РЕФЕРАТ

Тема данной дипломной работы – «Разработка алгоритма инфокоммуникационной услуги в концепции IMS». Дипломная работа содержит 88 страниц, из них 20 рисунков. В работе использовано 18 источников.

Ключевые слова: сеть мобильной связи, IP Multimedia Subsystem, услуга, функциональный элемент сети, Session Initiation Protocol (SIP), присутствие, сервер приложений, агент, наблюдатель, пользователь.

В данной дипломной работе проведен анализ текущего этапа развития сетей подвижной связи, обоснована необходимость перехода к архитектуре сети на основе IP Multimedia Subsystem (IMS). Выполнен обзор IMS и приведено описание ее основных функциональных элементов. Разработан алгоритм работы инфокоммуникационной услуги – услуги контроля присутствия, построенной в концепции IMS, намечен подход к расчету вероятностно-временных характеристик услуги.

Результаты дипломной работы имеют шанс лечь в основу разработки приложения услуги контроля присутствия, актуальность внедрения которой в современной сети мобильной связи подтверждается многими специалистами, а также успешным опытом введения в коммерческую эксплуатацию подобного типа услуг на сетях мобильной связи в России и в мире.

СОДЕРЖАНИЕ

РЕФЕРАТ 5
ВВЕДЕНИЕ 7
ГЛАВА 1. Эволюция телекоммуникационных услуг: на пути к IMS 10
1.1 Специфика предоставления мультимедийных услуг в сетях мобильной связи 10
1.2 Эволюция сети доступа 11
1.3 Переход к пакетной коммутации 12
1.4 Стандарты 3GPP 14
1.5 Причины перехода к архитектуре IMS 15
ГЛАВА 2. Обзор архитектуры IMS. 19
2.1 Функции управления сессиями вызовов (CSCF) 21
2.1.1 Прокси функция управления сессиями вызовов (P-CSCF) 21
2.1.2 Опрашивающая функция управления сессиями вызовов (I-CSCF) 23
2.1.3 Обслуживающая функция управления сессиями вызовов (S-CSCF) 23
2.2 Базы данных. 25
2.3 Функции предоставления сервисов 27
2.4 Функции взаимодействия 29
2.5 Функции поддержки. 30
2.6 Функции учета стоимости. 32
ГЛАВА 3. Услуга контроля присутствия. 35
3.1 Преимущества внедрения услуги 35
3.2 Принцип работы услуги 36
3.3 Жизненный цикл услуги контроля присутствия. 39
ГЛАВА 4. Формат информации присутствия 43
4.1 Понятие PIDF 43
4.2 Содержимое PIDF. 44
4.3 Информационная модель SIP 48
4.4 Расширенный формат информации присутствия (RPID). 50
4.5 Возможности. 54
ГЛАВА 5. Информация присутствия. 61
5.1 Публикация информации присутствия. 61
5.2 Подписка и уведомления. 62
5.3 Информация о наблюдателях. 64
ГЛАВА 6. Оптимизация услуги контроля присутствия 66
6.1 Списки ресурсов. 66
6.2 XML Configuration Access Protocol 68
6.3 Механизм частичного уведомления. 70
6.4 Фильтрация уведомлений. 72
ГЛАВА 7. Интеграция услуги контроля присутствия в сеть IMS 73
ГЛАВА 8. Подходы к расчету вероятностно-временных характеристик услуги 81
ЗАКЛЮЧЕНИЕ 83
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 84
СПИСОК СОКРАЩЕНИЙ 86

ВВЕДЕНИЕ

В настоящее время операторы сетей мобильной связи поколения 2.5G сталкиваются с тенденцией снижения темпов роста доходов, получаемых в результате предоставления услуг мобильной телефонии и простых услуг обмена сообщениями. Данная тенденция развивается под воздействием нескольких факторов. Снижение темпов роста доходов связано со снижением темпов роста абонентской базы операторов, так как рынок услуг мобильной связи постепенно переходит в состояние насыщения, то есть дальнейшее привлечение абонентов возможно только за счет перехода абонентов от одного оператора к другому, но не за счет подключения новых абонентов. На протяжении последних лет основным средством «переманивания» абонентов от оператора к оператору служила политика демпинга цен на услуги, которая напрямую снижает показатель ARPU (average revenue per user) – средней выручки на одного пользователя мобильной связи.

Помимо традиционных услуг мобильной телефонии (голос, обмен короткими сообщениями), портфели операторов, как правило, включают в себя дополнительные услуги добавочной стоимости (VAS – Value Added Services), с предоставлением которых операторы связывают дальнейшее успешное ведение бизнеса. Однако спрос на такие услуги на сегодняшний день является незначительным и не может сыграть решающей роли в сложившейся ситуации, так как предоставляемые услуги являются достаточно сложными как с точки зрения их подключения, так и с точки зрения использования. Кроме того, информационное наполнение данных услуг (контент) в большинстве случаев является однообразным и не привлекает достаточного числа потребителей.

Попытки внедрения высокотехнологичных персонифицированных услуг с интересным наполнением, которые могли бы исправить положение, в

существующих 2.5G сетях сталкиваются с архитектурными ограничениями этих сетей. В первую очередь, это неприспособленность таких сетей к предоставлению «тяжелых» услуг, которые требуют передачи большого объема информации через сеть доступа. Во-вторых, это сложность внедрения большого количества услуг, так как существующая архитектура 2.5G сетей допускает построение услуг только по вертикальному принципу, что приводит к сложности их интеграции между собой и усложнению сети оператора в целом.

Выходом из сложившейся ситуации многие специалисты считают переход к сетям третьего поколения 3G на основе IP Multimedia Subsystem, основным отличием которых от сетей 2.5G являются усовершенствованная технология доступа и новая среда предоставления услуг. Новая технология доступа 3G сети заранее спроектирована для предоставления услуг, связанных с передачей больших объемов информации. Среда предоставления услуг 3G сети позволяет уйти от вертикальной архитектуры, выполняя внедрение услуг в горизонтальной архитектуре с использованием стандартных интерфейсов, что облегчает их интеграцию. Горизонтальная архитектура подразумевает использование общих элементов для предоставления услуг, что не ведет к заметному усложнению сети оператора, как это происходит в случае использования вертикальной архитектуры. Кроме того, IMS архитектура проектировалась как независимая от технологии сети доступа, что позволяет получать доступ к IMS услугам с любого терминала по любой подходящей технологии доступа (W-CDMA, WiMax, GSM).

Все вышеперечисленные особенности сетей третьего поколения способствуют созданию новых высокотехнологичных персонифицированных услуг, позволяющих сохранить и приумножить доходы операторов, а также удовлетворить спрос пользователей на новые качественные сервисы.

Одной из новых услуг, создание которой становится возможным благодаря переходу к архитектуре IMS, является услуга контроля присутствия. Влияние появления данной услуги на бизнес внедрившего ее оператора связи трудно переоценить. Являясь услугой дополнительной стоимости сама по себе, услуга контроля присутствия непосредственным образом влияет на возможность внедрения новых услуг, связанных с предоставлением информации о статусе пользователей. Например, услуга обмена мгновенными сообщениями полностью меняет свой облик после интеграции с услугой контроля присутствия, когда пользователю достаточно взгляда на список пользователей для определения возможности информационного обмена и получения большого количества другой полезной информации. Внедрение услуги снижает количество неуспешных вызовов по причине недоступности или занятости абонентов, увеличивается трафик обмена данными в целом, обеспечивая преимущество внедрившему ее оператору в условиях конкуренции на рынке.

Данная дипломная работа посвящается разработке алгоритма работы услуги контроля присутствия, а также аспектам ее внедрения в сеть IMS. В работе рассматриваются вопросы перехода к IMS сети, содержится обзор архитектуры IMS сети, описываются ее основные функциональные элементы и их назначение. Рассматривается услуга контроля присутствия в целом, определяются ее участники и обмен информацией между ними. Описывается обмен сигнальной информацией по протоколу SIP, а также расширения данного протокола, используемые в работе услуги. Последняя глава обозначает подход к расчету вероятностно-временных характеристик, получение которых необходимо для внедрения услуги контроля присутствия на реальной сети.

ГЛАВА 1. Эволюция телекоммуникационных услуг: на пути к IMS.

1.1 Специфика предоставления мультимедийных услуг в сетях мобильной связи

На протяжении двух последних десятилетий сети мобильной связи эволюционировали в целях удовлетворения и создания рыночного спроса на телекоммуникационные услуги. На заре эры мобильной связи этот спрос ограничивался простыми голосовыми сервисами, предоставляемыми, как правило, бизнес сегменту рынка. Затем произошел ощутимый скачок в распространении мобильной связи, так как ограниченное использование услуг мобильной телефонии бизнес сегментом переросло во всемирный рынок, породивший спрос на голосовые сервисы и простые текстовые сервисы передачи данных.

Сегодня, после первых пробных шагов в направлении мультимедийных мобильных услуг, появился спрос на услуги, аналогичные предоставляемым в сети Интернет пользователям с фиксированным доступом. Однако в мобильных сетях предоставление данных услуг должно удовлетворять определенному количеству условий. Спрос на новые услуги будет существовать только в том случае, если они будут цельными и персонализированными. Они должны быть интуитивны в вопросах доступа и использования. То есть, в настоящее время потребители желают получить сложные персонифицированные сервисы, предоставляемые в любое время любым способом через любое устройство.

IMS предоставляет возможность удовлетворить данный спрос простым способом, обеспечивающим быстрое и гибкое создание услуг, снижение стоимости их разработки и использования.

Несмотря на то, что IMS оказывает радикальное воздействие на наборы предоставляемых сервисов и бизнес модели операторов мобильной связи, как этап развития сетей она должна рассматриваться в качестве эволюционного, а не революционного шага.

Для того чтобы понять, какое место занимает IMS в терминах развития сервисов и технологий, полезно вспомнить процесс эволюции мобильных сетей в целях удовлетворения потребительского спроса.

1.2 Эволюция сети доступа

Эффективное использование полосы пропускания является одним из главных принципов операторов беспроводной связи и инженеров, разрабатывающих сети. Неэффективное использование полосы пропускания ведет к уменьшению трафика, переносимого сетью, уменьшение трафика ведет к уменьшению пользователей и уменьшению отдачи от использования инвестируемых средств.

На протяжении последних лет GSM операторы прикладывали все усилия на увеличение эффективности своих сетей, для того чтобы справиться с растущим числом абонентов, одновременно пытаясь найти способ предоставления требовательных к полосе пропускания Интернет-подобных услуг, от которых зависит их будущее.

Одним из способов усовершенствования работы мобильной сети является улучшение технологии сети доступа. Эта часть архитектуры беспроводной сети, предоставляющая связь между устройством пользователя и ядром сети.

Технология доступа UMTS W-CDMA передает цифровую информацию через широкополосный CDMA радиоканал. При данной технологии большое число пользователей могут одновременно использовать ресурсы одного широкополосного канала. Кроме того, использование более широкой полосы пропускания предоставляет более широкий канал переноса информации, который недостижим в распространенной сейчас технологии GSM. W-CDMA технология доступа обеспечивает операторам более широкую полосу пропускания, требуемую для предоставления насыщенных контентом приложений.

1.3 Переход к пакетной коммутации

Не менее важным шагом в эволюции сетей к сетям третьего поколения был переход от коммутации каналов к коммутации пакетов в ядре сети. Это технология, отвечающая за доставку и направление трафика в другие части сети. До появления технологи GPRS GSM сети были построены исключительно с использованием технологии коммутации каналов. Технология коммутации каналов подразумевает, что при установлении соединения между вызывающим и вызываемым абонентами устанавливается выделенный канал связи. Основной недостаток данной технологии состоит в том, что данный канал становится недоступным для использования кем-либо еще на протяжении всего времени разговора.

Технология пакетной коммутации, напротив, работает по принципу расщепления трафика (голоса или данных) в набор контейнеров, называемых пакетами. Впоследствии эти пакеты передаются вместе с пакетами других пользователей через один канал связи, затем они перераспределяются и собираются воедино уже в устройстве пользователя, которому они предназначены.

Такое совместное использование ресурсов вместе с возможностью использования обычных сетевых протоколов и инфраструктуры ведет к более эффективной системе передачи информации и повышению удобства пользователя.

Для GSM операторов появление технологии GPRS также означало, что их сети поддерживали индустриальный стандартный транспорт, такой как IP. Пакетная коммутация более удобна для пользователя, так как она обеспечивает возможность предоставления так называемых «всегда – на - связи» услуг, используемых на обычных персональных компьютерах, подключенных к Интернет.

После того, как соединение установлено, пользователи получают постоянное виртуальное соединение с сетью, которое позволяет быстро принять или передать информацию, если таковая имеется.

Поскольку технология коммутации пакетов использует более эффективные технологии маршрутизации, сети с коммутацией пакетов предоставляют большие скорости передачи данных по сравнению с сетями коммутации каналов. Кроме того, домен с коммутацией пакетов обеспечивает возможность использования более одной услуги в рамках одной сессии. Например, в процессе голосового вызова через сеть пакетной коммутации возможно передать картинку или видеоклип от абонента к абоненту.

1.4 Стандарты 3GPP

Стандарты IMS определяют сетевой домен, предназначенный для управления мультимедийными сервисами и их интеграции. Данный домен является частью архитектуры сети третьего поколения, описанной в пятом выпуске стандартов 3GPP.

Первая волна стандартов 3GPP, определяющих большинство существующих на данный момент сетей третьего поколения была завершена в 1999 году и известна под названием «выпуск 99».

Эти стандарты представляли новый 3G интерфейс (W-CDMA) для ядра 2G сетей. Два года спустя 3GPP выпустила серию стандартов улучшения радио доступа под названием «выпуск 4»

В марте 2002 года 3GPP выпускает пятую серию стандартов, которые описывали технологию HSPDA, улучшающую характеристики нисходящего потока и главное усовершенствование окружения сервисов – стандарты IMS.

Хотя 3GPP был ответственным за написание большинства стандартов IMS, IMS является системой, построенной на основе протоколов, разработанных IETF. С того момента, как 3GPP определила понятие IMS, другие участники индустрии, такие как 3GPP2 и ETSI внесли большой вклад в ее развитие.

Несмотря на то, что IMS была разработана для изменения и эволюции UMTS сети, спецификации были детально разработаны как не зависимые от технологии доступа. Другими словами, IMS поддерживает множество способов доступа – GSM, W-CDMA, CDMA2000, wireline broadband access,

WiMAX, WLAN. Одной из целей создателей IMS было создание архитектуры гибкого сервисного домена, независимого от уровня доступа.

1.5 Причины перехода к архитектуре IMS

Если попытаться ответить на вопрос, почему же именно IMS необходима сейчас операторам, то можно подобрать следующие аргументы.

Без IMS попытки разработать и внедрить комплекс услуг, который удовлетворял бы различным запросам пользователей, представляется очень сложной, беспорядочной и дорогостоящей задачей.

В самом начале появления информационных сервисов для мобильных сетей операторы создавали «вертикальные» сервисные платформы, которые управляли предоставлением нескольких ключевых услуг (рис. 1.1).

