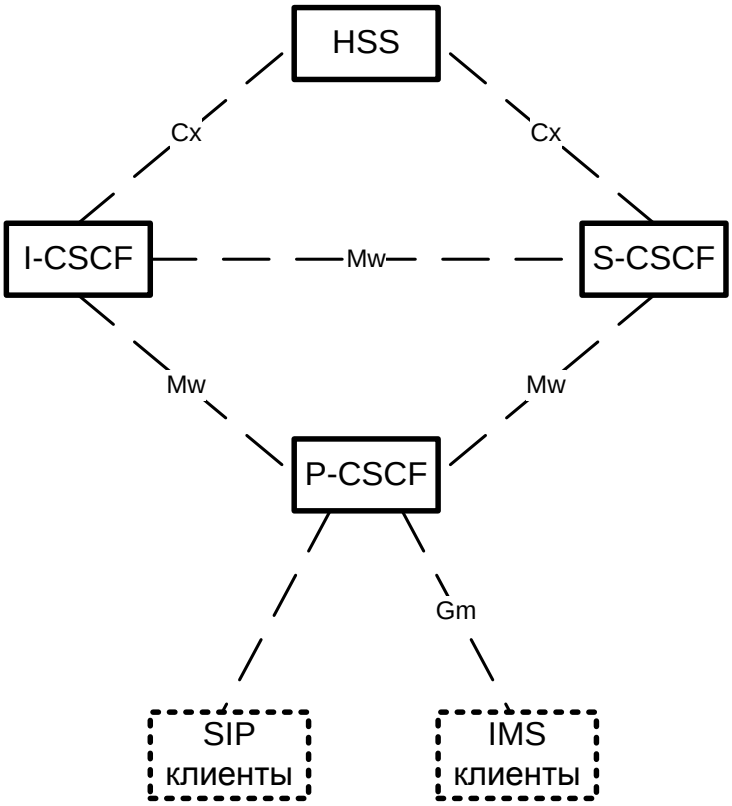

Рис. 2.2. Архитектура OpenIMSCore

Все компоненты являются открытыми программными продуктами со свободной лицензией GNU/GPL. Центральный компонент ядра сети IMS – функции P-CSCF, I-CSCF и S-CSCF были разработаны как расширение открытого программного SIP сервера SIP Express Router (SER).

Полноценное функционирование ядра сети IMS невозможно без сервера базы данных пользователей. Университет FOKUS разработал свой прототип пользовательских баз данных HSS, который использует для хранения пользовательских данных БД MySQL.

OpenIMSCore позволил создать IMS сеть полигона СОТСБИ-У, в которой можно создавать пользователей, регистрировать их и устанавливать различные мультимедийные сессии.

Рабочее место

Рабочее место магистра для выполнения практических работ представляет собой совокупность аппаратных и программных средств. Аппаратные средства представлены персональным компьютером и набором пе-

риферийных устройств, в том числе для приема и передачи мультимедийной информации (гарнитура и видеокамера). Программные средства представлены программным IMS терминалом Monster, средствами программного мониторинга сетевого трафика Wireshark, программными SIP телефонами SJPhone, Ekiga, Linphone и Twinkle.

На рабочем столе персонального компьютера (рис. 2.3) расположены следующие ярлыки:

- ярлык для запуска программы мониторинга сетевого трафика Wireshark локально (ярлык «Wireshark»);
- ярлык для запуска программы мониторинга сетевого трафика Wireshark на SIP-сервере (ярлык «Wireshark на сервере»);
- ярлык для запуска программного IMS терминала Monster;
- ярлык для запуска программного телефона SJPhone;
- ярлык для запуска программного телефона Ekiga;
- ярлык для запуска программного телефона Twinkle;
- ярлык для запуска программного телефона Linphone;
- ярлык среды эмуляции СОТСБИ-SIPp;
- ярлык для запуска трафик-генератора СОТСБИ-АРА;
- ярлык для запуска web-интерфейса IP PBX Asterisk – СОТСБИ-X;
- ярлык для запуска web-интерфейса OpenIMSCore HSS;
- ярлык электронной библиотеки СОТСБИ-Lib, содержащей различную дополнительную литературу, необходимую при выполнении практической и исследовательской работы – Библиотека.

Имена и IP-адреса рабочих мест указаны на табличках рядом с персональным компьютером.

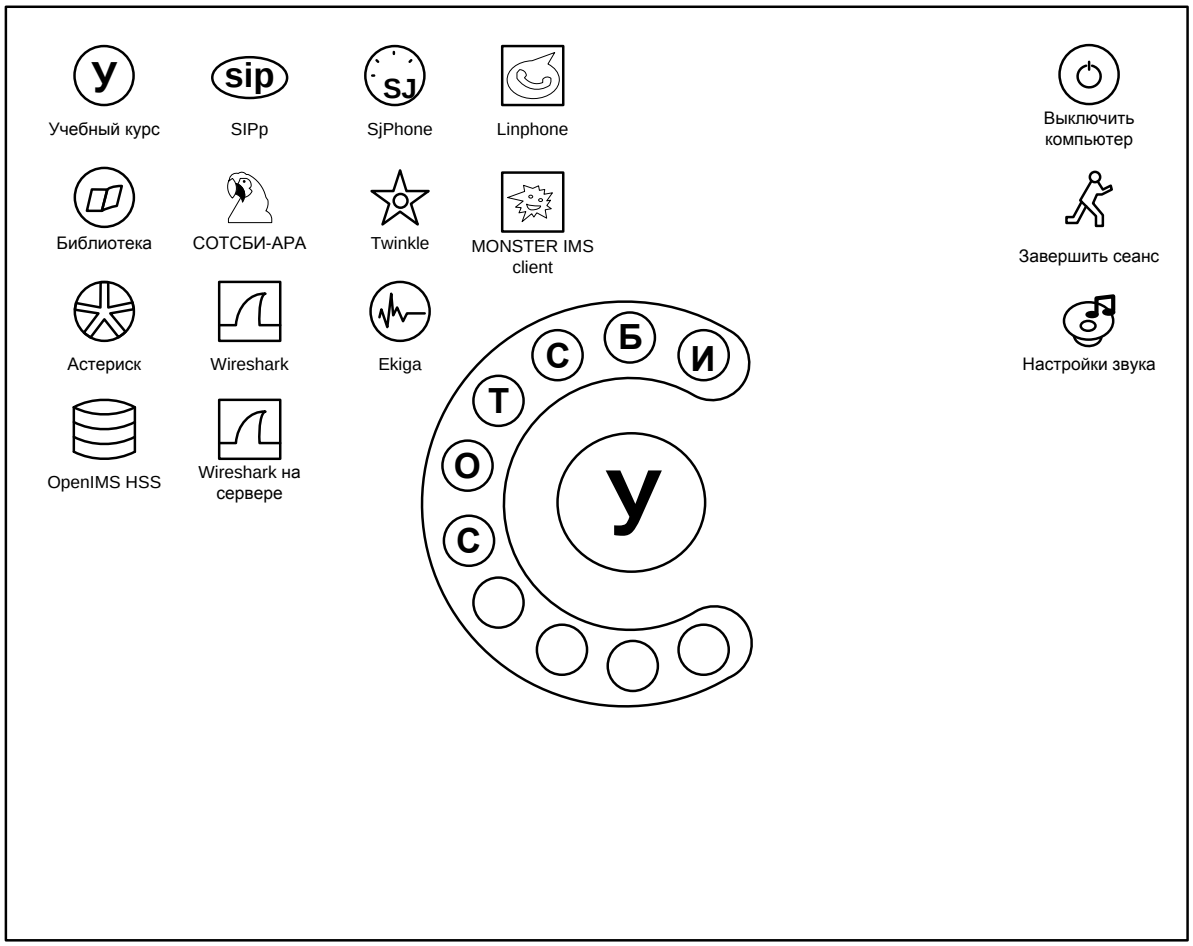

Рис. 2.3. Рабочий стол

3. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

Для выполнения практических занятий формируются бригады из расчета по 3 рабочих места на одну бригаду (далее РМ1, РМ2, РМ3).

