

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№ 7 (205)/2010

Системы управления абонентскими устройствами



СИСТЕМЫ
АВТОМАТИЗАЦИИ

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Редакция:

Дмитриев В.Ю.
viad@jet.msk.su

Некрасова Н.А.
nekrasova@jet.msk.su

Слободчикова Т.А.
slobodchikova@jet.msk.su

Шедова Е.А.
eshedova@jet.msk.su

Верстка:

Кулешова Ю.В.

Корректурa:

Андрюшко О.Ю.

Над номером работали:

Багдасарян Е.Ю.

Думчев В.Г.

Николаев А.Б.

Издатель:

Компания «Инфосистемы Джет»

Контакты:

тел. (495) 411 76 01

<http://www.jetinfo.ru>

От редакции

Давайте представим, что ваша компания провела корпоративный День здоровья. И чего там только не было: спортивные игры, интеллектуальные, азартные, творческие мастерские и т.д. Но во всем этом калейдоскопе оставалось одно централизованное управляющее воздействие — по сути, все ваши активности были организованы «зачинщиками» мероприятия. Т.е. все, что вам нужно было сделать, чтобы прекрасно провести время — это прийти вовремя к обозначенному месту встречи. А дальше все развивалось по заданным схемам и алгоритмам, несмотря на все разнообразие предпочтений участников действия. Вас в прямом смысле подключили к празднику!

Примерно по такой же схеме происходит каждодневная работа СРЕ — абонентских устройств, управление которыми по протоколам широкополосного доступа задано операторами. Об этом и пойдет речь в июльском номере. Тема не просто актуальна, она как нельзя более востребована, поскольку автоматизация процессов управления СРЕ упрощает жизнь не только пользователям, получающим услуги из «коробки», но и операторам, у которых исчезает «головная боль»

при подключении новых абонентов и предоставлении новых услуг уже имеющимся. А уж как быстро растёт клиентская база и набор услуг операторов для нашей с вами насыщенной жизни в сети не стоит даже и подсчитывать. И так понятно — колоссальными темпами! С этим растут и нагрузки на тех.службы оператора, выполняющие рутинные функции подключения, настройки, добавления новых услуг. Нервничает клиент, потому что приходится разбираться в тонкостях, нервничает оператор — не понятно, что происходит у абонента, что он не понимает, чего не договаривает, каких параметров не хватает, капают деньги операционных расходов... А для решения этих проблем всего то нужно — автоматизировать данные процессы, используя протокол, к примеру, CWMP (унификация средств и методов управления СРЕ), описываемый Спецификацией TR-069, и решение производителя, его поддерживающие, скажем, VoiceIP от компании AVSystem Corporation.

Удачных вам подключений!

С уважением, редакция JI

СОДЕРЖАНИЕ

Новости	5
Статистика	7
Тема номера	
Централизованное управление абонентским оборудованием (А. Николаев)	9
TR-069	11
Задача, которую нужно решать	19

NetApp SANscreen 6.0 повышает эффективность виртуализованных ЦОД

Компания NetApp (NASDAQ: NTAP) объявила о выпуске SANscreen® 6.0, новой версии своего популярного средства управления системами хранения данных, позволяющего поставщикам услуг и организациям повысить эффективность и быстродействие систем хранения во всех компонентах виртуализованных инфраструктур.

Технологии эффективного хранения позволяют экономить средства, хотя применяются они не везде, так как заказчики зачастую не в силах численно оценить их эффективность. Система SANscreen 6.0 решает эту проблему, так как обладает уникальной способностью измерять, анализировать и снижать возможности риска, связанные с применением технологий эффективного хранения данных, таких как точное выделение ресурсов и дедупликация в виртуализованных и облачных инфраструктурах. По мере появления в системе новых виртуальных приложений система SANscreen 6.0 расширяется и осуществляет их постоянный мониторинг и анализ, что помогает подразделениям ИТ измерять показатели эффективности, особо важные для готовности и быстродействия приложений. В результате заказчики не только увеличивают эффективность, масштабируемость и экономичность своих систем, но и получают более четкое представление об их работе и необходимости применения технологии эффективного хранения.

Новая версия SANscreen не только развивает возможности управления широкомасштабными разнородными системами, но и управляет средами хранения данных. Это помогает осуществлять интеллектуальное измерение показателей работы виртуальной инфраструктуры и ее управление, а также оптимизировать уровень использования дискового пространства, готовность и быстродействие.