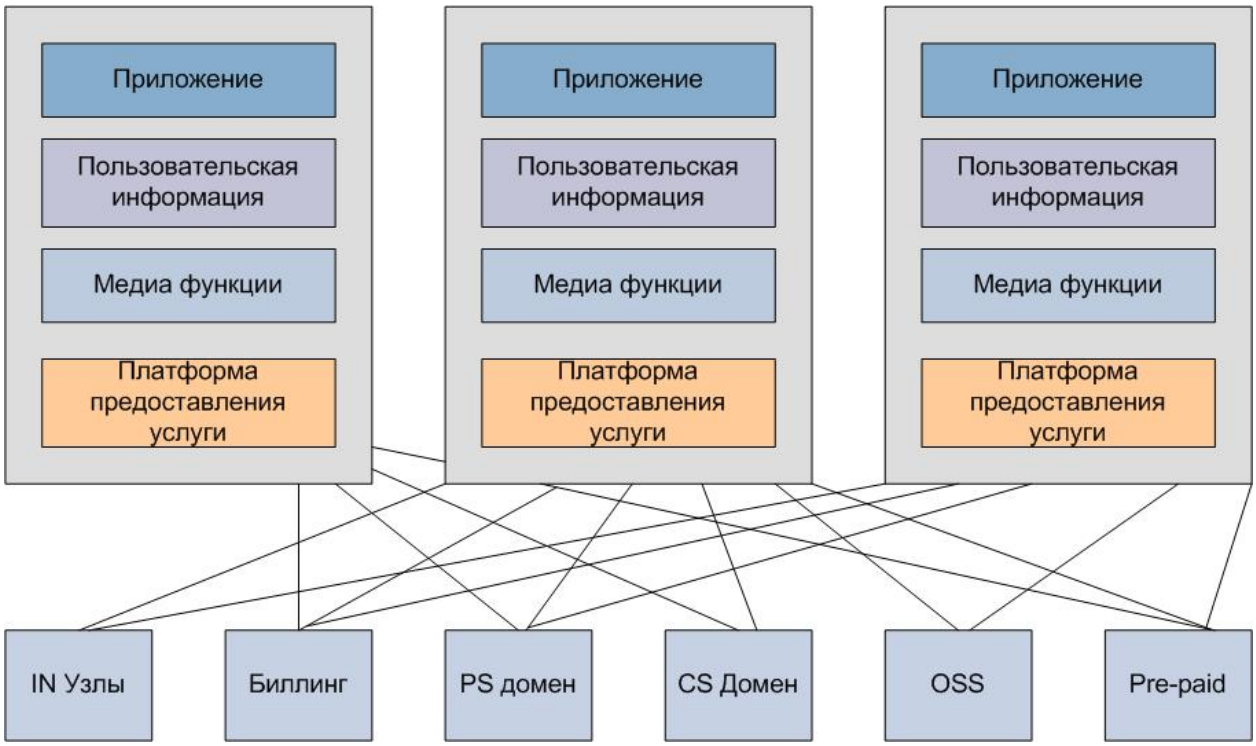

Рис. 1.1

Такие решения приводили к тому, что каждый сервис требовал размещения выделенных компонентов, что является допустимым при небольшом количестве сервисов, но становится громоздким, когда операторы пытаются предоставлять гибкость, персонализацию и быстрое увеличение количества сервисов, аналогичных предоставляемым пользователям сети Интернет с фиксированным доступом.

IMS предназначена для уменьшения стоимости создания сервисов за счет ухода от модели вертикальных сервисных платформ. Это осуществляется путем разработки конвергентной IP инфраструктуры, в которой транспортные ресурсы и ресурсы приложений являются разделяемыми между многими сервисами и многими способами доступа (рис 1.2).

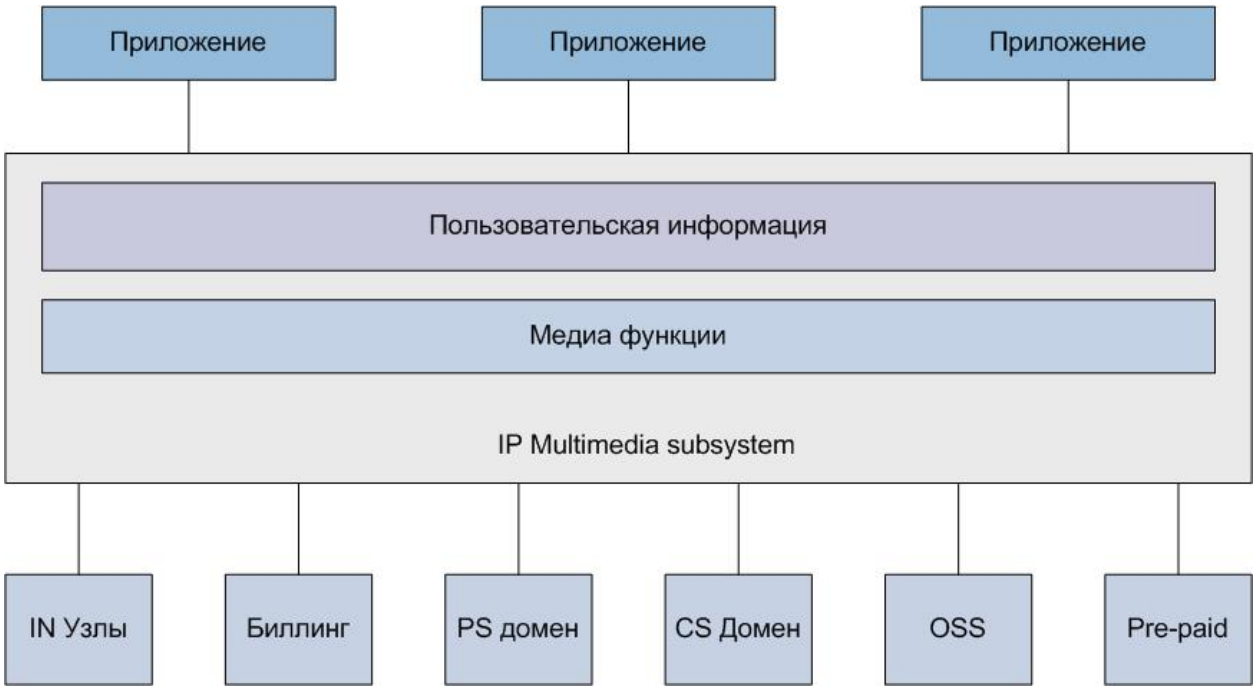

Рис. 1.2

IMS рационализирует способ внедрения сервисов в сети. Она создает логическую архитектуру, которая делает более простой и более эффективной разработку и внедрение новых персонализированных сервисов. Кроме того,

она позволяет пользователям получить доступ сразу к нескольким сервисам в рамках одной сессии.

Как правило, операторы желают использовать сервисы, разработанные сторонними производителями, комбинировать их и интегрировать с существующими сервисами. IMS определяет стандартные интерфейсы, которые должны использоваться разработчиками сервисов. Операторы имеют возможность создать мощный сервис, изготовленный несколькими производителями, они получают возможность избежать жесткого закрепления за определенным вендором для создания новых услуг.

Еще один аргумент, подтверждающий целесообразность использования архитектуры IMS – это то, что мультимедийные сервисы реального времени предоставляются по принципу best effort, без определенного качества обслуживания. То есть сеть не предоставляет каких-либо гарантий полосы пропускания, величины задержки пакетов и пр. Следовательно, качество предоставляемой услуги может варьироваться от хорошего до неприемлемого. Архитектура IMS подразумевает согласование уровня качества обслуживания до установления сессии, то есть пользователь заранее знает, на какое качество предоставления услуги он может рассчитывать.

И, наконец, IMS позволяет осуществлять тарификацию оказываемых услуг в соответствии с типом оказываемой услуги. Например, пользователь, участвующий в видеоконференции через домен коммутации пакетов, передает и принимает большое количество информации (закодированное аудио и видео). Как правило, в сетях 3G тарификация осуществляется на основе количества передаваемой и получаемой информации, что в рассматриваемом примере может обречь данного пользователя на большие затраты. Оператор не может следовать определенной бизнес модели и

тарифицировать пользователя в зависимости от используемого сервиса, так как не знает, каким сервисом пользуется абонент.

В другом случае, если оператор точно знает, каким сервисом пользуется абонент, он может предоставить альтернативную схему тарификации, более выгодную для пользователя. Например, в случае обмена сообщениями, оператор может осуществлять тарификацию из расчета каждого переданного сообщения, а мультимедийную сессию тарифицировать на основе ее длительности.

Благодаря этим преимуществам IMS позволяет создавать такие типы услуг как

- Услуга контроля присутствия – сервис, позволяющий пользователю показывать информацию о себе и своем устройстве другим пользователям. Например, он может публиковать информацию о своем местонахождении, готовности к определенному виду связи, настроении, типе устройства и его телекоммуникационных возможностях и др.
- Групповое общение – текстовые чаты, видео и аудио конференции.
- Push-to-talk – услуга обмена голосовой информацией по принципам, схожим с использованием рации но без ограничения на расстояние.
- Доска для записей – услуга, позволяющая нескольким абонентам совместно редактировать документы в режиме реального времени.
- Многопользовательские игры в реальном времени и многое другое.

ГЛАВА 2. Обзор архитектуры IMS.

Упрощенная архитектура сети IMS изображена на рис. 2.1

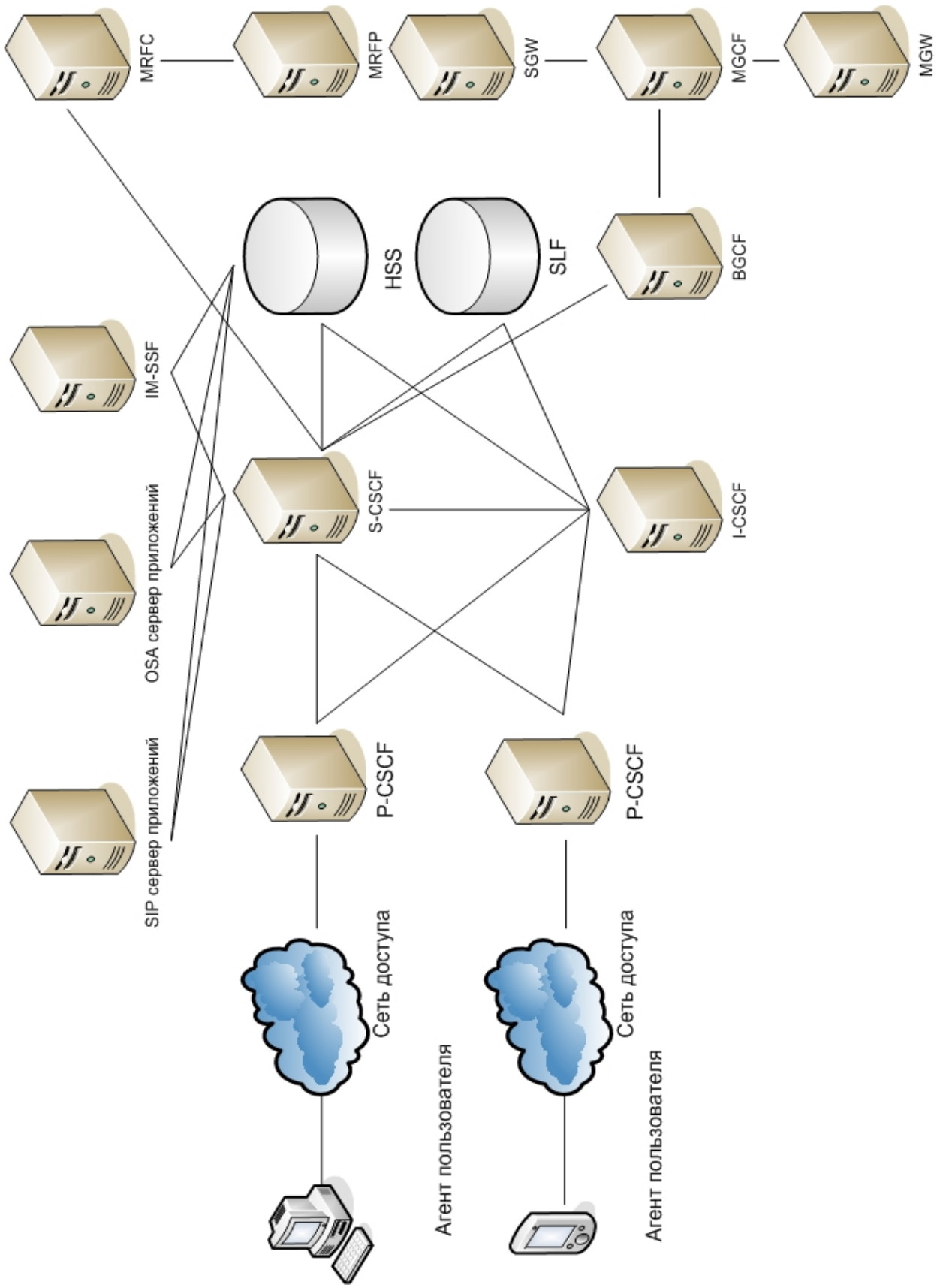
MRFC
MRFP
SGW
MGCF
MGW
HSS
SLF
BGCF
IM-SSF
S-CSCF
I-CSCF
OSA сервер приложений
SIP сервер приложений
P-CSCF
P-CSCF
Сеть доступа
Сеть доступа
Агент пользователя
Агент пользователя

Рис. 2.1

Элементы сети IMS [1] можно разделить на шесть групп:

1) элементы управления сессиями и маршрутизацией (CSCF)
2) базы данных
3) сервисные функции (Серверы приложений, MRFC, MRFP)
4) элементы взаимодействия (BGCF, MGCF, IMS-MGW, SGW)
5) элементы поддержки (PDF, SEG, THIG)
6) элементы учета стоимости услуг

2.1 Функции управления сессиями вызовов (CSCF)

Существует три вида функций управления сессиями вызовов:

- прокси функция управления сессиями вызовов
- обслуживающая функция управления сессиями вызовов
- опрашивающая функция управления сессиями вызовов.

Их общей чертой является то, что все они задействованы в процессе регистрации и установления соединения и формируют механизм маршрутизации SIP.

2.1.1 Прокси функция управления сессиями вызовов (P-CSCF)

Прокси функция управления сессиями вызовов – это первая точка взаимодействия сети IMS с пользователем. Весь сигнальный трафик SIP, поступающий от устройства пользователя, передается на P-CSCF. Аналогично, весь терминируемый трафик передается от P-CSCF к устройству пользователя. Всего P-CSCF выполняет четыре задачи:

- сжатие SIP

- работа по протоколу IPSec
- взаимодействие с функцией выполнения политик (PDF)
- распознавание экстренных вызовов.

Являясь текстовым протоколом, SIP содержит большое количество заголовков и параметров заголовков, а также расширения и информацию, касающуюся безопасности сессий, что приводит к тому, что размер сообщений превосходит размер сообщений в двоичных протоколах. Для увеличения скорости установления соединений 3GPP разработал процедуры сжатия SIP на участке между P-CSCF и устройством пользователя. P-CSCF должен выполнять сжатие сообщений SIP в случае, если устройство пользователя запрашивает его об этом.

P-CSCF отвечает за выполнение процедур проверки безопасности (SAs), целостности и конфиденциальности соединений. Для этого в процессе регистрации устройство пользователя и P-CSCF устанавливают IPSec SAs. После процедуры начальной регистрации P-CSCF может выполнять процедуры проверки целостности и конфиденциальности обмена сообщениями по SIP.

P-CSCF передает информацию об обмене сигнальными сообщениями и потоками данных в PDF в случае, если оператор желает использовать локальную сервисно ориентированную политику (SBLP). На основе получаемой информации PDF может определить авторизованную информацию о качестве обслуживания IP и передать ее в GGSN. Более того, на основе PDF возможен обмен информацией о стоимости услуг между GPRS и IMS, что позволяет объединять в биллинговой системе записи о стоимости услуг, поступающие из IMS и GPRS.

Аспекты, касающиеся распознавания экстренных вызовов в настоящее время не до конца специфицированы (работа над ними ведется в рамках Release 7). Планируется, что P-CSCF должен будет уметь выбирать CSCF для экстренных вызовов, так как это необходимо в случае роуминга, когда назначаемый S-CSCF не сможет маршрутизировать запрос в нужный центр обслуживания экстренных вызовов.

2.1.2 Опрашивающая функция управления сессиями вызовов (I-CSCF)

I-CSCF это точка взаимодействия в сети оператора, через которую проходят все соединения, устанавливаемые с абонентами данной сети. I-CSCF выполняет четыре задачи:

- получение из HSS имени следующего перехода (S-CSCF либо сервера приложений)
- назначение S-CSCF на основе информации о возможностях, получаемой из HSS. Назначение происходит в момент регистрации абонента в сети, либо в случае, если пользователь не зарегистрирован в сети, но подписан на услуги, работающие в то время, пока абонент не зарегистрирован в сети (голосовая почта).
- дальнейшая маршрутизация входящих вызовов к S-CSCF или серверу приложений
-выполнение функций шлюза, скрывающего топологию сети (THIG)

2.1.3 Обслуживающая функция управления сессиями вызовов (S-CSCF)

S-CSCF это центральная точка в IMS так как она отвечает за выполнение регистрационных процедур, принятие решений о маршрутизации и отслеживание состояния сессии, а также сохранение профилей сервисов.

Запрос на регистрацию, посылаемый пользователем, маршрутизируется на S-CSCF, которая получает информацию аутентификации из HSS. На основе этой информации S-CSCF генерирует ответ устройству пользователя. После получения ответа и определения его корректности S-CSCF принимает регистрацию и начинает контролировать статус этой регистрации. После данной процедуры пользователь может инициировать и принимать сервисы IMS. S-CSCF получает профиль сервисов из HSS как часть регистрационной информации.