При выполнении практических заданий используются следующие элементы сети IMS полигона СОТСБИ-У:

- сервер пользователей сети IMS – HSS;
- сервера P-CSCF, I-CSCF и S-CSCF, основными функциями которых являются регистрация пользователей и установление мультимедийных сессий;
- IMS терминал – программный IMS клиент Monster.

Перед выполнением заданий необходимо ознакомится с пользовательским интерфейсом программы мониторинга сетевого трафика Wireshark, программных телефонов, используемых на полигоне СОТСБИ-У.

Перед началом практической работы, а также после ее завершения, убедится, что настройки всех программных продуктов находятся в исходном состоянии.

3.1. Лабораторная работа 1. Процедура регистрации

Регистрация является основной процедурой любой сети IMS. Если пользователи не зарегистрированы, тогда они не смогут получить доступ к любым сервисам сети. Для успешной регистрации пользователь должен обладать определенными регистрационными данными, а сеть, в которой производится процесс регистрации, должна быть доступна для приема этих регистрационных данных. Данная лабораторная работа состоит из нескольких заданий, главная цель которой – проанализировать процедуру регистрации в сети IMS, определить основные элементы сети IMS, участвующие в процедуре регистрации, и протоколы взаимодействия.

Задание 1.1. Создание пользователя

Прежде чем зарегистрировать пользователя в сети IMS необходимо создать информацию об этом пользователе в базе данных пользователей HSS. Создание пользователей, редактирование и управление конфигурационными данными пользователей в HSS осуществляется с помощью web-интерфейса.

1. Запуск web-интерфейс HSS.

Для запуска веб-интерфейса необходимо нажать на ярлык OpenIMS HSS, расположенный на рабочем столе (рис. 2.2). В окне браузера появится окно авторизации пользователя (рис. 3.1), в котором необходимо ввести логин и пароль. В поле User Name необходимо ввести логин – hssAdmin. В поле Password необходимо ввести пароль – hss.

После авторизации пользователя появляется главная страница графического интерфейса HSS (рис. 3.2).

В верхней части страницы перечислены пункты меню: Главная, Пользователи IMS, Услуги, Конфигурация сети, Статистика.

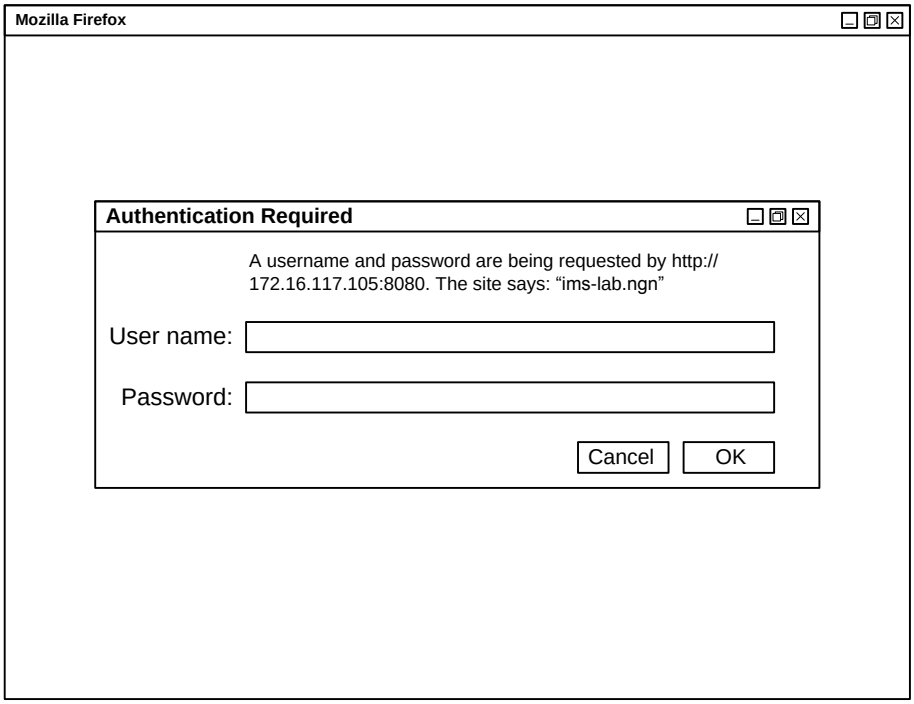

Рис. 3.1. Окно авторизации пользователя

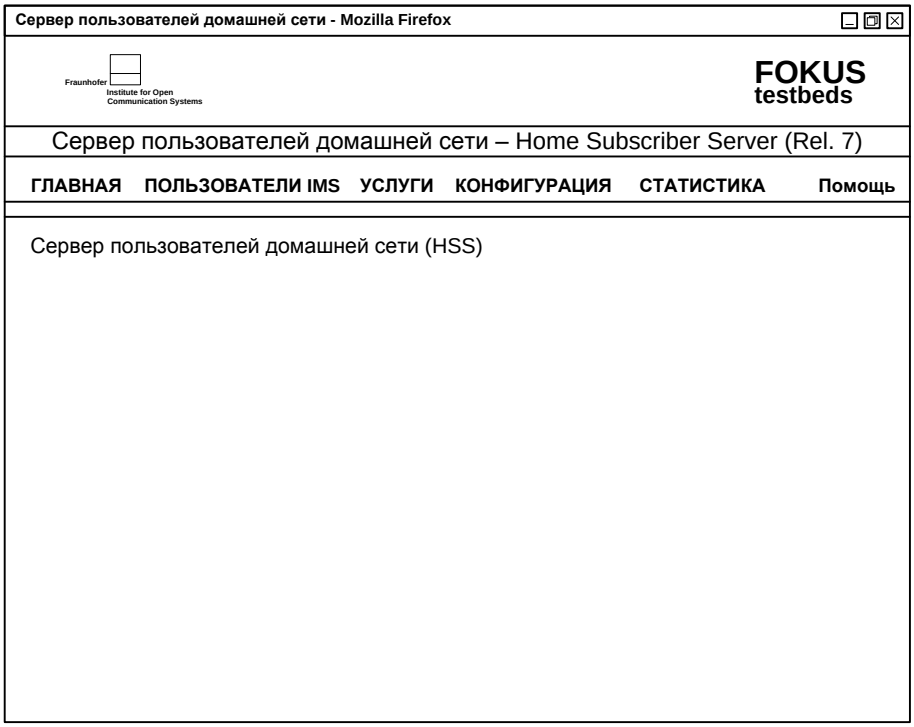

Рис. 3.2. Графический интерфейс OpenIMS HSS

2. Создание пользователя с именем User1[1] и паролем User1.

Для создания информации о пользователе в базе данных пользователей HSS необходимо выбрать пункт меню Пользователи IMS (рис. 3.3).

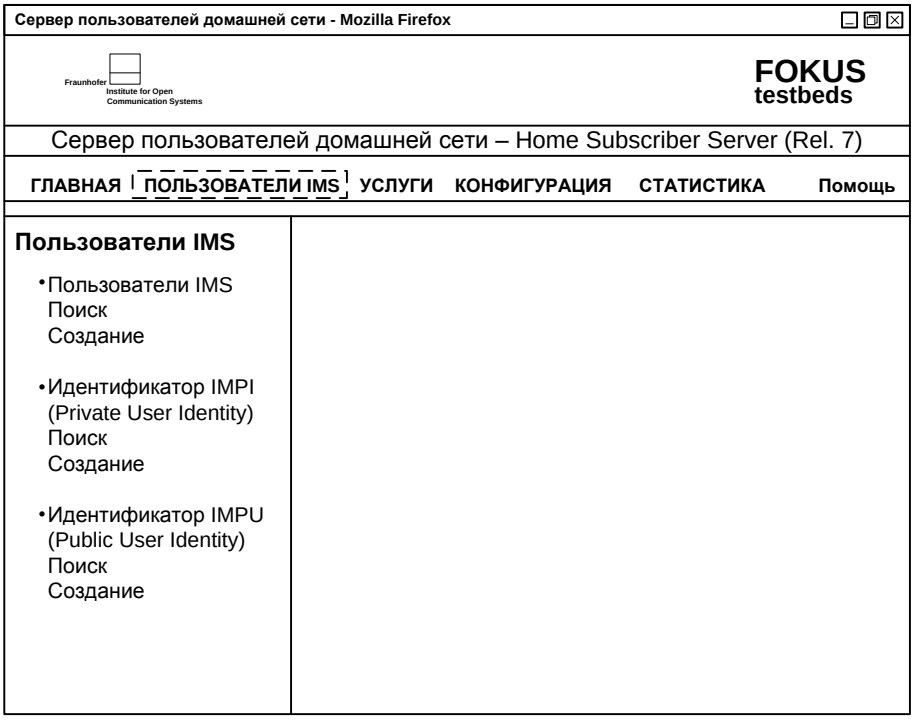

Рис. 3.3. Меню Пользователи IMS

Затем выбрать подпункт меню Пользователи IMS – Создание. В появившемся окне отображается таблица, поля которой необходимо заполнить (рис. 3.4).

[1] User2 – фамилия одного участника бригады, написанная строчными английскими буквами.

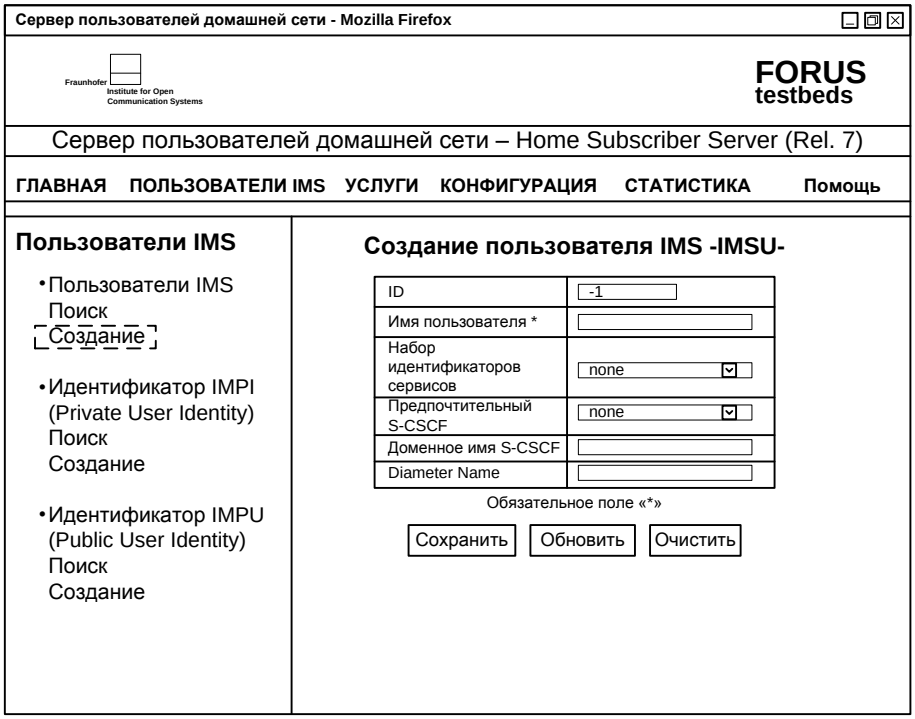

Рис. 3.4. Создание пользователя IMS

В поле «Имя пользователя» необходимо ввести имя пользователя User1[2] английскими строчными буквами. В поле Набор идентификаторов сервисов необходимо выбрать значение cap_set1, а в поле Предпочтительный S-CSCF необходимо выбрать значение scscf1 и нажать кнопку «Сохранить».

Далее необходимо прописать идентификатор Private User Identity для создаваемого пользователя. Для этого необходимо нажать значок «+», расположенный справа от пункта Создание и присвоение нового идентификатора IMPI (рис. 3.5).

[2] User1 – фамилия одного участника бригады.