Профиль сервисов является набором данных, определенных для каждого пользователя, который постоянно хранятся в HSS. S-CSCF получает определенный профиль, связанный с идентификатором пользователя, когда этот идентификатор регистрируется в сети. S-CSCF на основе данной информации принимает решение о том, когда и какой сервер приложений должен быть задействован, когда пользователь отправляет SIP запрос либо получает его от кого-либо. Кроме того, профиль сервиса может содержать инструкции о типе политики, которую S-CSCF должен применить. Например, в профиле может содержаться информация о том, что пользователь может обмениваться только аудио потоками и данными приложений, но не видео потоками.

S-CSCF отвечает за маршрутизацию, так как через нее проходят все инициируемые и терминируемые пользователем сессии и транзакции. Когда S-CSCF получает инициируемый устройством пользователя запрос через P-CSCF, она должна принять решение, необходимо ли взаимодействие с серверами приложений перед дальнейшей обработкой. После возможного взаимодействия с серверами приложений S-CSCF либо продолжает сессию в IMS, либо передает ее в домены коммутации каналов либо в другие домены пакетной коммутации. Кроме того, если устройство пользователя использует MSISDN в качестве адреса вызываемой стороны, то S-CSCF преобразует

такой номер в SIP URI для дальнейшей обработки запроса, так как IMS не может маршрутизировать запросы на основе MSISDN. Аналогично, S-CSCF получает все запросы, терминируемые устройством пользователя. Несмотря на то что S-CSCF известен IP адрес устройства пользователя из процедуры регистрации, все запросы маршрутизируются на P-CSCF, так как P-CSCF реализует функции сжатия SIP и обеспечения безопасности. До маршрутизации на P-CSCF S-CSCF может направить запрос на серверы приложений, к примеру, для проверки правил переадресации.
Помимо этого, S-CSCF способен отправлять информацию о счетах пользователей в систему тарификации реального времени.

2.2 Базы данных.

Архитектура IMS включает в себя две главные базы данных: сервер домашних абонентов (HSS) и функцию локации подписки (SLF).

HSS является главным хранилищем всей информации абонентов, а так же информации о сервисах IMS. Главное хранилище информации в HSS включает в себя идентификаторы пользователей, регистрационную информацию, параметры доступа и информацию активации сервисов. Идентификаторы пользователей состоят из двух частей: частные идентификаторы пользователей (Private user identities) и публичные идентификаторы пользователей (Public user identities). Частный идентификатор пользователя это идентификатор, назначаемый оператором домашней сети. Он используется в процедурах регистрации и авторизации. Публичный идентификатор пользователя используется для того, чтобы

другие пользователи могли запросить по нему обмен информацией с данным пользователем.

Параметры доступа IMS используются для установки сессии и включают в себя такие параметры как аутентификация пользователя, роуминговая авторизация, имена назначенных S-CSCF.

Информация активации сервисов используется для выполнения сервисов SIP. HSS так же предоставляет специфичные для каждого пользователя требования к возможностям S-CSCF. Эта информация используется I-CSCF для выбора наиболее подходящего S-CSCF для определенного абонента. В дополнение к функциям, относящимся к функциональности IMS HSS содержит поднабор функций Home Location Register (HLR) и Authentication Center (AUC), необходимые для доменов коммутации каналов и пакетов.

Функциональность HLR необходима для работы таких элементов домена коммутации пакетов как SGSN и GGSN. Это дает возможность абонентам пользоваться услугами домена коммутации пакетов. Аналогично, HLR поддерживает работу таких элементов домена коммутации каналов как MSC/GMSC, что позволяет абонентам использовать услуги домена коммутации каналов, а так же поддерживает роуминг в доменах коммутации каналов сетей GSM.

AUC хранит секретный ключ каждого мобильного абонента, который используется для генерации динамической информации для выполнения функций обеспечения безопасности. Эта информация используется для аутентификации IMSI и сети. Кроме того данная информация используется для выполнения процедур обеспечения целостности и шифрования обмена информацией на радио участке между устройством пользователя и сетью.

В зависимости от числа абонентов, емкости оборудования и организации сети в сети может присутствовать более одного HSS. SLF используется для того, чтобы I-CSCF, S-CSCF и серверы приложений могли определить адрес HSS, который содержит информацию определенного пользователя в случае наличия более чем одного HSS в сети.

2.3 Функции предоставления сервисов

Сервисные функции сети IMS включают в себя контроллер функции мультимедийных ресурсов (MRFC), процессор функции мультимедийных ресурсов (MRFP) и сервер приложений (AS).

Серверы приложений не являются элементами сети IMS в чистом виде, они, скорее, являются функциями поверх IMS. С другой стороны, серверы приложений предоставляют такие сервисы добавочной стоимости сети IMS как сервис присутствия и PoC. Сервер приложений может находиться как в домашней сети, так и в другой сети, либо это может быть отдельный сервер приложений. Главными функциями серверов приложений являются:

- возможность обрабатывать входящую из сети IMS сессию SIP
- возможность инициировать SIP запросы
- возможность отправлять информацию о стоимости услуги в функции учета стоимости

Сервер приложений SIP это SIP сервер, включающий в себя определенное количество мультимедийных услуг добавочной стоимости. Сервер приложений SIP может быть использован для предоставления сервиса присутствия, обмена сообщениями, PoC, сервиса конференции и др.

Сервер приложений может быть создан для одной услуги, пользователь же может иметь больше чем один сервис, таким образом на одного пользователя может быть один или более серверов приложений. Кроме того, в одной сессии может быть задействован один или более серверов приложений. Например, оператор может иметь один сервер приложений для контроля терминируемого в сторону абонента трафика на основе настроек пользователя (например, переадресовывать все входящие мультимедийные сессии на автоответчик между 23 и 8 часами) и другой сервер для адаптации контента обмена мгновенными сообщениями в соответствии с возможностями устройства пользователя (размер экрана, количество цветов и пр.).

MRFC и MRFP предоставляют механизмы для работы таких сервисов как конференция, проигрывание подсказки пользователю, или перекодирование носителя в архитектуре IMS. MRFC предназначен для поддержки обмена сообщениями по SIP от и к S-CSCF и для контроля MRFP. MRFP в свою очередь предоставляет ресурсы, запрашиваемые MRFC. MRFP выполняет следующие функции:

- - смешивание входящих медиа потоков,
- - источник медиа потока (для проигрывания мультимедийных сообщений)
- - обработка медиа потока (например, аудио перекодирование, медиа анализ)

2.4 Функции взаимодействия

В процессе маршрутизации S-CSCF принимает решение о том, необходим ли переход в домен коммутации каналов. Для осуществления перехода S-CSCF отправляет SIP запрос на функцию контроля шлюза перехода (BGCF), выбирая, где будет выполняться данный переход. Переход может выполняться либо в той же сети, в которой расположен BGCF, либо в другой сети. Если переход происходит в той же сети, то BGCF выбирает функцию контроля медиа шлюза (MGCF) для дальнейшего управления сессией. Если переход выполняется в другой сети, то BGCF перенаправляет сессию к другой BGCF в выбранной сети. Последний случай позволяет маршрутизировать сигнальные сообщения и медиа потоки через IP ближе к вызываемому абоненту.

Когда SIP запрос достигает MGCF, она выполняет преобразование протоколов SIP в ISUP и посылает преобразованный запрос через сигнальный шлюз (SGW) в сеть с коммутацией каналов. SGW выполняет преобразование сигнализации в обе стороны на транспортном уровне между основанной на IP передаче сигнализации и (то есть между Sigtran SCTP/IP и SS7 MTP) и основанной на SS7 передаче сигнальной информации. SGW не распознает сообщения уровня приложений (например, ISUP). MGCF также управляет IMS медиа шлюзом (IMS MGW). IMS MGW предоставляет связь в плоскости пользователя между сетью коммутации каналов и IMS. Он терминирует несущие каналы со стороны домена коммутации каналов и медиа потоки из основной сети (например, RTP потоки в IP сети или AAL2/ATM соединения в ATM сети), выполняет преобразования между этими двумя потоками и выполняет перекодирование и обработку сигналов для плоскости пользователя, когда это необходимо. Кроме того, IMS-MGW

может проигрывать тональные сигналы и подсказки пользователям домена коммутации каналов.

Аналогично, вся входящая сигнализация управления вызовом от пользователя CS к пользователю IMS направляется на MGCF, который выполняет необходимое преобразование протоколов и отправляет SIP запрос к I-CSCF для терминирования сессии. В то же время, MGCF взаимодействует с IMS-MGW и резервирует необходимые IMS-MGW ресурсы в плоскости пользователя.

2.5 Функции поддержки.

Функция применения политики (PDF) предназначается для принятия решения по политике обслуживания на основе информации о сессии и медиа потоках, получаемой от P-CSCF. Она функционирует как точка принятия решений для управления сервисно-ориентированной локальной политикой (SBLP).

Шлюз безопасности (SEG) несет в себе функцию защиты трафика плоскости управления между доменами безопасности. Домен безопасности обозначает сеть, которая управляется определенным административным ответственным лицом. Обычно его границы совпадают с границами оператора. SEG размещается на границе домена безопасности, и осуществляет политику безопасности домена по отношению к другим SEG в доменах безопасности точки назначения. Весь трафик внутри IMS маршрутизируется через SEG, особенно если трафик является внутридоменным, то есть трафик, источник которого находится в другом домене безопасности нежели домен безопасности получателя. Защита внутридоменного трафика подразумевает

под собой соблюдение принципов конфиденциальности, целостности информации и аутентификации.

Межсетевой шлюз сокрытия топологии (THIG). Данная функциональность может быть использована для сокрытия конфигурации, емкости и топологии сети от внешних сетей. Если оператор желает использовать функциональность сокрытия, то он должен разместить THIG на пути маршрутизации при получении запросов либо ответов от других IMS сетей. Аналогично, THIG должен быть помещен на маршрутном пути запросов и ответов, генерируемых для другой IMS сети. THIG выполняет шифрование и дешифрование всех заголовков, которые раскрывают топологическую информацию о сети оператора.

Обслуживающий узел поддержки GPRS (SGSN) связывает сеть радио доступа (RAN) и пакетную сеть. Он отвечает за выполнение как функций управления, так и функции контроля трафика в домене коммутации пакетов. Управление включает в себя две основные функции: управление мобильностью и управление сессией. Управление мобильностью связано с определением местонахождения и состояния устройства пользователя, а также аутентификацией как пользователя, так и устройства пользователя. Управление сессией включает в себя контроль установления соединения и контроль любых изменений в существующих соединениях. Кроме того, он также управляет сервисами и ресурсами 3G. Контроль трафика является частью выполняемого управления сессией. SGSN выполняет функции шлюза для туннелирования пользовательской информации, другими словами, он передает трафик пользователя между устройством пользователя и GGSN. SGSN также обеспечивает соединение с необходимым уровнем QoS и генерирует информацию учета стоимости.

Шлюзовый узел поддержки GPRS (GGSN) обеспечивает взаимодействие с внешними пакетными сетями передачи данных. Первичной функцией GGSN является соединение устройства пользователя с внешней пакетной сетью передачи данных, которые содержат IP ориентированные приложения и сервисы. Внешней сетью передачи данных с коммутацией пакетов, к примеру, может быть сеть IMS или Internet. Другими словами, GGSN маршрутизирует пакеты IP, содержащие сигнальную информацию SIP от устройства пользователя к P-CSCF и наоборот. Кроме того, GGSN выполняет маршрутизацию медиа IP пакетов в сеть назначения (например, к GGSN сети назначения). Предоставляемый сервис взаимодействия реализуется как точка доступа, относящаяся к различным сетям, к которым хочет подключиться абонент. В большинстве случаев IMS имеет свои точки доступа. Когда устройство пользователя активирует носитель (PDP контекст) к точке доступа IMS, GGSN выделяет динамический IP адрес устройству пользователя. Этот IP адрес используется в процессе IMS регистрации, а также в качестве контактного адреса устройства пользователя при установлении сессии. Кроме того, GGSN управляет использованием PDP контекстов для медиа трафика IMS и генерирует информацию учета стоимости.

2.6 Функции учета стоимости.

Безлимитная и основанная на объеме передаваемых данных схемы учета стоимости являются традиционными схемами учета стоимости в современных IP сетях. IMS использует новые модели тарификации, которые, в свою очередь, открывают новые бизнес модели для IMS операторов. Способность производить тарификацию, основываясь на сессии, событии или сервисе является одним из ключевых преимуществ, предоставляемых

IMS операторам. Для конечных пользователей также появляются очевидные преимущества. Например, оператор может предоставлять сетевые игры как предоплачиваемый сервис (то есть пользователь должен иметь деньги на счете для пользования услугой), а остальные мультимедийные сессии как сервисы с постоплатой (то есть пользователь периодически платит за услуги, например, раз в месяц), мгновенный обмен сообщениями может предоставляться как безлимитный сервис, но обмен сообщениями, основанный на сессии, может быть тарифицирован по-другому (например, основываясь на продолжительности сессии или на основе количества переданных байт).

Для предоставления сервисов постоплаты IMS необходимо поддерживать механизм отложенной тарификации. Отложенная тарификация – это тарификация, при которой информация учета стоимости накапливается после окончания сессии, и система тарификации не влияет на сервис в режиме реального времени. При таком принципе тарификации пользователь обычно получает счет, например, ежемесячно, в котором отражены тарифицируемые услуги за указанный период. Предоплачиваемые сервисы требует поддержки тарификации в режиме реального времени. Это значит, что элементы сети IMS должны координировать свою работу с системой тарификации реального времени (OCS) перед тем, как разрешить пользователям использовать услугу. OCS отвечает за взаимодействие со счетом пользователя в режиме реального времени и за мониторинг или контроль оплаты использования сервиса.

Элементы сети IMS отслеживают, когда выполняется условие начала тарификации. После выполнения данного условия элемент сети собирает необходимую информацию из запроса SIP, и либо запрашивает разрешение продолжить обработку запроса у системы тарификации (тарификация в режиме реального времени), либо отправляет необходимую информацию в

систему учета стоимости для генерации CDR для последующей обработки (отложенная тарификация), и разрешает продолжение обработки SIP запроса. Триггер включения тарификации может быть включен инициацией сессии, изменением сессии, завершением сессии или просто любой SIP транзакцией, например MESSAGE, PUBLISH, SUBSCRIBE запросом (тарификация по событию). Кроме того, триггером может являться факт присутствия определенного заголовка SIP или информации SDP. Основываясь на получаемой информации, система тарификации либо снимает деньги со счета абонента (тарификация в режиме реального времени), либо передает CDR в биллинговую систему.

ГЛАВА 3. Услуга контроля присутствия.

3.1 Преимущества внедрения услуги

Услуга контроля присутствия полностью изменяет современное представление о коммуникациях. Она усовершенствует сервис обмена мгновенными сообщениями, а также может быть задействована во многих других приложениях и услугах.

Услуга контроля присутствия представляет собой динамический профиль пользователя, видимый другим пользователям и используемый для предоставления пользователем информации о себе и управления услугами. Эта информация может включать в себя статус пользователя и устройства, информацию о местонахождении или условиях окружающей обстановки, возможности терминала пользователя, предпочитаемый метод общения и предпочитаемые сервисы.

Услуга контроля присутствия может удовлетворить спрос различных групп пользователей. Эти группы могут варьироваться от корпоративных бизнес клиентов до тинэйджеров, первые из которых будут использовать услугу для более удобного управления доступностью сотрудников, а вторые как новый способ выразить себя.

Базовая услуга присутствия работает в настоящее время как публикация-получение информации людьми друг о друге. Операторы могут использовать ее для отображения атрибутов присутствия, связанных с инфраструктурой сети, таких как местонахождение абонента и возможности его терминала в определенной сети. Услуга контроля присутствия позволяет создавать такие приложения как маршрутизация вызовов на основе информации присутствия, сетевые игры с использованием информации присутствия, выделение новых,

нацеленных на определенную группу пользователей, рекламных каналов. Одним из наиболее ярких примеров приложений, задействующих услугу контроля присутствия, является динамическая телефонная книга, в которой динамически изменяется информация о состоянии абонентов.

Услуга контроля присутствия может внести вклад в существующий бизнес и создать новый бизнес сама по себе. Предоставление базовой услуги присутствия дает операторам связи большое преимущество по сравнению с теми операторами, которые ее не предоставляют. Предоставляя свою личную информацию оператору, абоненты дают оператору возможность внедрять новые виды услуг, которые без этой информации использовать было бы невозможно. Услуга контроля присутствия также гарантирует появление дополнительного трафика в рамках других сервисов, например, сервиса обмена сообщениями. Кроме того, услуга контроля присутствия минимизирует количество несостоявшихся вызовов, которые происходят по причине недоступности или занятости абонентов.