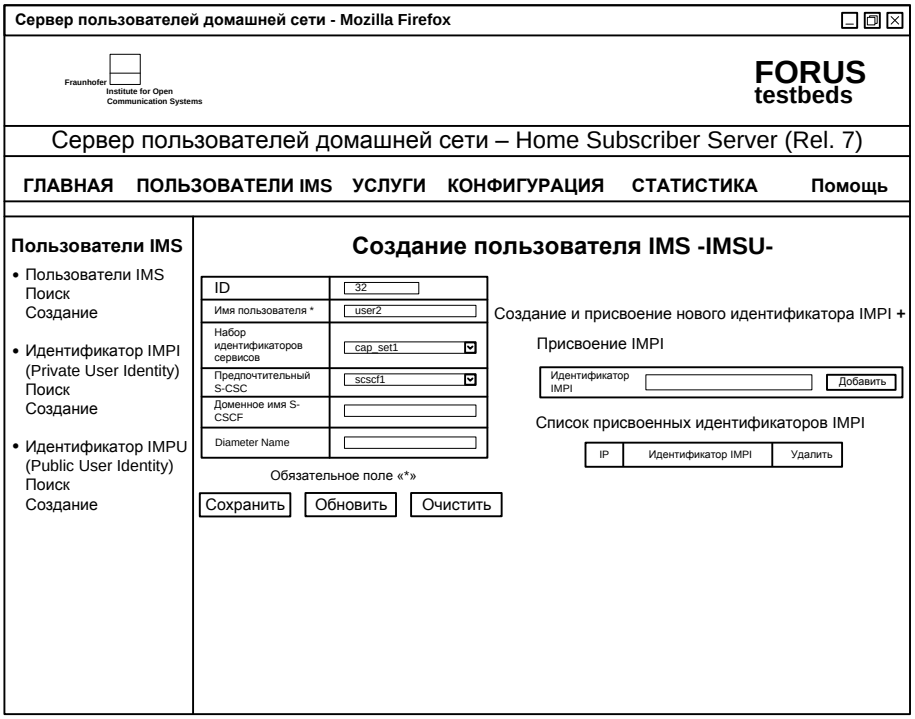

Рис. 3.5. Создание идентификатора Private User Identity

В появившемся окне в поле Идентификатор IMPI необходимо ввести идентификатор Private User Identity вида ***user1@ims-lab.ngn*** (рис. 3.6). В поле Секретный ключ необходимо ввести пароль user1[3] для доступа создаваемого пользователя в сеть. Затем выбрать все алгоритмы аутентификации, отметив соответствующее поле «галочкой», а из выпадающего списка «По умолчанию» выбрать Digest–AKAv1–MD5 и нажать кнопку «Сохранить».

Затем необходимо прописать идентификатор Public User Identity для создаваемого пользователя. Для этого необходимо нажать значок «+», расположенный справа от пункта Создание и присвоение нового идентификатора IMPU (рис. 3.7).

[3] User1 – фамилия одного участника бригады, написанная строчными английскими буквами.

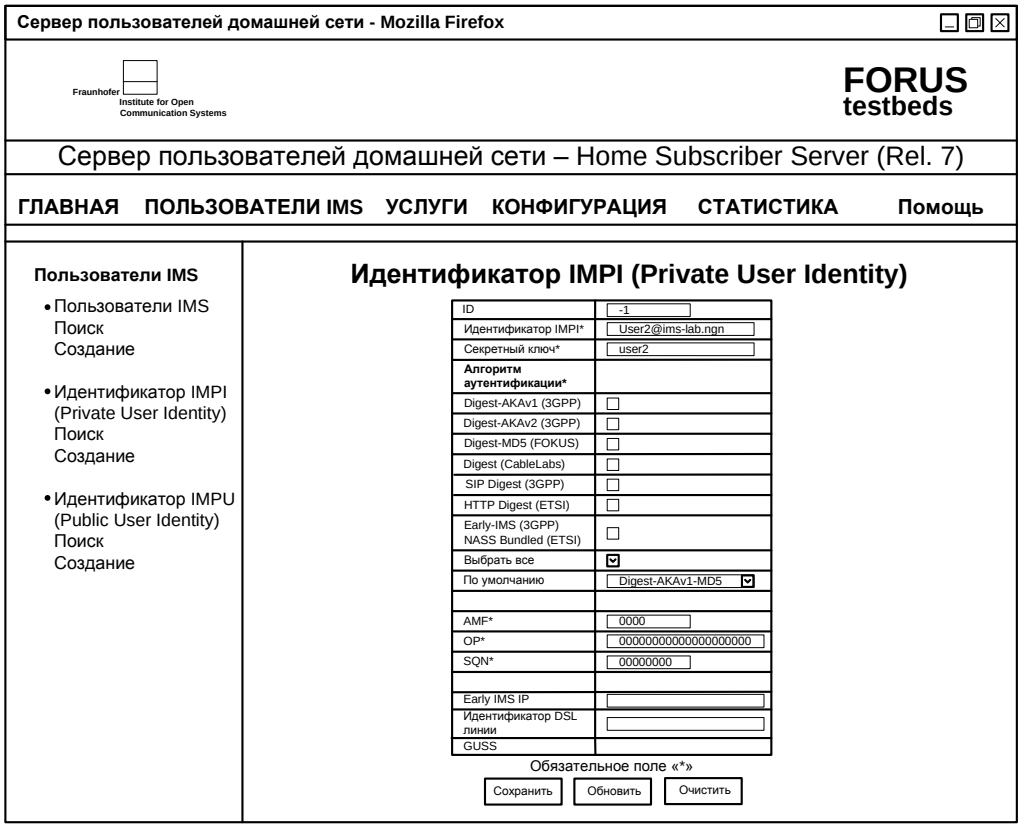

Рис. 3.6. Параметры идентификатора Private User Identity

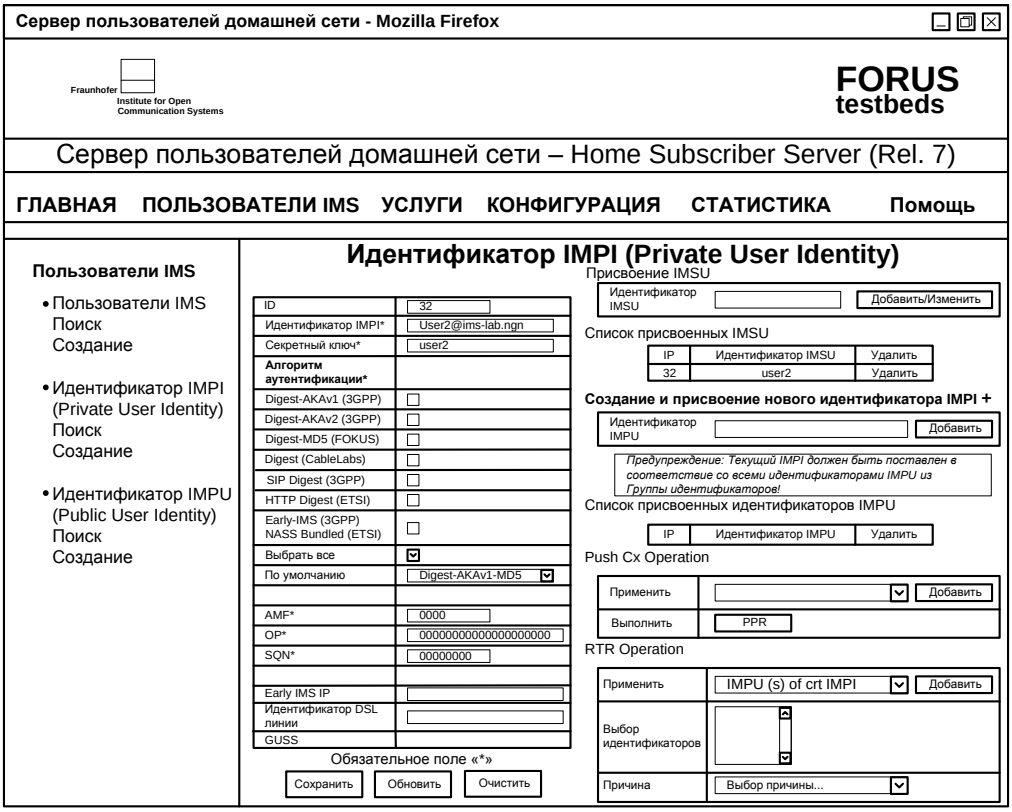

Рис. 3.7. Создание идентификатора Public User Identity

В появившемся окне в поле Идентификатор IMPU необходимо ввести идентификатор Public User Identity вида ***sip:user1@ims-lab.ngn*** (рис. 3.8). Из выпадающего списка поля Профиль обслуживания выбрать значение default_sp. Для поддержки возможности регистрации установить «галочку» в поле Разрешить регистрацию. В поле Тип IMPU выбрать значение Public_User_Identity, а в поле Отображаемое имя пользователя ввести отображаемое имя создаваемого пользователя user1 и нажать кнопку «Сохранить».