3.2 Принцип работы услуги

- Услуга контроля присутствия несет в себе две составляющие: предоставление информации пользователя другим пользователям
- предоставление данному пользователю информации о других пользователях.

Такая информация может включать в себя

- доступность терминала и владельца терминала

- предпочтения в способах общения
- возможности терминала
- текущая деятельность
- местонахождение абонента
- доступные сервисы

Алгоритм работы услуги контроля присутствия определяет следующих участников (рис. 3.1)

Рис. 3.1

Участник, предоставляющий информацию присутствия о себе, называется пользователем присутствия. Пользователь генерирует информацию присутствия (набор атрибутов, характеризующих свойства пользователя, такие как статус, возможности, и др.). Один пользователь присутствия может владеть несколькими устройствами. Эти устройства несут в себе функции агента пользователя, они которые предоставляют информацию присутствия о данном пользователе.

На рисунке 3.1 изображены три агента пользователя – терминал IMS, лэптоп и настольный компьютер. Каждый из них обладает частью информации о пользователе. Лэптоп владеет информацией о том, использует ли его пользователь в настоящее время, такой же информацией обладает компьютер. IMS терминал знает статус регистрации пользователя и то, является ли он участником какого-либо типа информационного обмена в настоящий момент. Кроме того, они могут обладать более богатой информацией, такой как, например, время, когда пользователь вернется с обеда, доступен ли пользователь для видеоконференции, настроение пользователя. Все агенты пользователя отправляют доступные им элементы информации агенту присутствия, который собирает их воедино и получает полное представление о состоянии пользователя.

На рисунке также изображены два наблюдателя. Наблюдатель – это участник, который получает текущую информацию присутствия пользователя от агента присутствия. Существует несколько типов наблюдателей. Неподписанный наблюдатель – это наблюдатель, который запрашивает информацию присутствия у агента присутствия. Подписанный наблюдатель – это наблюдатель, который должен уведомляться о каждом изменении информации присутствия пользователя, то есть подписанный наблюдатель обладает точным обновляемым образом информации присутствия пользователя.

Как правило, приложения объединяют функциональности наблюдателя и пользователя присутствия, таким образом, скрывая функциональные различия между публикацией и запросом информации присутствия конечным пользователем.

Услуга контроля присутствия – это отдельное приложение, построенное на основе технологии уведомлений о событиях SIP. Данная функциональность

позволяет агенту пользователя подписываться на информацию присутствия пользователя с помощью SUBSCRIBE транзакции. Состояние подписки хранится в агенте присутствия пользователя, который выступает как уведомитель. Агент присутствия уведомляет всех подписанных наблюдателей с помощью NOTIFY транзакции в случае, если в информации подписки пользователя происходят изменения.

Все SUBSCRIBE/NOTIFY транзакции содержат заголовок Event, идентифицирующий событие, с которым связана подписка или оповещение. RFC 3856 [2] определяет расширение SIP для реализации услуги контроля присутствия, которое определяется значением «presence» заголовка Event запросов SUBSCRIBE и NOTIFY.

Традиционно Интернет технологии используют URI для идентификации ресурсов, которые могут быть получены с помощью определенного протокола (например, sip, http, ftp) или связанных с определенной функциональностью (например, tel, mailto). Услуга контроля присутствия определяет pres URI для идентификации пользователя присутствия или наблюдателя.
Пример pres URI:
pres:user@example.com

3.3 Жизненный цикл услуги контроля присутствия.

В течение жизненного цикла информация присутствия пользователя претерпевает определенное число изменений, начиная с создания, хранения и заканчивая доставкой потребителю. На рис. 3.2 схематично изображен жизненный цикл информации присутствия.

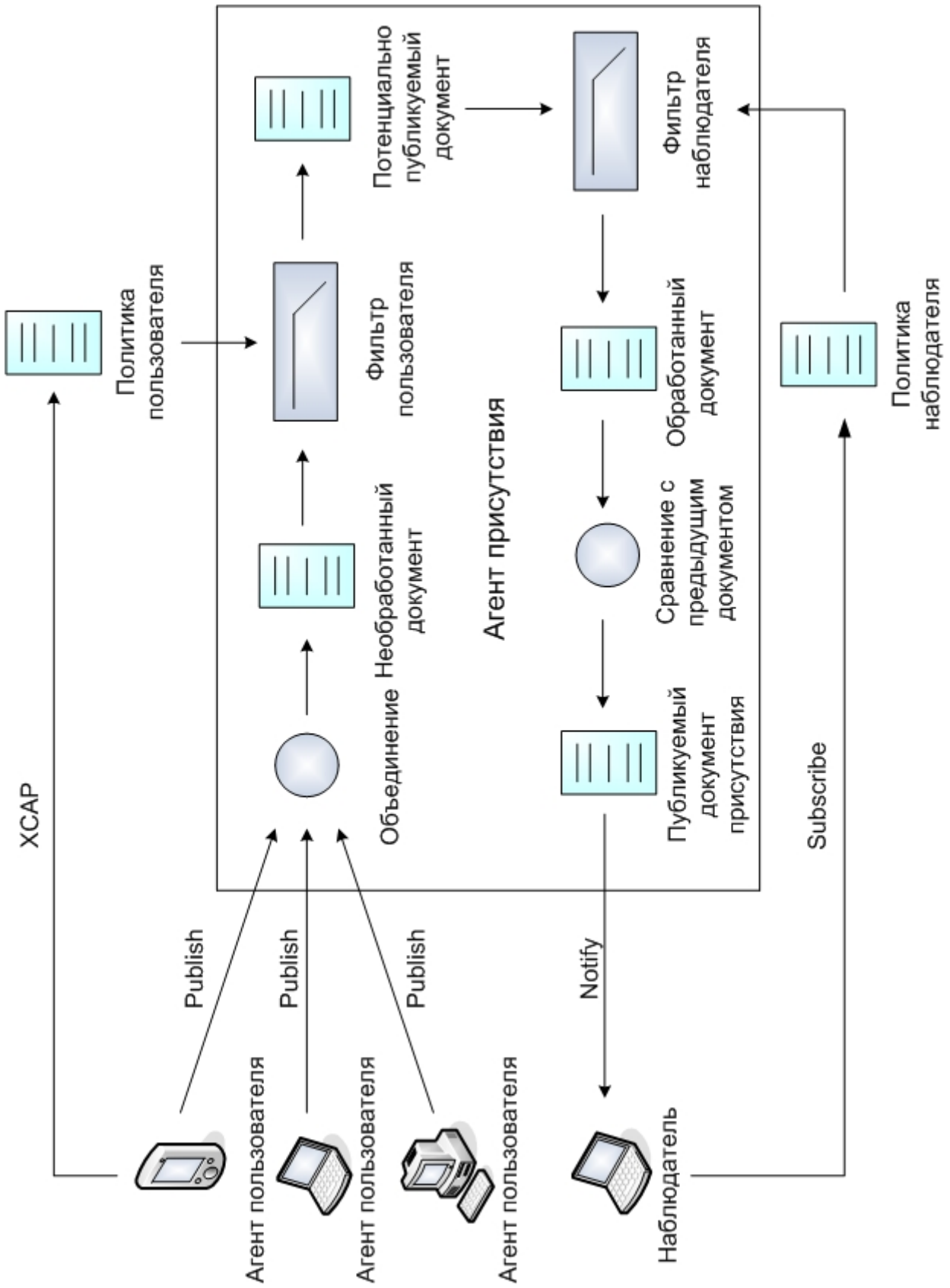
XCAP
Политика пользователя
Publish
Publish
Publish
Агент пользователя
Агент пользователя
Агент пользователя
Объединение
Необработанный документ
Фильтр пользователя
Потенциально публикуемый документ
Агент присутствия
Фильтр наблюдателя
Обработанный документ
Сравнение с предыдущим документом
Публикуемый документ присутствия
Notify
Наблюдатель
Subscribe
Политика наблюдателя

Рис. 3.2

Пользователь присутствия публикует определенную информацию присутствия. Эта информация может слегка варьироваться в зависимости от того, какой агент пользователя используется в данный момент. Например, пользователь может быть не за компьютером, но участвовать в разговоре по мобильному телефону, так что эти подробности будут отображены в информации присутствия пользователя.

В определенный момент времени каждый агент пользователя отправляет запрос PUBLISH, содержащий информацию присутствия в документе присутствия. Документ присутствия, получаемый агентом Присутствия, передается на обработку, которая объединяет документы присутствия с трех разных агентов пользователя в один необработанный документ.

Затем этот документ проходит процедуру фильтрации, в процессе которой к документу присутствия применяются фильтры пользователя, удаляющие из документа нежелательную для публикации информацию. Для этого пользователь предварительно загружает документ политики присутствия на агент присутствия, который определяет, какие наблюдатели имеют доступ к той или иной информации. Агент присутствия применяет политику присутствия пользователя к необработанному документу и после этого получает потенциально публикуемый документ.

Потенциально публикуемый документ проходит еще одну процедуру фильтрации, в процессе которой к документу применяются фильтры, накладывающие ограничения наблюдателя на получаемую информацию. Эти фильтры позволяют отфильтровать информацию, в получении которой наблюдатель не заинтересован.

После фильтрации документа агент пользователя сверяет документ присутствия с копией предыдущего опубликованного документа для того, чтобы определить разницу между их содержимым. После этого агент присутствия может публиковать только изменения, произошедшие с пользователем, а не полный документ присутствия.

Агент присутствия формирует запрос NOTIFY, содержащий документ присутствия с изменениями статуса пользователя, и отправляет его наблюдателям.

Наблюдатели сверяют новый документ с копией предыдущего документа присутствия, объединяют их и получают полную информацию присутствия наблюдаемого пользователя.

ГЛАВА 4. Формат информации присутствия

4.1 Понятие PIDF

Формат информации присутствия (PIDF) - это не зависящий от протокола документ, который разработан для передачи информации присутствия между двумя участниками услуги контроля присутствия.

PIDF специфицирован в RFC 3863 [3]. Он представляет собой общий профиль присутствия таким образом, что различные протоколы, а не только SIP, могут использовать его для прозрачной передачи информации присутствия.

PIDF содержит минимальный набор инструментов, необходимый для выполнения базовых требований. Этот малый набор параметров гарантирует возможность повторного использования PIDF в других протоколах. С другой стороны, PIDF является хорошо расширяемым протоколом, то есть протокол можно расширить при необходимости выхода за пределы минимальной модели.

PIDF кодирует информацию присутствия в документ XML, в результате чего он может быть передан, как и другие MIME документы, при публикации (в PUBLISH транзакции) и при операции подписки/уведомления (SUBSCRIBE/NOTIFY транзакции). PIDF определяет новый MIME тип – application/pidf+xml для обозначения типа приложения и кодирования.

4.2 Содержимое PIDF.

Документ PIDF содержит информацию присутствия пользователя. Эта информация состоит из определенного числа элементов, каждый из которых называется кортеж. Каждый кортеж определяет статус пользователя (open или closed, что означает соответственно доступен/недоступен), опциональный элемент contact, который определяет URI для контакта, опциональные элементы note и timestamp, и, возможно, другие элементы расширения.

PIDF определяет только статусы open и closed, что является недостаточным для многих приложений, но он допускает расширения, определяющие другие статусы, такие как at home, on the phone, away и другие.

На рис. 4.1 приведен PIDF документ пользователя, чей кортеж содержит только то, что он доступен для коммуникаций. Он предоставляет свой TEL URI в качестве контактной информации и комментарий note о том, что это сотовый телефон.

```
<xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
          entitiy="pres:user@example.com">
     <tuple id="qoica32">
          <status>
               <basic>open</basic>
          </status>
          <contact priority="0.9">tel:+1555876543</contact>
          <note>my cell phone</note>
     </tuple>
</presence>
```

Рис. 4.1

Так как PIDF является протоколонезависимым, он не «углубляется» в информацию, чтобы идентифицировать ее содержимое. Он отображает информацию присутствия пользователя как серию кортежей, но не определяет однозначно, что моделирует тот или иной кортеж, и не определяет, как отображать кортежи на различные элементы протокола SIP.

Интернет – проект «Информационная модель для услуги контроля присутствия» ликвидирует этот вакуум, предоставляя модель, которая отображает кортежи в систему коммуникаций SIP. Данная модель построена на трех основных свойствах пользователя присутствия:

- Сервис. Коммуникационный сервис, такой, как обмен сообщениями или телефония. Это система для взаимодействия между пользователями, которая предоставляет определенные возможности или контент.
- Устройство. Коммуникационное устройство – это физический компонент, с которым взаимодействует пользователь для того, чтобы инициировать или принять соединение. Это может быть телефон, PDA, персональный компьютер.
- Человек. Конечный пользователь, в целях создания информации присутствия характеризуемый состояниями, такими, как «занят», «расстроен» и пр., которые отображают его способность или желание участвовать в коммуникациях.

На рис. 4.2 показана информационная модель услуги контроля присутствия.

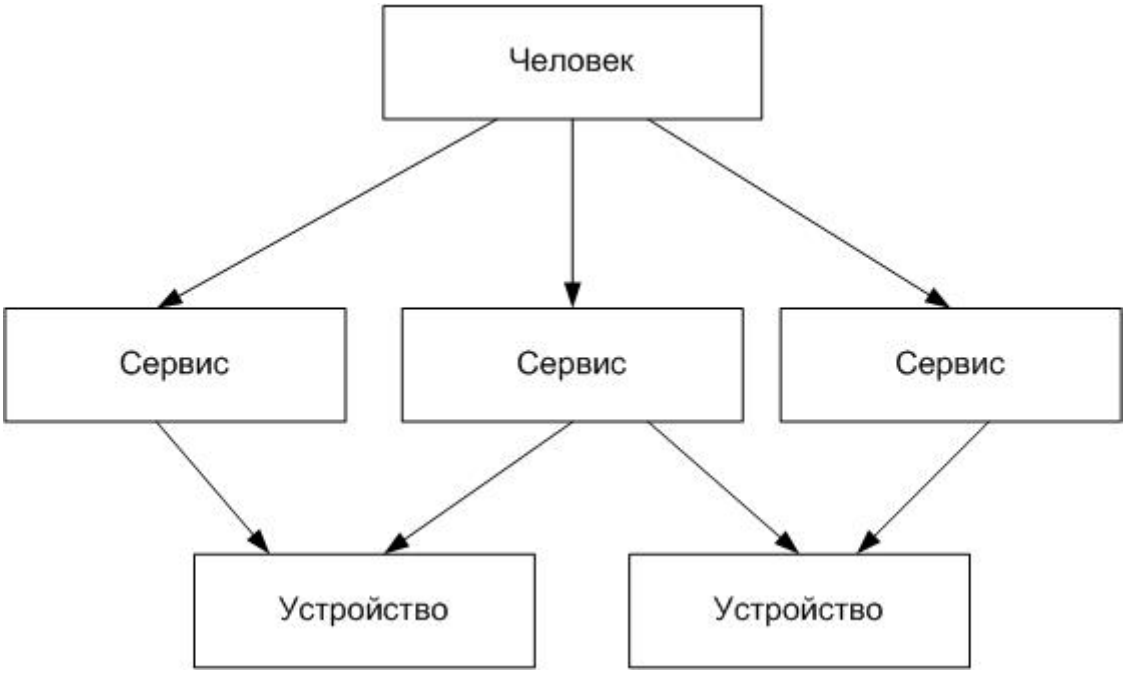

Рис. 4.2

Данная модель подразумевает, что пользователь присутствия характеризуется четырьмя различными информационными компонентами: URI, человек, сервис, устройство. Информационная модель учитывает, что один пользователь может иметь несколько URI. Обычным является случай, когда пользователь представлен с pres URI и SIP URI.

Информационный компонент «Человек» предоставляет информацию о конечном пользователе. Данный компонент подразумевает описание двух аспектов, связанных с пользователем, – его характеристики и его статус. Характеристики – это статистическая пользовательская информация, которая не изменяется во времени, такая как рост или дата рождения. Статус отображает динамическую информацию о пользователе, такую как деятельность пользователя (говорит по телефону, на совещании), или его настроение (доволен, счастлив и пр.)

SIP модель присутствия допускает наличие только одного информационного элемента «Человек» для одного пользователя, хотя, допускается, что компонент «Человек» указывает на что-либо, что ведет себя как человек, но им не является, например, это группа людей в контакт-центре или животное.

Пользователи получают доступ к сервисам, и желание их взаимодействовать с различными сервисами моделируется с помощью информационного компонента «Сервис». «Сервис» может включать в себя видео телефонию, push-to-talk, обмен сообщениями и т. д. Как и информационный компонент «Человек», компонент «Сервис» может быть описан в терминах характеристик (статическая информация) и статусов (динамическая информация). Характеристики сервисов могут включать в себя, например, SIP методы, поддерживаемые устройством, возможности предоставлять сервисы (видео, аудио). Статус включает в себя, например, желание пользователя участвовать в том или ином виде коммуникаций. Сервисы также могут описывать URI, которые нужно использовать для доступа к ним.
Последний информационный компонент – это компонент устройства. Данный компонент моделирует физическую платформу, на которой работают сервисы. Как и компоненты «Человек» и «Сервис», компонент «Устройство» описывается в терминах характеристик и статусов. Характеристики включают в себя размер экрана, количество цветов и пр. Статусы включают в себя уровень заряда батареи, географическое местонахождение устройства и т. д. Устройства идентифицируются с помощью Device ID, то есть Uniform device name или URN. Это может быть IMEI, ESN, MAC адрес.

4.3 Информационная модель SIP

Так как PIDF был создан ранее SIP информационной модели присутствия, и так как цель PIDF – стать минимальным общим звеном в различных системах присутствия, появляется необходимость отображать существующую информационную модель SIP в PIDF. Идея состоит в том, чтобы использовать существующую модель PIDF, где это возможно, а во всех других случаях расширить его.

Отображение информационной модели SIP в PIDF достигается использованием существующих XML элементов PIDF, где это возможно, и созданием новых элементов, для того чтобы оперировать с новыми информационными компонентами.

Отображение информационной модели SIP услуги контроля присутствия изображено на рис. 4.3.

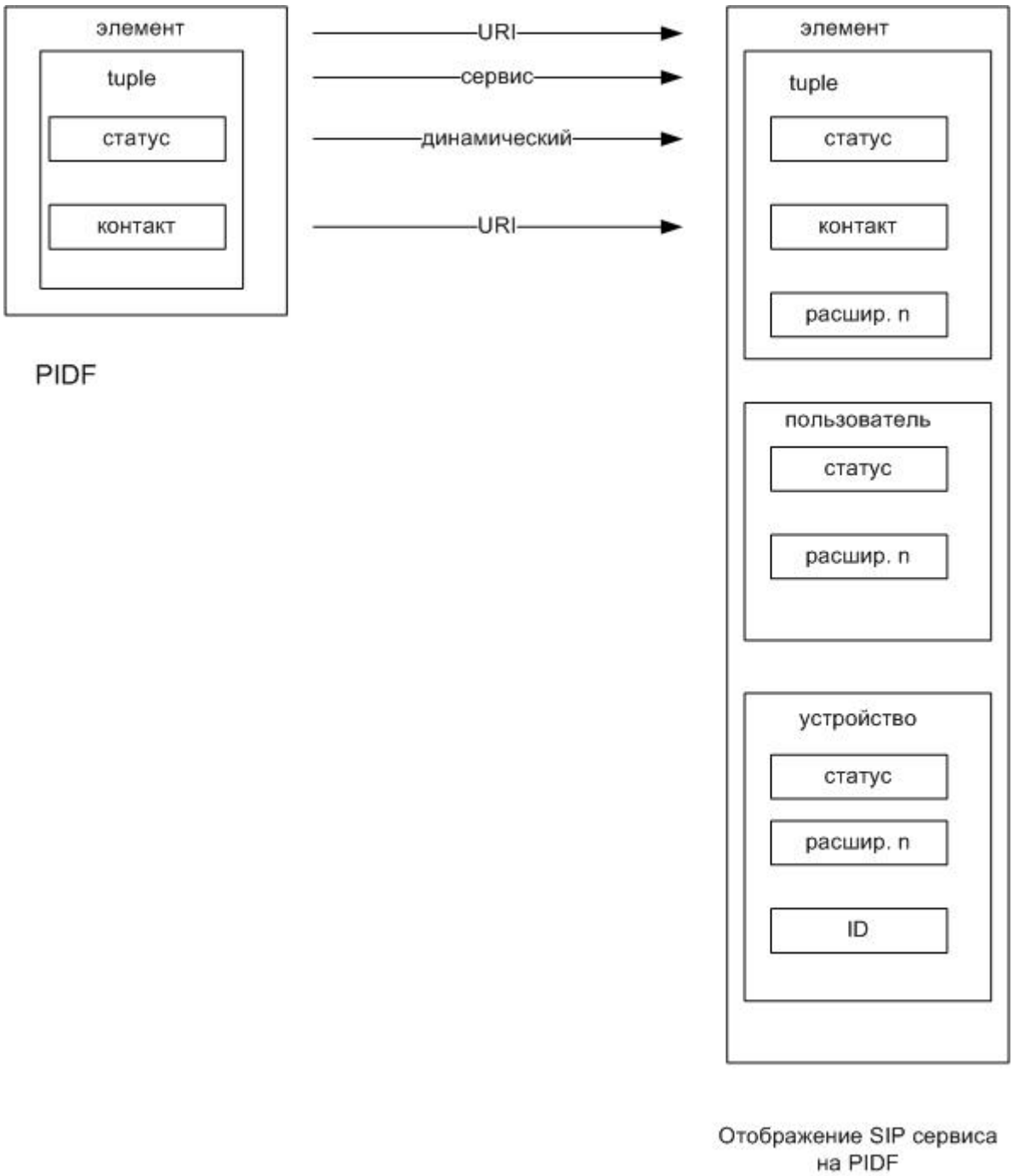

Рис. 4.3

Корневой элемент presence содержит атрибут entity, который в случае информационной модели SIP присутствия описывает URI пользователя.

Элемент tuple используется для описания информационного компонента «Сервис». Дочерний элемент status используется для описания характеристик или динамической информации о сервисе. Элемент contact содержит URI

сервиса. Статическая информация о сервисе становится новым элементом расширения в виде дочернего элемента tuple.

Новый элемент person создается для отображения информационного компонента «Человек». Дочерний элемент status содержит динамическую информацию о пользователе, в то время как элементы расширения содержат статическую информацию. Новый элемент device является дочерним элементом presence, он используется для отображения информационного компонента «Устройство». Он также содержит компонент status, содержащий динамические свойства устройства и некоторое количество расширений для хранения статической информации.

4.4 Расширенный формат информации присутствия (RPID).

PIDF документ отображает минимально необходимую информацию о пользователе присутствия, которой, скорее всего, будет недостаточно для коммерческого применения. Например, пользователь может желать проинформировать наблюдателей о том, что он находится в состоянии online но не хочет участвовать ни в каком обмене информацией, так как ведет машину. PIDF не предоставляет возможности отразить это состояние пользователя.

Расширенный формат информации присутствия Rich Presence Information Data Format (RPID) является расширением PIDF, позволяющим описать состояние пользователя в деталях. Как и PIDF, RPID кодируется с помощью XML. RPID имеет обратную совместимость с PIDF. Если наблюдатель не понимает RPID, он может хотя бы получить минимальное количество

информации из PIDF. RPID расширение специфицировано в Интернет проекте “RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)” [4].

Пользователь может задавать свою информацию присутствия как вручную, так и автоматически. Например, приложение-календарь может автоматически заполнять информацию присутствия о том, что пользователь online или участвует в собрании в соответствии со своим расписанием работы. Телефон пользователя может автоматически обновлять информацию о состоянии абонента, например, о том, что он участвует в разговоре.

RPID определяет новый элемент activities, который отображает вид деятельности, в котором задействован абонент. Спецификация допускает использование следующих видов деятельности: разговаривает по телефону, вышел, на запланированной встрече, завтракает, обедает, ужинает, не на работе по причине праздника, на работе, на совещании, ведет машину, путешествует, в отпуске, спит, занят, на спектакле, играет, на презентации, смотрит телевизор, занимается неизвестной деятельностью.

Данный список является расширяемым, поэтому возможно появление новых видов деятельности.

Элемент class позволяет пользователю сгруппировать сходные элементы «Человек», «Сервис» или «Устройство» в один класс.

Элемент deviceID содержит идентификатор устройства, предоставляющего определенный сервис. Он позволяет отличать устройства, относящиеся к одной информации присутствия. Этот идентификатор является URN, идентифицирующим устройство.

Новый элемент mood позволяет описать настроение пользователя (счастлив, грустен, смущен).

RPID включает в себя два элемента, содержащих информацию о местонахождении пользователя. Один из этих элементов place-is. Он содержит свойства помещения, например, шумное, темное, тихое, слишком яркое, некомфортное, неподходящее. Элемент place-type позволяет передавать тип помещения, где находится пользователь, например, дом, офис, библиотека, театр, отель, ресторан, школа, улица, автобус и многие другие.

RPID также включает в себя элемент privacy, определяющий тип медиа, который пользователь может использовать в данное время без того, чтобы посторонние люди были в курсе предмета обсуждения.

Элемент relationship показывает, какие отношения существуют между пользователем и альтернативным контактом. Возможные значения отношений к альтернативному контакту включают в себя такие как семья, друг, коллега, помощник, сам пользователь, начальник и пр.

Элемент user-input позволяет определить, используется ли клавиатура или джойстик устройства пользователем в настоящий момент, или нет.

На рис. 4.4 показан пример RPID документа, предоставляемый пользователем наблюдателям.

```
<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf
   xmlns:xsi="http://www.w3.org/2001/XMLNSschema-instance"
   xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
   xmlns:r="urn:ietf:params:xml:ns:pidf:rpid"
   entity="pres:alice@example.com">
     <tuple id="3bfua">
       <status>
         <basic>open</basic>
       </status>
       <r:deviceID>urn:device:001349038B74</r:deviceID>
       <r:service-class><r:electronic/></r:service-class>
       <r:status-icon>
            http://www.example.com/alice/icon.jpg
       </r:status-icon>
       <contact priority="0.8">
            sip:alice@pc.example.com
       </contact>
       <timestamp>2007-05-15T07:52:14Z</timestamp>
     </tuple>

     <dm:device id="vjsa43">
       <r:user-input idle-threshold="300">
          last-input="2007-05-15T00:23:21">idle</r:user-input>
       <dm:deviceID>urn:device:00134098B74</dm:deviceID>
       <dm:note>PC</dm:note>
     </dm:device>

     <dm:person id="alice">
       <r:activities><r:away/></r:activities>
       <r:mood><r:happy/></r:mood>
       <r:place-is>
          <r:audio>
             <r:quiet/>
          </r:audio>
          <r:video>
            <r:quiet/>
          </r:video>
       </r:place-is>
       <r:place-type>
          <r:home/>
       </r:place-type>
       <r:privacy>
          <r:audio/>
          <r:video/>
          <r:text/>
       </r:privacy>
       <r:sphere><r:home/></r"sphere>
     </dm:person>
     <note>I have some visitors at home</note>
</presence>
```

Рис 4.4

Информация поступает с персонального компьютера пользователя, в ней говорится, что пользователь не за компьютером в данный момент, находится дома, в тихой обстановке, и у него хорошее настроение.

4.5 Возможности.

Каждый наблюдатель, получающий информацию о пользователе, хотел бы получать информацию о функциональности, поддерживаемой пользователем. Это было бы полезно, когда наблюдатель выбирает тот или иной способ общения с пользователем. Например, если пользователь публикует информацию о том, что его устройство поддерживает аудио и видео, наблюдатель выберет видео или аудио сессию, а не обмен сообщениями.

Для этих целей был создан проект “User Agent Capability Extension to the Presence Information Data Format”, описывающий расширение PIDF, которое позволяет отображать предпочитаемые пользователем способы взаимодействия, описанные в RFC 3840 [5], в новые XML элементы документа PIDF.

Возможности разделяются на возможности сервисов и возможности устройств. Возможности сервисов описывают такие возможности как поддержка видео, аудио, обмена сообщениями, дуплекса и др. Возможности устройств характеризуют свойства устройств, например, фиксированное это устройство или мобильное. Данные расширения построены на основе

информационной модели присутствия, и, следовательно, они расширяют элементы tuple и device.

Для переноса информации о возможностях сервисов и устройств определяется два новых элемента: соответственно, servcaps и devcaps.

Возможности сервисов передаются в XML элементе servcaps. Он является дочерним элементом по отношению к элементу tuple, определенному в PIDF, так как элементы tuple используются для описания сервисов в соответствии с информационной моделью. Элемент servcaps может включать в себя следующие подэлементы:
audio, application, data, control, video, text, message, type, automata, class, duplex, description, event-packages, priority, methods, extensions, schemes, actor, isfocus, languages.

Элементы audio, video, application, data, control, text являются булевыми переменными, которые отображают, поддерживает ли сервис потоки аудио, видео, текстовые потоки, потоки управления, приложений или информационный потоки.

Элемент type показывает, какие возможные MIME типы может принимать сервис. MIME типы, как правило, отображаются в заголовке Content-Type сообщения SIP.

Элемент class показывает, используется ли сервис для делового общения или в личных целях.

Элемент duplex показывает, может ли сервис одновременно отправлять и получать медиа (full), либо может только отправлять или получать

поочередно (half), либо только отправлять (send-only) или только получать (receive-only).

Элемент description содержит текстовое описание сервиса.

Элемент event-packages содержит список event-packages SIP, которые поддерживает сервис. Как и в случае с поддерживаемыми медиа потоками, данный элемент относится к расширениям SIP, поддерживаемым сервисом.
Элемент priority показывает, какие приоритеты SIP поддерживает данный сервис. Приоритеты обозначаются целыми числами, и приложение может показать диапазон возможных приоритетов, поддерживаемых им.

Элемент method показывает поддерживаемые сервисом SIP методы.

Элемент extensions показывает список поддерживаемых сервисом расширений SIP. Этот элемент представляет собой список поддерживаемых option-tags, которые могут появиться в заголовках Supported или Required.

Элемент schemes показывает, какие схемы URI поддерживает данный сервис.

Элемент Isfocus показывает, является ли данный сервис централизованным сервисом конференций.

Элемент languages показывает способность сервиса отображать различные языки.

Способности устройства передаются в элементе devcaps. Элемент devcaps является дочерним по отношению к элементу device, определенному в информационной модели. Данный элемент может содержать следующие подэлементы: mobility, priority, description.

Первый из них показывает, является ли устройство мобильным.

Второй показывает приоритет вызова, который устройство будет обслуживать. Данный элемент может содержать диапазон значений, которые поддерживаются данным устройством. Последний из элементов содержит текстовое описание устройства.