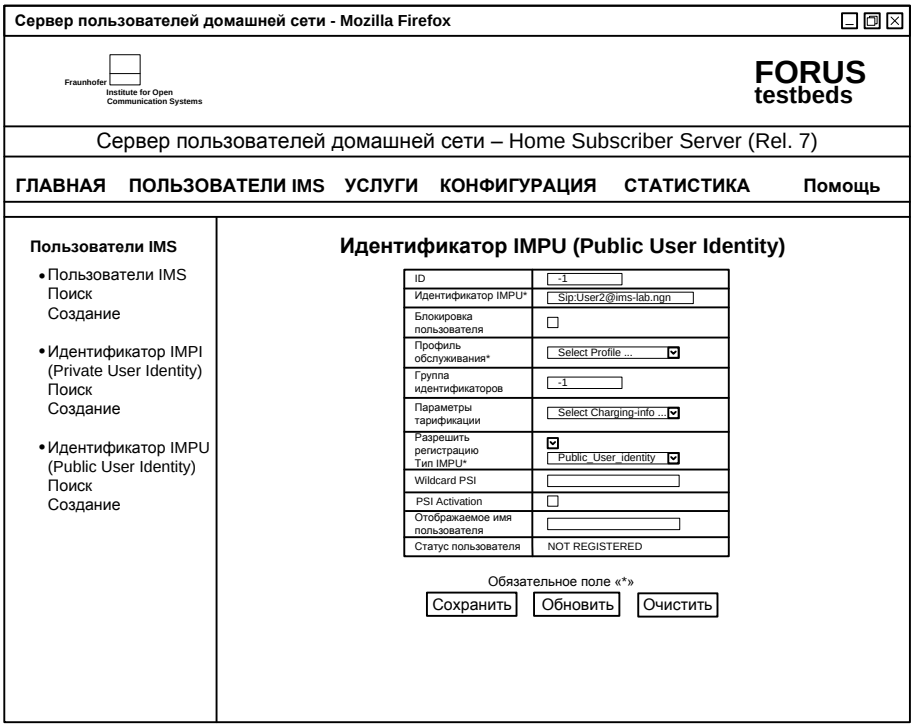

Рис. 3.8. Параметры идентификатора Public User Identity

В поле Добавить визитные сети необходимо выбрать значение ***ims-lab.ngn,*** нажать кнопку «Добавить» (рис. 3.9) и далее – кнопку «Сохранить».

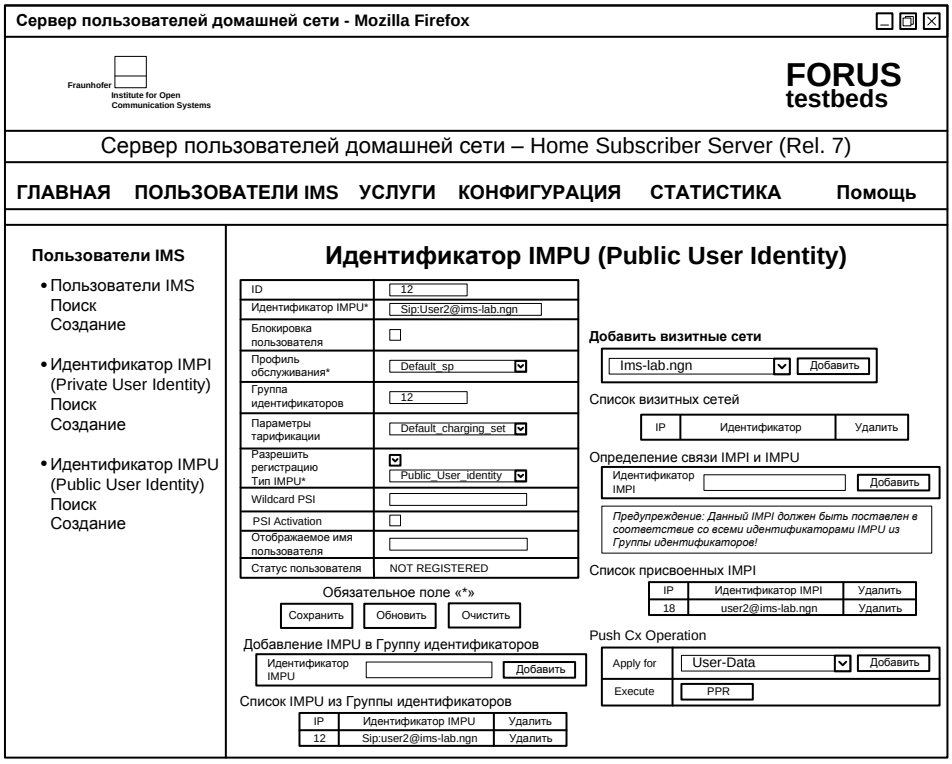

Рис. 3.9. Добавление сети

3. Создать пользователя с именами User2 и паролями User2[4], заполнив соответствующие поля меню web-интерфейса аналогично п. 2.

Задание 1.2. Регистрация

Определение местоположения пользователя сети IMS в текущий момент осуществляется с помощью процедуры регистрации. Так как пользователь регистрируется в сети IMS впервые, то ему необходимо пройти процедуру аутентификации.

1. Запустить Wireshark.
2. Настроить терминалы PM 1, 2 (IMS Monster).
3. На терминалах PM 1, 2 последовательно активировать учетные записи с именами пользователей, созданных в задании 1.1.
4. Проанализировать трейсы, полученные с помощью программы Wireshark (составление отчета):

- определить элементы сети IMS, участвующие в процедуре регистрации пользователей сети, и протоколы взаимодействия;
- указать алгоритм обмена сообщениями между элементами сети IMS для процедуры регистрации и отмены регистрации;
- определить протокол взаимодействия с базой данных пользователей HSS и указать назначение передаваемых сообщений;

[4] User2 – фамилия второго участника бригады.

- определить, в заголовке какого сообщения и протокола передается идентификатор пользователя Public User Identity при регистрации;
- определить в заголовке, какого сообщения, какого протокола передается идентификатор пользователя Private User Identity при регистрации;
- определить заголовок, содержащий контактный адрес пользователя при регистрации;
- определить отличия запросов REGISTER, отправляемого при инициировании процедуры регистрации и отправляемого в ответ на сообщение 401 Unauthorized;
- определить используемый алгоритм аутентификации;
- проанализировать значение заголовка Expires в запросах REGISTER;
- определить окончательный ответ при регистрации пользователя.

Задание 1.3. Отказ в регистрации

В случае если данные пользователя не прописаны в базе данных HSS, то данный пользователь не сможет зарегистрироваться в сети IMS.