На рис. 4.5 показан документ PIDF, расширенный с помощью информационной модели присутствия и возможностей.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf
   xmlns:xsi="http://www.w3.org/2001/XMLNSschema-instance"
   xmlns:cap="urn:ietf:params:xml:ns:pidf:caps"
   xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
   entity="pres:alice@example.com">

   <tuple id="3bfua">
     <status>
        <basic>open</basic>
        <cap:servcaps>
          <cap:audio>true</cap:audio>
          <cap:video>true</cap:video>
          <cap:message>true</cap:message>
          <cap:duplex>
             <cap:supported>
               <cap:full/>
             </cap:supported>
          </cap:duplex>
          <cap:description>General service</cap:description>
          <cap:methods>
             <cap:supported>
               <cap:INVITE/>
               <cap:ACK/>
               <cap:CANCEL/>
               <cap:BYE/>
               <cap:MESSAGE/>
               <cap:PRACK/>
               <cap:UPDATE/>
             </cap:supported>
          </cap:methods>
          <cap:event-packages>
             <cap:supported>
               <cap:reg/>
             </cap:supported>
          </cap:event-packages>
          <cap:extensions>
             <cap:supported>
               <cap:100rel/>
               <cap:precondition/>
             </cap:supported>
          </cap:extensions>
          <cap:schemes>
             <cap:supported>
               <cap:s>sip</cap:s>
               <cap:s>sips</cap:s>
             </cap:supported>
          </cap:schemes>
        </cap:servcaps>
```


Рис. 4.5/лист 1

```
      </status>
      <contact>sip:alice@example.com</contact>
      </tuple>