1. Запустить Wireshark.
2. Настроить терминал PM1 (IMS Monster).
3. На терминале PM1 активировать учетную запись с именем пользователя, не прописанным в базе данных пользователей HSS.
4. Проанализировать трейсы, полученные с помощью программы Wireshark (составление отчета):
   - определить ответ на запрос регистрации REGISTER;
   - определить сообщение протокола Diameter, передаваемое базой данных пользователей HSS и информирующее о невозможности регистрации пользователя;
   - сравнить сценарий обмена сообщениями при отказе в регистрации со сценарием обмена сообщениями при успешной регистрации (см. задание 1.2), объяснить причины отличия.
5. На терминале PM1 активировать учетную запись с именем пользователя, прописанным в базе данных пользователей HSS (с именами пользователей, созданных в задании 1.1), но ввести неверный пароль.
6. Проанализировать трейсы, полученные с помощью программы Wireshark (составление отчета):
   - определить ответ на запрос регистрации REGISTER;
   - сравнить сценарий обмена сообщениями при отказе в регистрации со сценарием обмена сообщениями при успешной регистрации (см. задание 1.2), объяснить причины отличия.

Задание 1.4. Мобильность пользователя

Рассмотреть роль процедуры регистрации при реализации услуги персональной мобильности пользователя в сети и при реализации ситуации, когда пользователь доступен по нескольким адресам.

1. Смоделировать ситуацию, когда в сети одновременно активирована одна и та же учетная запись на двух разных терминалах:

- активировать учетную запись с именем пользователя, прописанным в базе данных пользователей HSS, на PM3;
- активировать другую учетную запись с именем пользователя, прописанным в базе данных пользователей HSS, на PM1 и осуществить вызов этого пользователя с PM3;
- активировать эту же учетную запись на PM2 и осуществить вызов пользователя с PM3.

2. Проанализировать трейсы, полученные с помощью программы Wireshark (составление отчета):

- определить поведение элементов сети IMS в смоделированной ситуации;
- указать алгоритм обмена сообщениями между элементами сети IMS для данной ситуации.

Задание 1.5. Регистрация пользователя с SIP-терминала (SJPhone, Twinkle)

1. Запустить Wireshark.
2. Попытаться осуществить регистрацию пользователей сети IMS, имена которых прописаны в базе данных HSS, с SIP-терминалов SJPhone и Twinkle (использовать на одном PM софтфон Twinkle, а на другом SJPhone).
3. Проанализировать трейсы, полученные с помощью программы Wireshark (составление отчета):

- сравнить сценарий обмена сообщениями при регистрации пользователя с SIP-терминала со сценарием обмена сообщениями при успешной регистрации (см. задание 1.2), объяснить причины отличия.

3.2. Лабораторная работа 2. Типы сессий в IMS

Задание 2.1. Аудиосессия

1. Настроить терминалы (IMS Monster) на PM1, PM2.
2. Запустить Wireshark.
3. Осуществить вызов от пользователя PM1 к пользователю PM2.
4. Ответ пользователя PM2, разговор, отбой пользователя PM1.

5. Определить элементы сети IMS, участвующие в процессе установления и поддержания мультимедийной сессии, по трейсам с помощью программы Wireshark.

6. Определить сообщения SIP (запросы и ответы), отправленные для установления сессии, по трейсам с помощью программы Wireshark.

7. Анализ участвовавших в соединении запросов и ответов SIP (составление отчета):

- определить идентификатор Public User Identity вызывающего пользователя;
- определить идентификатор Private User Identity вызываемого пользователя;
- определить Идентификатор сессии;
- определить заголовок, в котором передается название терминала пользователя (вызываемого, вызывающего);
- определить длительность фазы установления соединения, фазы разговора, используя данные о времени отправки пакетов; (предполагается, что задержка прохождения пакетов по сети – нулевая);
- определить параметры мультимедийной сессии: параметры передачи речи (используемый кодек, номер порта для обработки медиаинформации на стороне вызывающего пользователя, номер порта для обработки медиаинформации на стороне вызываемого пользователя).

Задание 2.2. Видеосессия

1. Настроить терминалы (IMS Monster) на PM1, PM2.
2. Запустить Wireshark.
3. Осуществить видео вызов от пользователя PM1 к пользователю PM2.
4. Ответ пользователя PM2, разговор, отбой пользователя PM1.
5. Определить элементы сети IMS, участвующие в процессе установления и поддержания мультимедийной сессии, по трейсам с помощью программы Wireshark.
6. Определить сообщения SIP (запросы и ответы), отправленные для установления сессии, по трейсам с помощью программы Wireshark.
7. Анализ участвовавших в соединении запросов и ответов SIP (составление отчета):

- определить сообщение, содержащее предлагаемые параметры мультимедийной сессии;
- определить параметры мультимедийной сессии:
  - параметры передачи речи (используемый кодек, номер порта для обработки медиаинформации на стороне вызывающего пользователя, номер порта для обработки медиаинформации на стороне вызываемого пользователя);

- параметры передачи видео (используемый кодек, номер порта для обработки медиаинформации на стороне вызывающего пользователя, номер порта для обработки медиаинформации на стороне вызываемого пользователя).

Задание 2.3. Текстовая сессия

В рамках текстовой сессии рассматриваются две услуги: Chat (чат) и Instant message (передача мгновенного сообщения).

Услуга Chat (чат)

1. Настроить терминалы (IMS Monster) на PM1, PM2.
2. На PM1 запустить Wireshark на сервере, а на PM2 – локально.
3. Осуществить обмен текстовыми сообщениями в режиме реального времени (чат) между пользователем PM1 и пользователем PM2.
4. Определить элементы сети IMS, участвующие в процессе реализации услуги, по трейсам с помощью программы Wireshark.
5. Определить сообщения SIP (запросы и ответы), отправленные для установления сессии, по трейсам с помощью программы Wireshark.
6. Анализ участвовавших в соединении запросов и ответов SIP (составление отчета);

- определить параметры мультимедийной сессии;
- определить протокол, используемый для передачи тестовых сообщений.

Услуга Instant message

1. Настроить терминалы (IMS Monster) на PM1, PM2.
2. Запустить Wireshark.
3. Отправить мгновенное сообщение от пользователя PM1 к пользователю PM2.
4. Определить элементы сети IMS, участвующие в процессе реализации услуги, по трейсам с помощью программы Wireshark.
5. Анализ участвовавших в соединении запросов и ответов SIP (составление отчета);

- определить и проанализировать сообщения SIP (запросы и ответы), отправленные при передаче мгновенного сообщения, по трейсам с помощью программы Wireshark;
- определить заголовок, содержащий информацию о типе передаваемых данных;
- проанализировать тело сообщения, отправленного для передачи мгновенного сообщения.

Определить основные отличия услуг Chat и Instant message. Дать краткое определение каждой услуге.

Задание 2.4. Файловая сессия

File Transfer – услуга по передаче файлов с одного устройства на другое. Файл может быть передан или получен как с компьютера, так и с мобильного телефона. Файл может передаваться одному или нескольким пользователями.

1. Настроить терминалы (IMS Monster) на PM1, PM2.
2. Запустить Wireshark.
3. Отправить любой файл от пользователя PM1 к пользователю PM2.
4. Определить элементы сети IMS, участвующие в процессе передачи файла, по трейсам с помощью программы Wireshark.
5. Анализ участвовавших в соединении запросов и ответов SIP (составление отчета);

- определить сообщения SIP (запросы и ответы), отправленные при передаче файла, по трейсам с помощью программы Wireshark;
- определить протокол, по которому осуществляется передача файла;
- проанализировать тела сообщений, отправленные при передаче файла.

Задание 2.5. Изменение параметров сессии

Аудиосессия

1. Настроить терминалы (IMS Monster) на PM1, PM2.
2. На PM1 запустить Wireshark на сервере, а на PM2 запустить Wireshark локально.
3. Осуществить аудио вызовы от пользователя PM1 к пользователю PM2, используя последовательно 3 типа аудиокодеков.
4. По трейсам с помощью программы Wireshark:

- определить протокол, используемый для передачи параметров мультимедийной сессии;
- определить протокол, предназначенный для передачи аудиоинформации по сети IMS;
- определить путь передачи RTP трафика.

5. В полученном с помощью программы Wireshark трейсе отфильтровать пакеты по протоколу RTP и с помощью меню Statistics – Summary определить величину полосы пропускания и сопоставить с величиной скорости передачи (кбит/с) используемого кодека.
6. С помощью меню Telephony – RTP – Stream Analysis программы Wireshark определить джиттер, потери пакетов RTP, общее число пакетов RTP, переданных вызывающей и вызываемой сторонами.
7. Осуществить аудиовызовы от пользователя PM1 к пользователю PM2, используя на вызывающей и вызываемой сторонах разные типы аудиокодеков.

8. Сделать вывод о зависимости возможности установления мультимедийной сессии от ее параметров.

Видеосессии

1. Настроить терминалы (IMS Monster) на PM1, PM2.
2. На PM1 запустить Wireshark на сервере, а на PM2 запустить Wireshark локально.
3. Осуществить видеовызовы от пользователя PM1 к пользователю PM2, используя последовательно 3 типа видеокодеков.
4. По трейсам с помощью программы Wireshark:

- определить протокол, используемый для передачи параметров мультимедийной сессии;
- определить протокол, предназначенный для передачи видеоинформации по сети IMS;
- определить путь передачи RTP трафика.

5. В полученном с помощью программы Wireshark трейсе отфильтровать пакеты по протоколу RTP и с помощью меню Statistics – Summary определить величину полосы пропускания и сопоставить с величиной скорости передачи (кбит/с) используемого кодека.
6. С помощью меню Telephony – RTP – Stream Analysis программы Wireshark определить джиттер, потери пакетов RTP, общее число пакетов RTP, переданных вызывающей и вызываемой сторонами.
7. Осуществить видеовызовы от пользователя PM1 к пользователю PM2, используя на вызывающей и вызываемой сторонах разные типы видеокодеков.
8. Сделать вывод о зависимости возможности установления мультимедийной сессии от ее параметров.

3.3. Лабораторная работа 3. Мультимедийные сессии

Одной из функциональных возможностей подсистемы IMS является поддержка мультимединых сессий для предоставления широкого спектра услуг. С появлением IMS становится возможным комбинировать различные медиасреды: голос, видео и графику.

Задание 3.1. Аудиосессия с передачей файлов

Реализовать на базе полигона СОТСБИ-У следующую ситуацию. Пользователи **А** и **Б** являются зарегистрированными пользователями сети IMS и находятся в сети. Пользователь **А** устанавливает аудиосессию с пользователем **Б**. В процессе разговора пользователь **А** передает пользователю **Б** файл. При завершении разговора пользователь **Б** осуществляет отбой.

1. Запустить Wireshark.
2. Реализовать на базе полигона СОТСБИ-У, описанную ситуацию.
3. По трейсам с помощью программы Wireshark:

- определить элементы сети IMS, участвующие в процессе организации услуги.
- определить сообщения SIP (запросы и ответы), отправленные для установления аудиосессии и передачи файлов.
- составить диаграмму обмена сообщениями SIP между всеми участниками сессии.

Задание 3.2. Аудиосессия с передачей мгновенного сообщения Instant message

Реализовать на базе полигона СОТСБИ-У следующую ситуацию. Пользователи **А**, **Б** и **В** являются зарегистрированными пользователями сети IMS и находятся в сети. Пользователь **А** устанавливает аудиосессию с пользователем **Б**. В процессе разговора пользователь **А** отправляет мгновенное сообщение пользователю **В** с вопросом о его местонахождении. Пользователь **В** получает сообщение и отправляет мгновенное сообщение пользователю **А** с ответом. Разговор между пользователями **А** и **Б** продолжается, и при завершении разговора пользователь **Б** осуществляет отбой.

Для реализации услуги необходимо использовать третий IMS-терминал, задействуется дополнительное рабочее место, свободное на данный момент.

1. Запустить Wireshark.
2. Реализовать на базе полигона СОТСБИ-У описанную выше ситуацию.
3. По трейсам с помощью программы Wireshark:

- определить элементы сети IMS, участвующие в процессе организации услуги.
- определить сообщения SIP (запросы и ответы), отправленные для установления аудиосессии и передачи мгновенных сообщений.
- составить диаграмму обмена сообщениями SIP между всеми участниками сессии.

Задание 3.3. Видеосессия и передача текстовых сообщений чата (Chat)

Реализовать на базе полигона СОТСБИ-У следующую ситуацию. Пользователи **А, Б** и **В** являются зарегистрированными пользователями сети IMS и находятся в сети. Пользователь **А** устанавливает видеосессию с пользователем **Б**. В процессе видеосессии пользователь **А** получает текстовое сообщение в чате от пользователя **В**. Пользователь **А** отправляет ответ пользователю **В**. Разговор между пользователями **А** и **Б** продолжается, и при завершении разговора пользователь **Б** осуществляет отбой.

Для реализации услуги необходимо использовать третий IMS-терминал, задействуя дополнительное рабочее место, свободное на данный момент.

1. Запустить Wireshark.
2. Реализовать на базе полигона СОТСБИ-У описанную выше ситуацию.
3. По трейсам с помощью программы Wireshark:

- определить элементы сети IMS, участвующие в процессе организации услуги;
- определить сообщения SIP (запросы и ответы), отправленные для установления видеосессии и передачи текстовых сообщений чата;
- составить диаграмму обмена сообщениями SIP между всеми участниками сессии.

3.4. Лабораторная работа 4. Дополнительные услуги

Задание 4.1. Постановка на удержание (Call Hold, CH)

Услуга Call Hold позволяет пользователю временно прервать передачу медиаинформации для того, чтобы инициировать новый исходящий вызов или ответить на входящий вызов, а затем вновь восстановить первоначально прерванный сеанс. Услугой может воспользоваться как вызывающая, так и вызываемая сторона соединения.