      <dm:device>
         <cap:devcaps>
           <cap:mobility>
             <cap:supported>
                <cap:mobile/>
             </cap:supported>
           </cap:mobility>
         </cap:devcaps>
      <dm:deviceID>urn:device:039fa209</dm:deviceID>
      </dm:device>
  </presence>
```

Рис. 4.5/лист 2

Пользователь отображает возможности, относящиеся и к сервису, которым он пользуется, и к устройству. Возможности сервиса включают в себя поддержку аудио, видео, текста и полнодуплексного обмена информацией. Затем приводится описание SIP методов, event-packages, SIP расширений и схем URI, поддерживаемых сервисом. В возможностях устройства пользователь отмечает, что данное устройство является мобильным.

ГЛАВА 5. Информация присутствия.

5.1 Публикация информации присутствия.

Очевидным механизмом для публикации информации присутствия является использование метода REGISTER. Транзакция REGISTER предоставляет информацию об IP адресе пользователя. Таким образом, если пользователь не зарегистрирован, агент присутствия отображает его состояние как offline, а когда он зарегистрирован, состояние меняется на online. С другой стороны, семантика метода REGISTER является очень простой и понятной: регистрируемый пользователь связывает публичный идентификатор пользователя с контактным адресом. Поэтому использование данного метода для переноса информации присутствия кажется не вполне подходящим. Соответственно, более удобно использовать какой-либо другой метод для загрузки информации с агента пользователя агент присутствия.

IETF определяет метод PUBLISH в RFC 3903 [6]. Целью использования данного метода является публикация event-state, используемого в сети SIP для SIP специфичных уведомлениях о событиях (RFC 3265 [7]). Таким образом, метод PUBLISH используется не только для публикации информации присутствия, он достаточно общ для использования в целях публикации любого состояния, используемого в event-package. На рис. 5.1 показан типичный обмен сообщениями при публикации информации присутствия.

Рис. 5.1

Агент пользователя отправляет запрос PUBLISH, содержащий PIDF/RPID документ, к агенту присутствия. Агент присутствия отвечает 200(OK).

5.2 Подписка и уведомления.

Интерфейс, определенный между наблюдателем и агентом присутствия, позволяет наблюдателю подписываться на получение информации присутствия о наблюдаемом пользователе. Подписка на получение информации присутствия выполняется с помощью SUBSCRIBE транзакции. Подписка может быть обычной однократной операцией запроса, в результате которой наблюдатель хочет получить текущую информацию о наблюдаемом пользователе и не хочет, чтобы его уведомляли обо всех последующих изменениях состояния пользователя. Подписка может действовать в течение определенного периода времени. В этом случае наблюдатель получает обновления информации присутствия пользователя в случае, если данная информация изменяется. Если наблюдатель хочет поддерживать подписку

активной на протяжении длительного периода времени, он должен обновлять свою подписку по мере ее истечения.

На рис. 5.2 изображен пример обмена сообщениями.

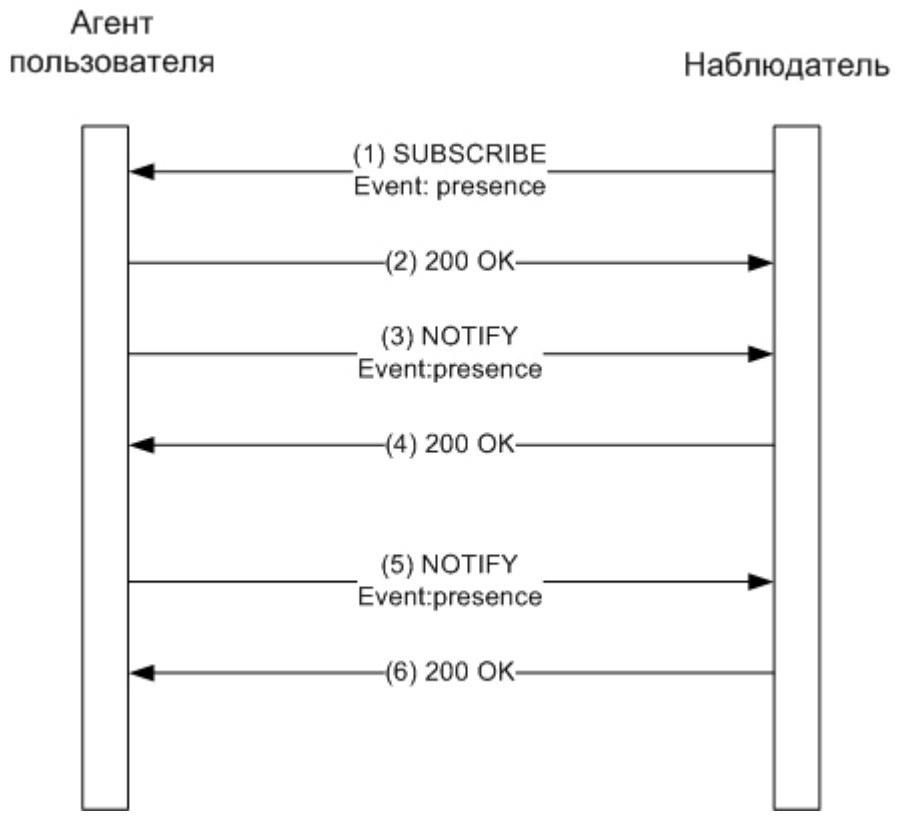

Рис. 5.2

Наблюдатель отправляет запрос SUBSCRIBE на агента пользователя, заголовок Event данного запроса имеет значение presence. Такой запрос говорит о том, что наблюдатель желает подписаться на информацию присутствия об определенном пользователе. Агент присутствия авторизует и аутентифицирует наблюдателя и отвечает 200(OK), после чего отправляет запрос NOTIFY, который в большинстве случаев не содержит информации присутствия, а содержит только статус подписки. Наблюдатель отвечает 200(OK). В случае любого изменения информации присутствия пользователя агент присутствия отправляет запрос NOTIFY содержащий PIDF/RPID документ присутствия. Наблюдатель отвечает 200(OK).

5.3 Информация о наблюдателях.

Как правило, пользователя интересует, какие наблюдатели подписываются на получение его информации присутствия. Для решения данного вопроса IETF определила Watcher info event template-package в RFC 3857 [8]. Watcher info event template package предоставляет пользователю информацию о том, кто просматривает определенный ресурс. В случае использования данного event template-package заголовок Event должен иметь значение presence.winfo.

На рис. 5.3 показано, как работает данный метод.

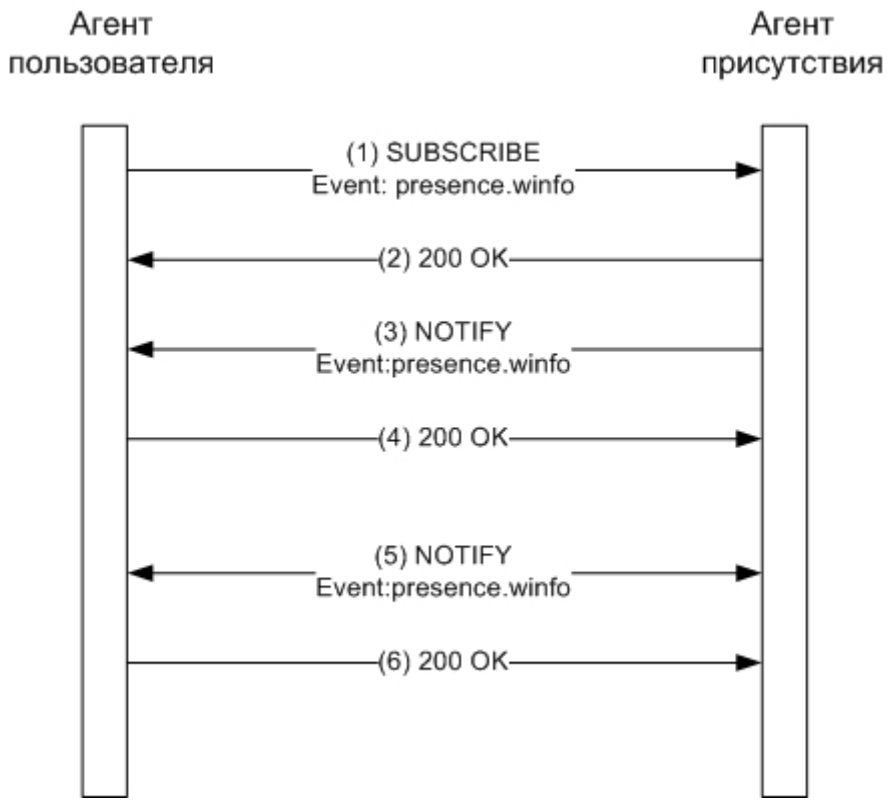

Рис. 5.3

Пользователь, как правило, это агент пользователя, отправляет запрос SUBSCRIBE агенту присутствия, заголовок Event данного запроса имеет

значение presence.winfo. Агент присутствия авторизует и аутентифицирует подписку и отвечает 200(OK). После этого он отправляет запрос NOTIFY для индикации статуса подписки. Кроме того, NOTIFY запрос может содержать XML документ со списком наблюдателей информации присутствия данного пользователя. Агент присутствия будет держать агента пользователя в курсе всех изменений этого списка с помощью последующих NOTIFY запросов.

Способность определять, какие наблюдатели получают информацию присутствия об определенном пользователе – это один, но не единственный мотив создания watcher info функциональности. Вероятно, главной причиной создания данного механизма является необходимость авторизации наблюдателей. Когда наблюдатель подписывается на получение информации присутствия о пользователе, пользователь может захотеть авторизовать эту подписку. Для данной авторизации пользователь должен знать, кто именно выполняет подписку. Все эти задачи решает watcher info event package.

Watcher info event package кодируется с помощью XML. Он определяет новый MIME тип – application/watcherinfo+xml.

ГЛАВА 6. Оптимизация услуги контроля присутствия

6.1 Списки ресурсов.

Как было описано ранее, каждый раз, когда наблюдатель желает подписаться на получение информации присутствия, он обменивается SUBSCRIBE и NOTIFY транзакциями с агентом пользователя только для того, чтобы установить подписку. Как минимум 4 сообщения необходимо отправить и принять наблюдателю для того, чтобы установить подписку на получение информации присутствия о каждом наблюдаемом пользователе. Если наблюдатель подписан на получение информации присутствия, скажем, о 100 пользователях, приложение услуги контроля присутствия данного наблюдателя должно принять и отправить 400 SIP сообщений каждый раз, когда он включает приложение. И это выполняется только для установки подписки. Как правило, запрос NOTIFY даже не содержит информации присутствия на этой стадии. Очевидно, что такой механизм является плохо масштабируемым, по крайней мере, для беспроводных устройств.

В целях решения данной проблемы IETF создал концепцию списка ресурсов [9]. Список ресурсов – это список SIP URI, который должен храниться в специальном функциональном элементе - сервере списков ресурсов. Этот список адресуется собственным SIP URI. В применении к сервису присутствия данный список также называют списком присутствия. Данный список содержит список всех пользователей, на получение информации о которых подписан владелец списка.

Сервер списков ресурсов получает запрос от агента пользователя и перенаправляет его к другим пользователям. Вместо того чтобы посылать

запрос SUBSCRIBE каждому пользователю списка присутствия, наблюдатель отправляет единственный запрос SUBSCRIBE, адресованный своему списку присутствия. Данный запрос принимается Сервером Списков Ресурсов, после чего он пересылает этот запрос всем пользователям, занесенным в список. После этого сервер получает запросы NOTIFY от пользователей, объединяет информацию присутствия от пользователей и отправляет один NOTIFY запрос владельцу списка. Такой способ обмена информацией значительно экономит полосу пропускания и вычислительную мощность агента пользователя.

Данный механизм определяет новый MIME тип данных – application/rlmi+xml. Документ содержит список ресурсов, каждый из которых указывает на PIDF документ каждого наблюдаемого пользователя. Как следствие, запрос NOTIFY содержит multipart/related документ, который включает в себя набор других XML документов.

Использование списка ресурсов, а не индивидуальной подписки, производит сторонний эффект – отсутствие надобности хранения списков присутствия в приложении сервиса присутствия. Данный способ хранения позволяет запускать приложение сервиса присутствия с различных терминалов. При использовании нового терминала пользователю необходимо только сконфигурировать URI списка присутствия вместо конфигурирования одного за другим URI всех наблюдаемых пользователей.

6.2 XML Configuration Access Protocol

Использование списка ресурсов влечет за собой необходимость создания инструмента для управления этим списком. Владелец списка должен иметь возможность добавить в него URI нового наблюдаемого абонента, удалить или изменить URI существующего абонента в списке.

Хорошим решением для создания инструмента управления списком является WEB страница. Однако WEB страница не предоставляет стандартного протокола для конфигурирования списка ресурсов, так как, хотя HTTP и является стандартизированным протоколом, содержимое HTML тела HTTP ответов стандартизированным не является. Этот факт делает использование для данной цели WEB страницы нежелательным, так как усложняет совместимость между терминалами различных производителей и серверами списков ресурсов. Особенно это касается мобильных терминалов, так как размер экрана терминала, устройства ввода и количество цветов дисплея варьируются в зависимости от производителя и отобразить страницу требуемым образом может быть непросто.

IETF выдвинула идею стандартизации не отображения WEB страницы, а протокола механизма модификации содержимого списка ресурсов. Данный протокол получил название XCAP (XML Configuration Access Protocol), он описан в Интернет-проекте “The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)” [10]. XCAP предоставляет пользователю инструмент для добавления, изменения и удаления конфигурационной информации XML любого вида, например, пользователей в списке присутствия, политик авторизации (например, список авторизованных наблюдателей), список участников конференции и пр. XCAP

не определяет, каким должен быть интерфейс пользователя, то есть графическое представление списка.

Как становится ясно из имени протокола, XCAP кодируется в XML. XCAP это всего лишь набор соглашений, которые указывают, как работать с удаленно хранимым XML документом. На рис. 6.1 изображен стек протоколов, поверх которого работает XCAP.

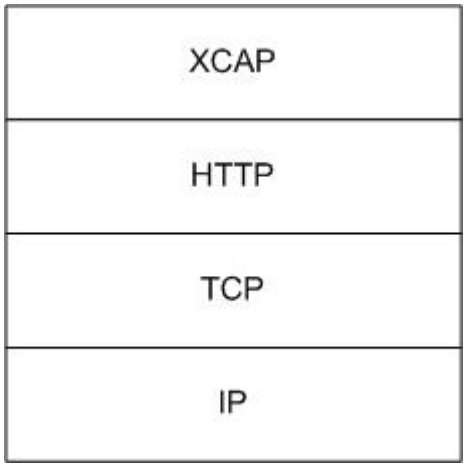

Рис. 6.1

XCAP определяет правила отображения XML документов и их компонентов в HTTP URI. Он также определяет правила, как модификация одного ресурса влияет на другой ресурс. Кроме этого, протокол определяет политики авторизации, связанные с доступом к ресурсам. XCAP определяет набор операций, который отображаются на обычные методы протокола HTTP 1.1. Данные операции устанавливают определенное значение для некоторых заголовков HTTP. XCAP предоставляет пользователю следующие возможные операции:

Создание нового документа, замещение существующего документа, удаление документа, создание нового элемента в существующем документе, замещение элемента в существующем документе, удаление элемента в

документе, создание атрибута в существующем элементе, замещение атрибута в существующем элементе, удаление атрибута из документа.

Пользователи услуги контроля присутствия могут использовать XCAP в целях управления списками присутствия, а также в целях авторизации наблюдателей, так что наблюдатели будут видеть только часть публикуемой информации.

Так как протокол XCAP является многофункциональным, IETF создало понятие идентификатора приложения с использованием XCAP. Для сервиса присутствия IETF определило следующие идентификаторы использования:
XCAP applications usage for resource list – предоставляет способы управления списком присутствия.
XCAP application usage for presence authorization – позволяет пользователю специфицировать набор правил, указывающих, какая часть публикуемой информации является доступной тем или иным пользователям.

6.3 Механизм частичного уведомления.

Частичное уведомление – это уведомление, которое может содержать набор информации присутствия о пользователе. Механизм частичного уведомления определяет новое тело XML документа, которое способно передавать частичное или полное состояние пользователя.

Тело XML аналогично PIDF, но включает в себя новый элемент, который показывает номер версии, а так же информацию о том, содержит документ

полную или частичную информацию. Новое XML тело определяет новый MIME тип application/pidf-partial+xml.

Принцип работы механизма изображен на рис. 6.2

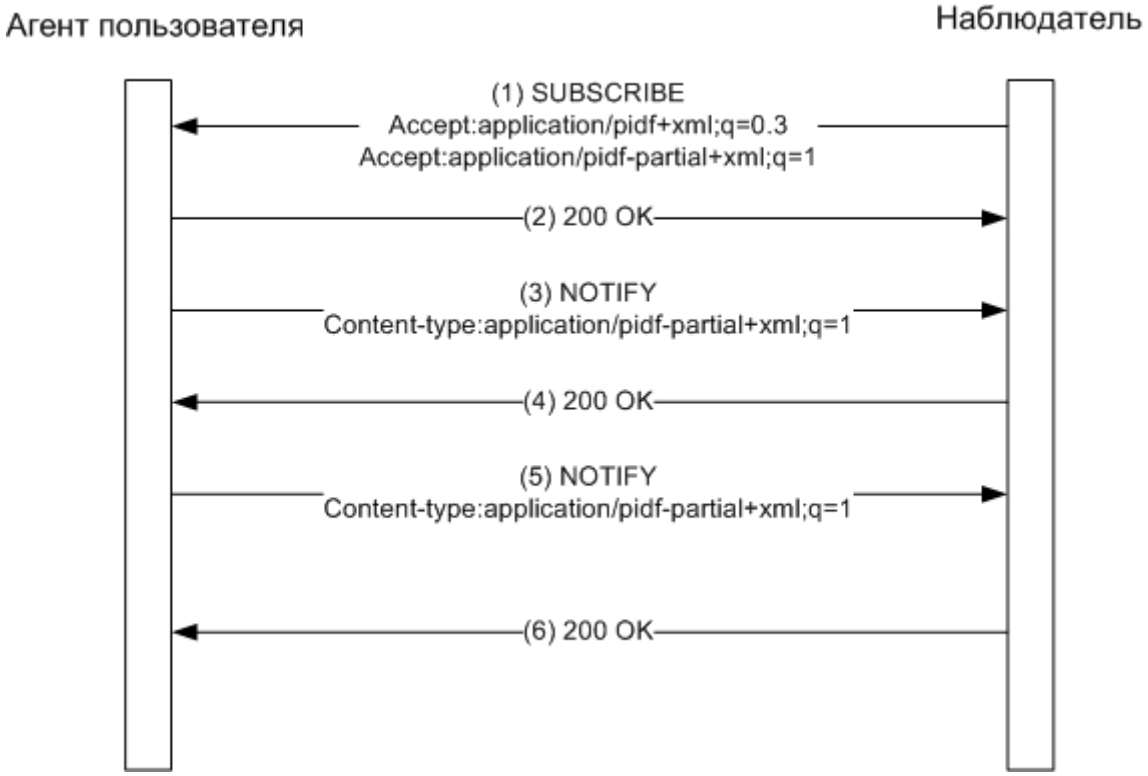

Рис. 6.2

Наблюдатель подписывается на получение информации присутствия об абоненте. Запрос SUBSCRIBE содержит заголовок Accept, в котором указывается, что сервис поддерживает как полный, так и частичный тип PIDF документа. Вес предпочитаемого типа также указан с помощью параметра q. агент присутствия устанавливает подписку и отправляет запрос NOTIFY, содержащий XML документ с полной информацией о пользователе, но закодированный в соответствии с правилами частичного уведомления. Поэтому заголовок Content-type запроса NOTIFY имеет значение application/pidf-partial+xml. Позднее, когда появляется необходимость уведомить наблюдателя об изменении информации присутствия, агент

присутствия посылает запрос NOTIFY, содержащий только изменения по отношению к предыдущему документу присутствия.

6.4 Фильтрация уведомлений.

В процессе работы агент присутствия может доставлять большое количество информации присутствия одному или более наблюдателям. Есть вероятность, что наблюдатели не будут заинтересованы в получении всей информации. Например, наблюдатель может быть заинтересован в том, когда пользователь online или offline, но не интересоваться деталями, такими как на собрании ли он, говорит ли по телефону или обедает. В другом случае, наблюдатель может быть заинтересован только в информации, касающейся обмена сообщениями, но не заинтересован в получении информации о почтовых адресах, номерах телефонов и пр.

Фильтрация уведомлений позволяет наблюдателям устанавливать наборы фильтров, которые будут применяться к поступающим уведомлениям. Данные фильтры могут применяться к информации присутствия XML, расширениям, атрибутам, изменениям между двумя определенными состояниями и др.

Отправляя запрос SUBSCRIBE на получение информации присутствия, наблюдатель может включить в него тело XML, определяющее фильтры, которые должны применяться к данной подписке. Данный документ обрабатывается агентом присутствия и в дальнейшем наблюдатель уведомляется только о событиях, в которых он заинтересован.