1. Запустить Wireshark.
2. Установить соединение от пользователя PM1 к пользователю PM2.
3. С терминала PM1 поставить вызов на удержание.
4. С терминала PM1 снять вызов с удержания.
5. Анализ полученных трейсов (составление отчета):

- определить запрос, осуществляющий постановку вызова на удержание, проанализировать параметры мультимедийного сеанса в этом запросе, определить их отличие от параметров мультимедийного сеанса в первом запросе INVITE;
- определить запрос, снимающий вызов с удержания, проанализировать параметры мультимедийного сеанса в этом запросе, определить их отличие от параметров мультимедийного сеанса в первом запросе INVITE;
- определить время, в течение которого пользователь находится на удержании;
- составить диаграмму обмена сообщениями SIP между всеми участниками сессии.

Задание 4.2. Услуга «Не беспокоить» (Do not Disturb, DND)

Если на IMS терминале активирована услуга «Не беспокоить», то при поступлении входящего вызова он выдает информацию о том, что пользователь занят.

1. Запустить Wireshark.
2. Активировать на терминале PM2 услугу «Не беспокоить».
3. Осуществить вызов с терминала PM1 на терминал PM2.

4. Анализ полученных трейсов (составление отчета): определить окончательный ответ на запрос INVITE, и составить диаграмму обмена сообщениями SIP между всеми участниками сессии.

Задание 4.3. Перевод вызова (Explisit Call Transfer, ECT)

Для реализации услуги необходимо использовать третий IMS-терминал, задействуется дополнительное рабочее место, свободное на данный момент.

Услуга ECT позволяет пользователю услуги перевести существующее соединение третьему пользователю.

1. Запустить Wireshark.
2. Осуществить вызов с терминала PM1 на терминал PM2.
3. Осуществить с терминала PM1 перевод вызова на терминал PM3.
4. Убедиться в наличии соединения между терминалами PM2 и PM3 и разрушении соединения между PM1 и PM2.
5. Анализ полученных трейсов (составление отчета):

- определить элементы сети IMS, участвующие в процессе реализации услуги;
- определить запрос, осуществляющий перевод вызова с терминала PM1;
- определить публичный идентификатор пользователя, на который необходимо осуществить перевод вызова;
- составить диаграмму обмена сообщениями SIP между всеми участниками соединения при реализации услуги.

3.5. Лабораторная работа 5. Неуспешные попытки установления мультимедийных сессий

Задание 5.1. Отбой вызывающего пользователя в предответном состоянии

1. Настроить терминалы (IMS Monster) на PM1 и PM2.
2. Запустить Wireshark.
3. Установить соединение от пользователя PM1 к пользователю PM2.
4. Отбой пользователя PM1 до ответа пользователя PM2.
5. Анализ участвовавших в соединении запросов и ответов SIP (составление отчета):

- определить запрос, который используется при отбое вызывающего пользователя в предответном состоянии и ответ на него;
- определить окончательный ответ на запрос INVITE.

Задание 5.2. Вызов пользователя отсутствующего в сети

1. Настроить терминал (IMS Monster) на PM1.
2. Запустить Wireshark.
3. Осуществить вызов от пользователя PM1 к пользователю, учетная запись которого прописана в базе данных пользователей HSS, но не активирована ни на одном из терминалов.
4. По трейсам с помощью программы Wireshark:

- определить элементы сети IMS, участвующие в процессе установления мультимедийной сессии;
- определить сообщения SIP (запросы и ответы) и сообщения DIAMETER, отправленные для установления сессии, по трейсам с помощью программы Wireshark;
- определить в каких сообщениях SIP и Diameter передается информация о невозможности установить сессию.

5. составить диаграмму обмена сообщениями между всеми участниками сессии.

Задание 5.3. Вызов несуществующего пользователя

1. Настроить терминал (IMS Monster) на PM1.
2. Запустить Wireshark.
3. Осуществить вызов от пользователя PM1 к пользователю, учетная запись которого не прописана в базе данных пользователей HSS.
4. По трейсам с помощью программы Wireshark:

- определить элементы сети IMS, участвующие в процессе установления мультимедийной сессии;
- определить сообщения SIP (запросы и ответы) и сообщения DIAMETER, отправленные для установления сессии, по трейсам с помощью программы Wireshark;
- определить, в каких сообщениях SIP и Diameter передается информация о невозможности установить сессию.

5. Составить диаграмму обмена сообщениями между всеми участниками соединения.

Задание 5.4. Аудиосессия с SIP-терминала

1. Запустить Wireshark.
2. Настроить терминал (IMS Monster) на PM1.
4. Запустить Wireshark.
5. Настроить SIP-терминалы (SJPhone и Twinkle) согласно заданию 1.5, и осуществить вызов на PM1.
6. Проанализировать трейсы, полученные с помощью программы Wireshark (составление отчета):

- определить элементы сети IMS, участвующие в процессе установления сессии;
- сравнить сценарий обмена сообщениями при организации аудиосессии с SIP-терминала со сценарием обмена сообщениями при организации аудиосессии с IMS-терминала (см. задание 2.1), объяснить причины отличия.

ЛИТЕРАТУРА

Основная

1. *Гольдштейн, А.Б.* Softswitch / А. Б. Гольдштейн, Б. С. Гольдштейн – СПб. : БХВ-Санкт-Петербург, 2006.

2. *Гольдштейн, Б.С.* Сети связи/ Б. С. Гольдштейн, Н . А. Соколов, Г .Г . Яновский - СПб. : БХВ-Санкт-Петербург, 2010.

Дополнительная

2. *Гольдштейн, Б.С.* Справочник по телекоммуникационным протоколам. Протокол SIP / Б. С. Гольдштейн, А. А. Зарубин, В. В. Саморезов. – СПб. : БХВ-Санкт-Петербург, 2005.

3. *Атцик, А.А.* Протокол MEGACO/H.248: справочник по телекоммуникационным протоколам / А. А. Атцик, А. Б. Гольдштейн, Б. С. Гольдштейн. – СПб. : БХВ-Санкт-Петербург, 2009.

4. *Гольдштейн, Б.С.* Справочник по телекоммуникационным протоколам. Протоколы AAA: RADIUS и Diameter / Б. С. Гольдштейн,
В. С. Елагин, Ю. Л. Сенченко. – СПб. : БХВ-Санкт-Петербург, 2011.

Сайты

5. http://www.skri.sut.ru
6. http://www.niits.ru
7. http://www.sotsbi.spb.ru

Гольдштейн Борис Соломонович
Гойхман Вадим Юрьевич
Сибирякова Нина Геннадьевна
Столповская Юлия Владимировна

СЕТИ NGN. ОБОРУДОВАНИЕ IMS

УЧЕБНОЕ ПОСОБИЕ

*Редактор **Л. А. Медведева***

План 2010 г., п. 5

***

Подписано к печати 15.12. 2010
Объем 3,75 усл.-печ. л. Тираж 200 экз. Зак. 121

****

Издательство «ТЕЛЕДОМ» ГОУВПО СПбГУТ
191186 СПб., наб. р. Мойки, 61
Отпечатано в СПбГУТ

Б.С. Гольдштейн, В.Ю. Гойхман
Н.Г. Сибирякова, Ю.В. Столповская

СЕТИ NGN. ОБОРУДОВАНИЕ IMS

УЧЕБНОЕ ПОСОБИЕ

САНКТ-ПЕТЕРБУРГ
2010