ГЛАВА 7. Интеграция услуги контроля присутствия в сеть IMS.

На рис. 7.1 изображен способ реализации услуги контроля присутствия в сети IMS.

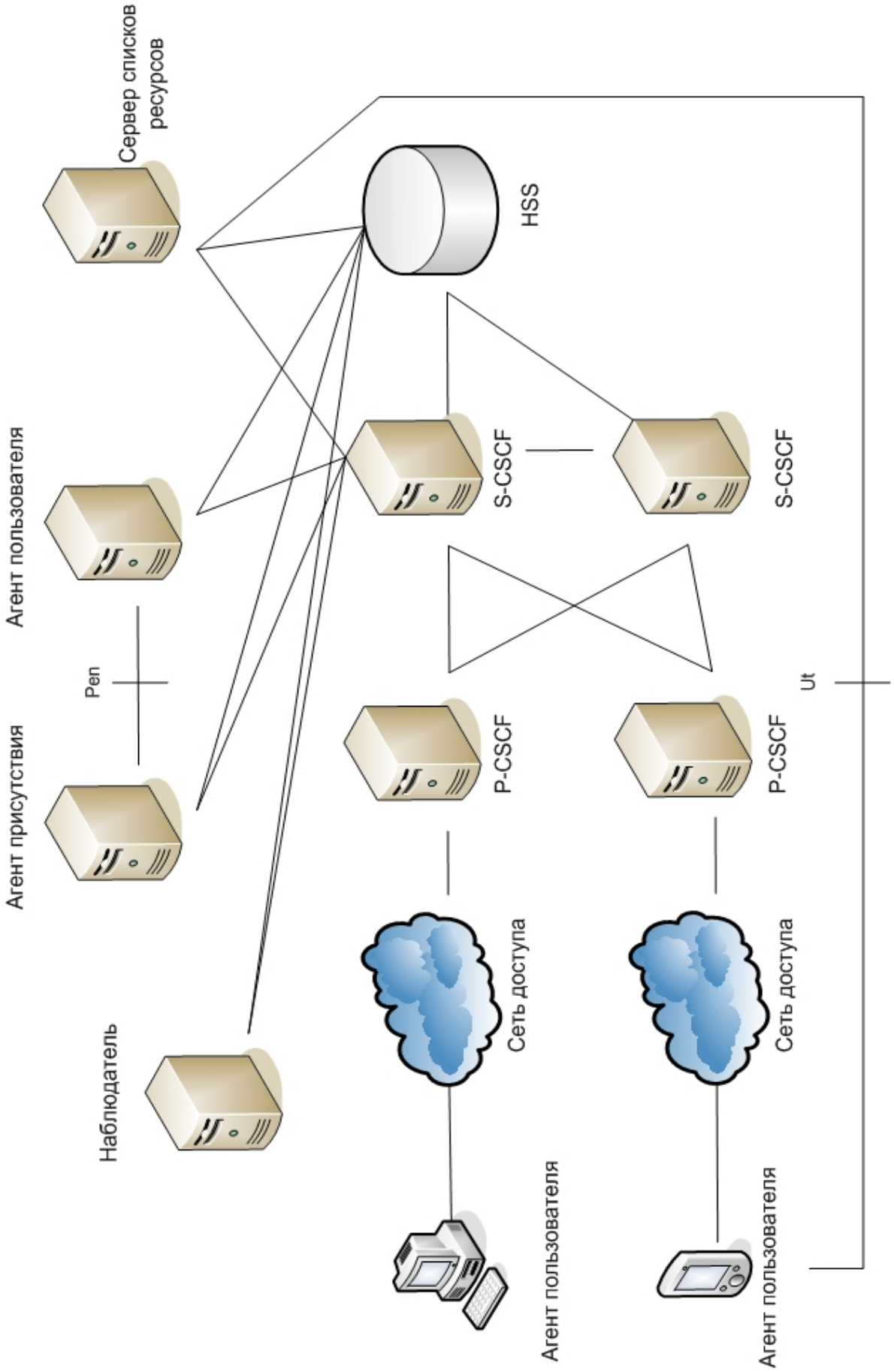
Сервер списков ресурсов
Агент пользователя
Pen
Агент присутствия
Наблюдатель
HSS
S-CSCF
S-CSCF
P-CSCF
P-CSCF
Ut
Сеть доступа
Сеть доступа
Агент пользователя
Агент пользователя

Рис. 7.1

Большинство интерфейсов между элементами сети – это существующие IMS SIP или Diameter интерфейсы, отображаемые на функцию предоставления услуги контроля присутствия.

В сети появляется два новых интерфейса - интерфейс Pen и интерфейс Ut. Интерфейс Pen позволяет серверу приложений, выступающему в роли агента пользователя, публиковать информацию о статусе пользователя в его агенте присутствия.

Еще один новый интерфейс - это Ut интерфейс. Этот интерфейс работает на участке между терминалом абонента и сервером приложений. Данный интерфейс позволяет пользователю конфигурировать услугу контроля присутствия, используя протокол XCAP.

Пользователь может выступать как наблюдатель со своего IMS терминала. В момент запуска приложения услуги контроля присутствия данное приложение подписывается на получение статуса наблюдаемых пользователей, которые включены в список присутствия, хранящийся в сервере списков ресурсов в домашней сети пользователя.

Обмен сообщениями при подписке наблюдателя изображен на рис 7.2

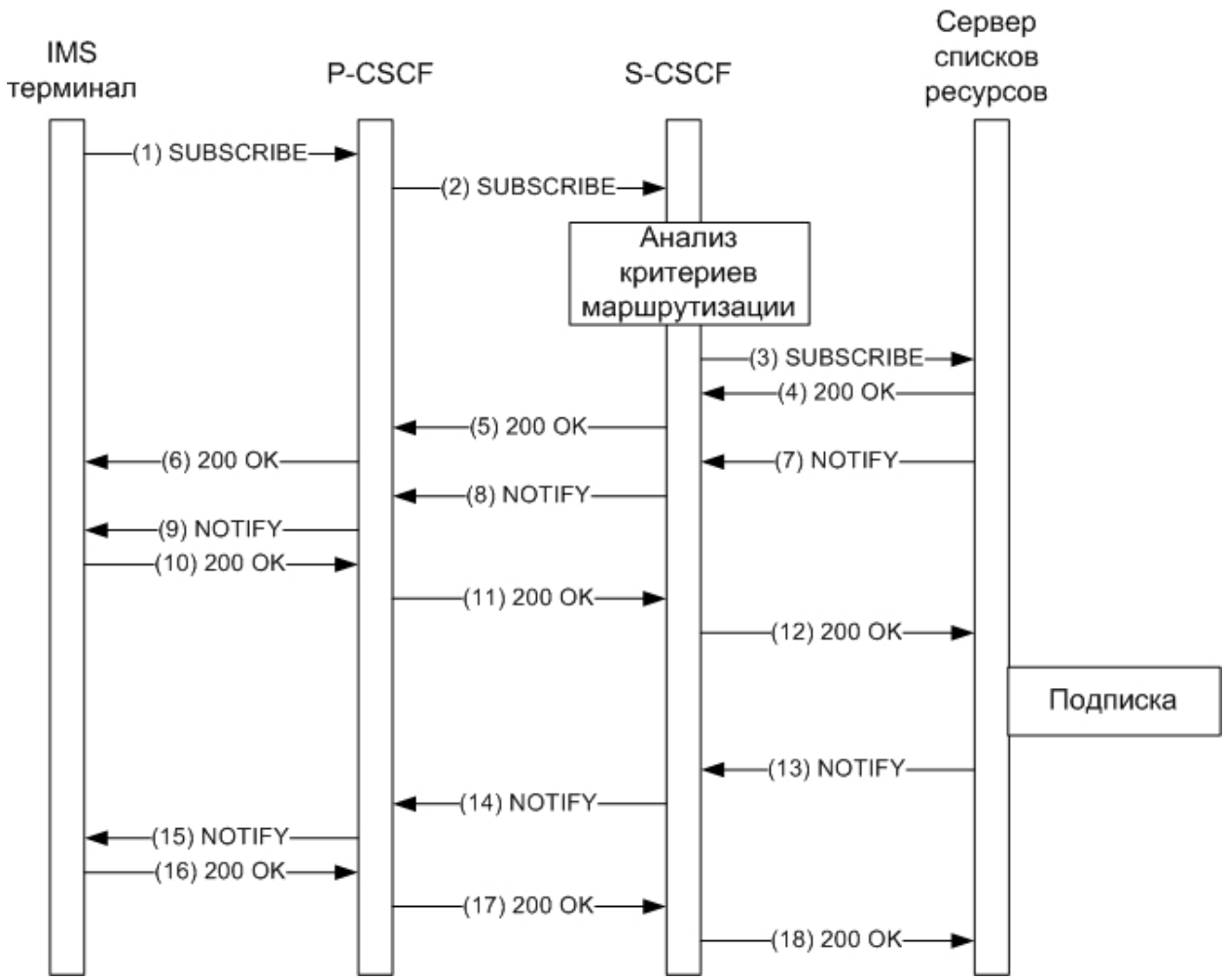

Рис. 7.2

Приложение присутствия, работающее в терминале пользователя, отправляет запрос SUBSCRIBE, адресованный списку наблюдаемых пользователей, например, sip:mylist@home1.net. Запрос SUBSCRIBE содержит поле Event, значение которого выставлено в eventlist, чтобы показать, что подписка адресована списку наблюдаемых пользователей, а не определенному пользователю. Данный запрос поступает на обслуживающую функцию управления сессиями вызовов, которая анализирует начальные критерии фильтрации. Один из таких критериев гласит, что запрос должен быть перенаправлен на сервер приложений, который представляет собой сервер списков ресурсов. После верификации идентификатора пользователя и авторизации подписки сервер отправляет ответ 200(OK). Также сервер списков ресурсов отправляет запрос NOTIFY, содержащий статус подписки.

Затем сервер списков ресурсов по очереди подписывается на получение информации присутствия каждого из пользователей, перечисленных в списке, и, когда достаточное количество информации о присутствии получено от наблюдаемых пользователей, генерирует запрос NOTIFY, содержащий документ с агрегированной информацией присутствия,

На Рис. 7.3 изображен сервер списков ресурсов, подписывающийся на получение информации о пользователе, включенном в список наблюдаемых пользователей.

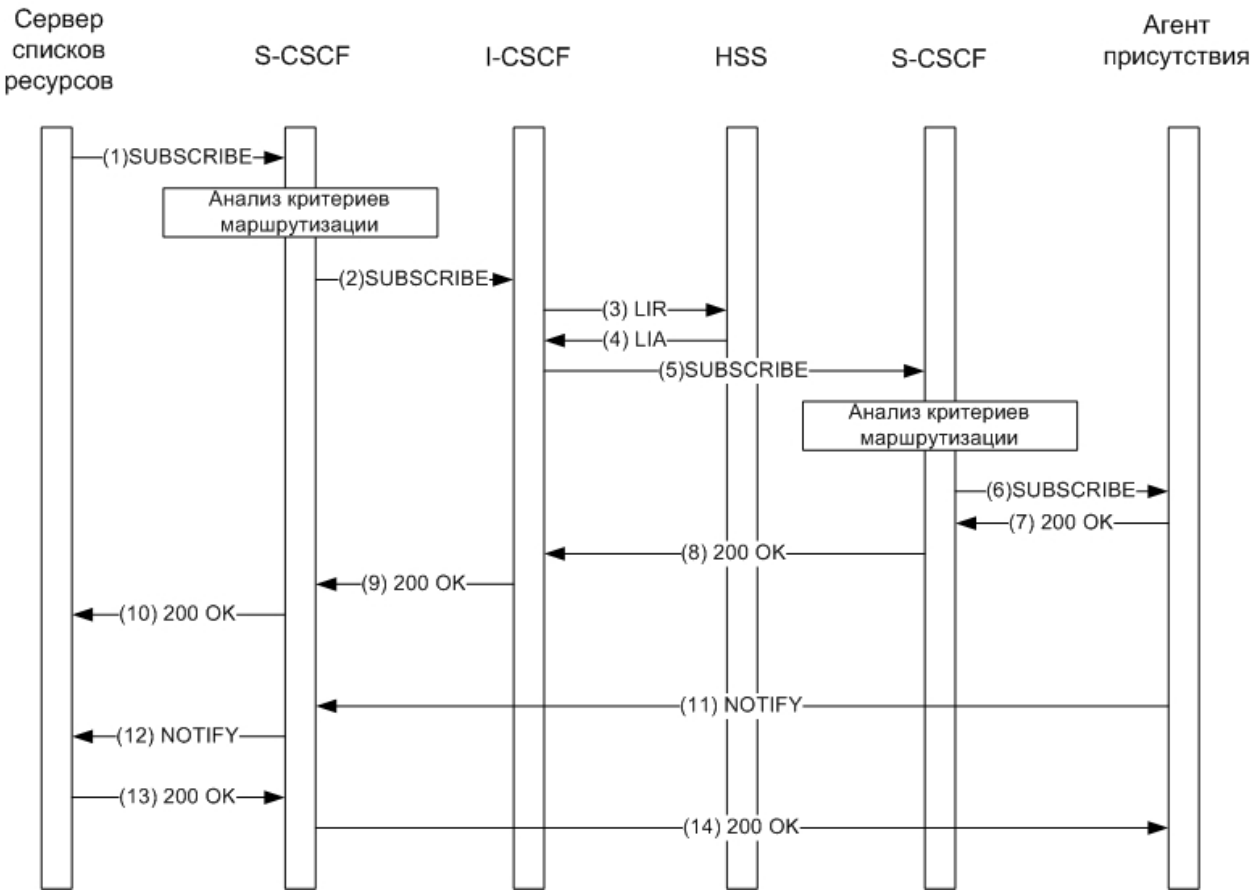

Рис. 7.3

Сервер списков ресурсов отправляет пользователю запрос SUBSCRIBE. Запрос содержит заголовок Event, значение которого выставлено в presence. Данный запрос перенаправляется обслуживающей функцией управления

сессиями вызовов домашней сети сервера списков ресурсов на опрашивающую функцию управления сессиями вызовов сети пользователя из списка. Опрашивающая функция управления сессиями вызовов обращается к HSS по протоколу Diameter для получения адреса обслуживающей функции управления сессиями вызовов, назначенной пользователю, и перенаправляет ей запрос SUBSCRIBE. Обслуживающая функция проверяет начальные критерии фильтрации, среди которых есть правило, указывающее на то, что запрос должен быть перенаправлен на агент присутствия. После получения и авторизации и аутентификации подписки агент присутствия отправляет ответ 200(OK) и запрос NOTIFY, который содержит информацию присутствия пользователя.

Когда приложение услуги контроля присутствия запускается в IMS терминале, агент пользователя подписывается на информацию о наблюдателях для того, чтобы пользователь видел информацию о том, кто наблюдает за его состоянием.

Поле Event запроса SUBSCRIBE имеет значение presence.winfo для уведомления агента присутствия о типе информации, в которой заинтересован пользователь.

Затем приложение услуги контроля присутствия публикует информацию о текущем состоянии пользователя. На Рис. 7.4 изображен поток обмена сообщениями.

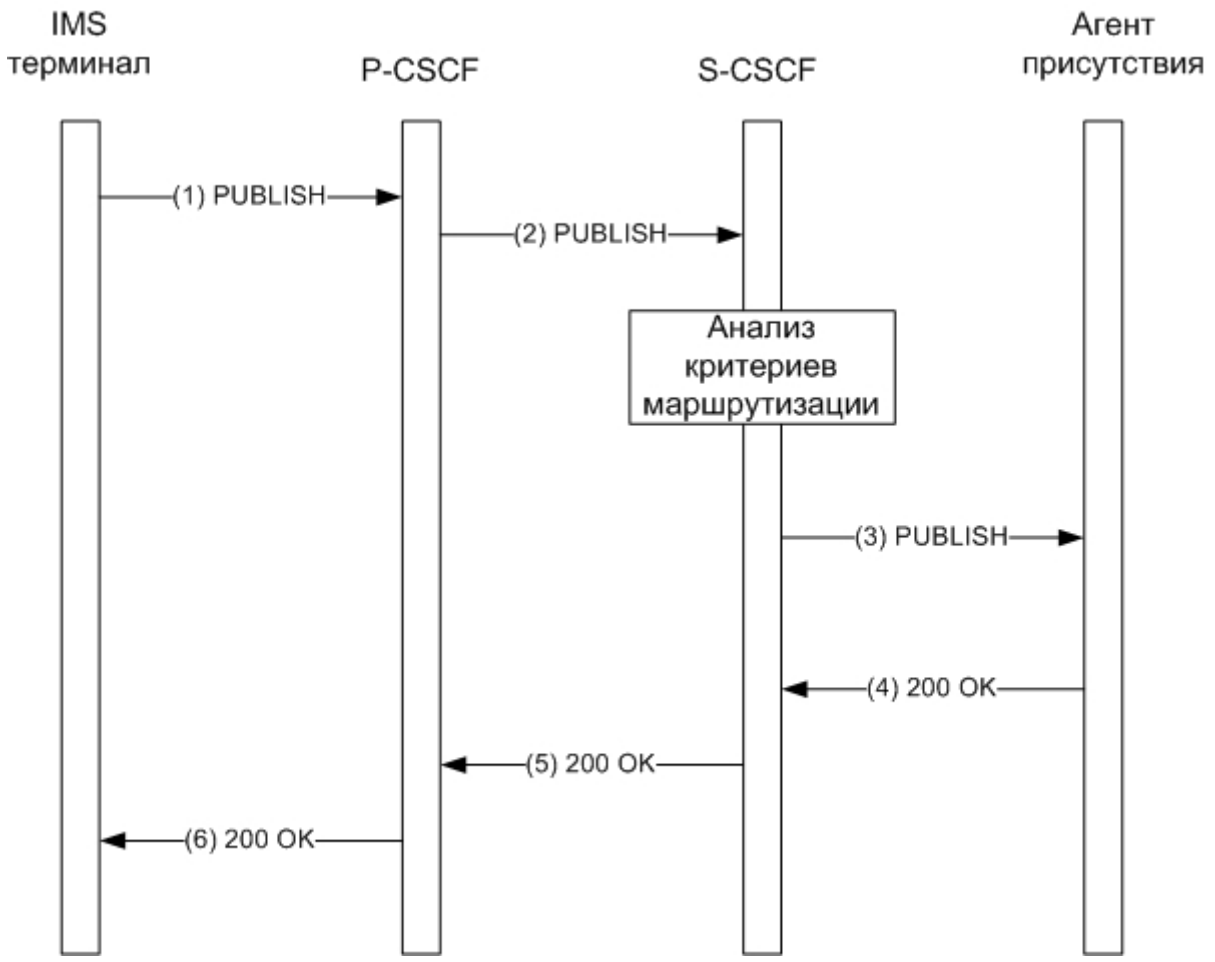

Рис. 7.5

IMS терминал посылает запрос PUBLISH, в котором заголовок Event имеет значение presence. Обслуживающая функция управления сессиями вызовов получает запрос и анализирует начальные критерии фильтрации. Один из этих критериев указывает на то, что запрос PUBLISH с заголовком Event, установленным в presence, должен быть перенаправлен на агента присутствия, в котором хранится информация о данном пользователе. Обслуживающая функция управления сессиями вызовов перенаправляет запрос на агента присутствия, который, в свою очередь, авторизует публикацию информации и отправляет ответ 200(OK).

Кроме агента пользователя, расположенного в IMS терминале пользователя другие агенты пользователя также могут публиковать информацию присутствия об определенном абоненте. Для этого в сети появляется Pen

интерфейс, который не стандартизован и является специфичным интерфейсом оператора.

Как было сказано ранее, 3GPP определил Ut интерфейс для работы на участке между IMS терминалом и сервером приложений. В контексте услуги контроля присутствия, сервером приложения является либо агент пользователя, либо сервер списков ресурсов.

Ut интерфейс предназначен для конфигурирования пользователем списка наблюдаемых пользователей, авторизации наблюдателей, загрузки политики пользователя на агент присутствия и т.д.

Данный интерфейс выполнен на основе HTTP 1.1, поверх которого используется XML Configuration Access Protocol (XCAP).

ГЛАВА 8. Подходы к расчету вероятностно-временных характеристик услуги

Новизна темы обусловила практически полное отсутствие аналитических моделей для расчета вероятностно – временных характеристик данной услуги. Поэтому наметим общий подход к расчету функциональной модели сервера агента присутствия, принцип работы которого изображен на рис. 3.2 главы 3.

На сервер агента присутствия поступают заявки от агентов пользователя. Каждая заявка представляет собой публикацию документа присутствия пользователя, который обрабатывается агентом присутствия в течение некоторого времени. Обработка включает в себя редактирование документа присутствия в соответствии с определенными правилами, а также его рассылку некоторому числу подписанных наблюдателей.

Рассмотрим поток заявок на обслуживание, поступающий на сервер. Ограничим время наблюдения за потоком одним часом, например, часом наибольшей нагрузки. В этот промежуток времени поток вызовов может считаться стационарным. Поток можно считать ординарным, так как в определенный момент времени поступление двух и более заявок является невозможным. Поток вызовов можно считать потоком без последействия, учитывая большое число источников заявок. Таким образом, поток заявок на обслуживание можно считать стационарным пуассоновским потоком, а функцию распределения промежутков времени между заявками - показательной.

Количество наблюдателей, которым рассылается документ присутствия, а также объем этого документа различны для каждой отдельной

заявки, что позволяет считать функцию распределения длительности обслуживания также показательной.

Предположим, что сервер обслуживает поступающие заявки в режиме с потерями, то есть заявки, попадающие на систему в момент полной занятости ресурсов, получают отказ в обслуживании.

Вышеперечисленные предположения позволяют применить для расчета вероятностно-временных характеристик системы математическую модель, классифицируемую как M/M/m:loss – система с m обслуживающими логиками и дисциплиной обслуживания с явными потерями. Основной характеристикой такой системы является доля времени, когда все логики сервера являются занятыми, то есть поступающие заявки получают отказ в обслуживании. Этот параметр может быть рассчитан по B-формуле Эрланга рис. 8.1:

$$p(m) := \frac{\dfrac{\left(\dfrac{\lambda}{\mu}\right)^{m}}{m!}}{\displaystyle\sum_{k=0}^{m} \frac{\left(\dfrac{\lambda}{\mu}\right)^{k}}{k!}}$$

Рис. 8.1

где λ – интенсивность поступления заявок,

μ – интенсивность обслуживания заявок,

m – количество обслуживающих логик.

ЗАКЛЮЧЕНИЕ

Разработанный алгоритм работы услуги контроля присутствия является достаточно подробным для того, чтобы лечь в основу проектирования и создания оборудования для предоставления данной услуги пользователям.

Описанные процедуры обмена сигнальными сообщениями, информационные модели, используемые для передачи информации присутствия, новые функциональные элементы сети IMS, участвующие в работе услуги, дают представление о процессе внедрения услуги в реальную сеть мобильной связи.

Дальнейшая деятельность по созданию приложения услуги контроля присутствия должна быть направлена на детальную проработку алгоритмов работы логик, обслуживающих поступающие запросы пользователей, написание программного кода приложения, в т. ч. реализацию описанных протоколов и информационных моделей.

Выбранная в работе математическая модель позволяет приступить к расчету вероятностно-временных характеристик, необходимых для определения вычислительных мощностей аппаратного обеспечения услуги.

Таким образом, материалы дипломной работы удовлетворяют требованиям задания и могут использоваться в практических целях для разработки услуг добавочной стоимости в сетях, построенных по технологии IP Multimedia Subsystem.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] 3GPP. Network Architecture. TS 23.002, 3rd Generation Partnership Project (3GPP), March 2006.

[2] J. Rosenberg. A Presence Event Package for the Session Initiation Protocol (SIP). RFC 3856, Internet Engineering Task Force, August 2004.

[3] H. Sugano, S. Fujimoto, G. Klyne и др. Presence Information Data Format (PIDF). RFC 3863, Internet Engineering Task Force, August 2004

[4] H. Schulzrinne. RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF). Internet Draft draft-ietf-simple-rpid-07, Internet Engineering Task Force, June 2005.

[5] J. Rosenberg, H. Schulzrinne, P. Kuzivat и др. Indicating User Agent Capabilities in the Session Initiation Protocol (SIP). RFC 3840, Internet Engineering Task Force, August 2004.

[6] A. Niemi. Session Initiation Protocol (SIP) Extension for Event State Publication. RFC 3903, Internet Engineering Task Force, October 2004

[7] A. B. Roach. Session Initiation Protocol (SIP) – Specific Event Notification. RFC 3265, Internet Engineering Task Force, June 2002.

[8] J. Rosenberg. A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP). Internet Engineering Task Force, August 2004

[9] A. Roach, J Rosenberg, B. Campbell. A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists. Internet Draft draft-ietf-simple-event-list-07, Internet Engineering Task Force, January 2005.

[10] J. Rosenberg. The Extensible Markup Language (XML) Configuration Access Protocol (XCAP). Internet Draft draft-ietf-simple-xcap-07, Internet Engineering Task Force, June 2005.

[11] G. Camarillo, Miguel A. Garcia-Martin. The 3G IP Multimedia Subsystem (IMS). Wiley, 2006.

[12] 3GPP. Architectural Requirements. TS 23.221, 3rd Generation Partnership Project (3GPP), June 2004.

[13] J. Rosenberg, H. Schulzrinne, G. Camarillo и др. SIP: Session Initiation Protocol. RFC 3261, Internet Engineering Task Force, June 2002.

[14] M. Handley, V. Jacobson. SDP: Session Description Protocol. RFC 2327, Internet Engineering Task Force, April 1998

[15] Miikka Poikselka, Georg Mayer, Hisham Khartabil и др. The IMS. IP Multimedia Concepts and Services. Second Edition. Wiley, 2006.

[16] А.Б. Гольдштейн, Б.С. Гольдштейн. SOFTSWITCH. BHV-St. Petersburg, 2006.

[17] В.А. Фрейнкман. Эволюция технологий предоставления услуг IN в современных и перспективных сетях связи. «Технологии и средства связи», 2006.

[18] А.Б Гольдштейн, Н.А. Соколов. Подводная часть айсберга по имени NGN (Часть 2). «Технологии и средства связи», 2006

СПИСОК СОКРАЩЕНИЙ

2G	Second generation
2.5G	Second and a half generation
3G	Third generation
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAL	ATM Adaptation Layer
ARPU	Average Revenue Per User
AS	Application server
ATM	Asynchronous Transfer Mode
AUC	Authentication Centre
BCF	Bearer Charging Function
BGCF	Breakout Gateway Control Function
CDMA	Code Division Multiple Access
CDR	Charging Data Record
CS	Circuit switched
CSCF	Call Session Control Function
ETSI	European Telecommunications Standards Institute
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HLR	Home Location Register
HSPDA	High-Speed Downlink Packet Access
HSS	Home Subscriber Server
HTTP	Hypertext Transfer (or Transport) Protocol
I-CSCF	Interrogating CSCF
IETF	Internet Engineering Task Force
IM-SSF	IP Multimedia Service Switching Function
IMEI	International Mobile Equipment Identifier

IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identifier
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
LIA	Location Info Answer
LIR	Location Info Request
MAC	Message Authentication Checksum
MGCF	Media Gateway Control Function
MGW	Media Gateway Function
MIME	Multipurpose Internet Mail Extension
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber Integrated Services Digital Network
MTP	Message Transfer Part
OCS	Online Charging System
OMA	Open Mobile Alliance
OSA	Open Service Architecture
P-CSCF	Proxy CSCF
PA	Presence Agent
PDF	Policy Decision Function
PDP	Policy Decision Point
PIDF	Presence Information Data Format
PoC	Push to talk over the Cellular Service
PS	Packet Switched
QOS	Quality Of Service
RAN	Radio Access Network
RFC	Request For Comments

RPID	Rich Presence Information Data Fofmat
RTP	Real-time Transport Protocol
S-CSCF	Serving CSCF
SA	Security Association
SBLP	Service-Based Local Policy
SCTP	Stream Control Transmission Protocol
SDP	Service Description Protocol
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SGW	Signalling Gateway
SIP	Session Initiation Protocol
SLF	Subscriber Location Function
SS7	Signalling Systen No. 7
TCP	Transmission Control Protocol
THIG	Topology Hiding Inter-Network Gateway
UMTS	Universal Mobile Telecommunication Sytem
UTRAN	UMTS Terrestrial Radio Access Network
URI	Uniform Resource Identifier
URN	Uniform Resource Name
VAS	Value Added Services
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network
XCAP	XML Configuration Access Protocol
XML	Extensible Markup Language