*Подготовлено по материалам
компании NetApp*

VMware выпустила новую версию «облачной» операционной системы VMware vSphere

Компания VMware объявила о выходе новой версии платформы VMware vSphere 4.1 и о расширении пакета решений VMware vCenter для управления виртуальными инфраструктурами. Новая технология по работе с памятью VMware vSphere 4.1 позволяет сохранять высокую производительность системы даже при ее полной загрузке. Таким образом, виртуальные инфраструктуры, созданные на основе vSphere 4.1, будут на 25% эффективнее систем на базе более ранних программных продуктов, утверждают в VMware. Технология сжатия памяти способствует росту степени консолидации, обеспечивая снижение затрат пользователей на приложение — важный критерий полезности внедрения виртуализации. Также в новой версии ОС появилась возможность осуществлять до восьми одновременных перемещений vMotion для одного сервера. Увеличение скорости и гибкости модуля VMware vMotion обеспечивает исключительную реакцию и доступность платформы, подчеркнули в компании.

В то же время, VMware vSphere 4.1 предлагает новые средства управления, которые динамично размещают хранилища и ресурсы сети на виртуальных машинах согласно приоритетам бизнеса. В VMware vSphere технология ввода/вывода для сетей и СХД обеспечивает детальный контроль над тем, как возможности хранилища и сети распределяются между приложениями. Администраторы могут выбрать приоритеты работы виртуальных машин, и в соответствии с этими настройками инфраструктура VMware vSphere 4.1 автоматически распределит ресурсы. Более того, для увеличения производительности и продуктивности платформы в «облачных» средах VMware vSphere 4.1 обеспечивает теперь более тесную интеграцию с решениями партнеров VMware по СХД.

*Подготовлено по материалам
компании VMware*

Системы хранения данных Hitachi AMS 2000 интегрированы с ПО VMware vSphere 4.1

Компания Hitachi Data Systems (HDS), дочернее предприятие Hitachi, объявила об интеграции своих платформ с VMware vSphere 4.1, призванной помочь заказчикам оптимизировать инфраструктуру ИТ и облачных вычислений. Поддержка продуктами семейства Hitachi Adaptable Modular Storage (AMS) 2000 программного обеспечения VMware vSphere 4.1 позволяет осуществлять обработку данных на уровне массивов хранилищ, обеспечивая более высокую плотность виртуальных машин, повышение масштабируемости, ускорение окупаемости инвестиций и лучшую производительность виртуализированных приложений в средах vSphere.

Функции, открывающие новые возможности VMware в привязке к определенным аппарат-

ным платформам, доступны заказчикам систем класса Hitachi AMS 2000 и выше. В целом интеграция систем хранения данных Hitachi с программным обеспечением vSphere 4.1 включает в себя следующие элементы: поддержка блокировок на аппаратном уровне – предлагает альтернативный способ защиты метаданных файловой системы кластера VMFS; полное копирование – позволяет создавать полные копии данных внутри массивов без привлечения ресурсов сервера ESX Server для чтения и записи данных; обнуление блоков – позволяет обнулять неиспользуемые блоки данных на уровне массивов хранилищ, благодаря чему ускоряется развертывание виртуальных машин большого размера.

Подготовлено по материалам компании Hitachi Data Systems

Рынок услуг широкополосного доступа – ни шагу назад!

Актуальная ситуация

Сегодня рынок фиксированного широкополосного доступа¹ (ШПД) в Интернет растет более чем на 70% в год. И это несмотря на то, что с 2008 года появилось большое количество вариантов доступа в Интернет по мобильному устройству. По мнению аналитиков, фиксированный ШПД менее затратный и при этом более надежный и высокоскоростной.

Число абонентов «домашнего» широкополосного доступа в Интернет в декабре 2009 г. достигло 11,3 млн человек по сравнению с 10,990 млн человек в ноябре 2009 г. Об этом говорится в аналитическом отчете Advanced Communications & Media.

В Москве абонентская база ШПД выросла в декабре 2009 г. на 42 тыс или на 1 % до 2,929 млн пользователей. В Санкт-Петербурге прирост составил 20 тыс или + 1 %, а количество пользователей на конец декабря составило 1,049 млн.

По прогнозам экспертов, рынок фиксированного ШПД к 2014 году составит \$4 млрд. Происходит постепенное насыщение рынка: проникновение широкополосного Интернета в городах-миллионниках уже перешагнуло за 70%. До 2014 года проникновение ШПД по всем остальным городам страны будет выравниваться и стремиться

к столичному уровню. Это большой для отрасли темп прироста рынка, в то время как вся экономика растет не более чем на 4-5% в год. Как считают аналитики, рынок мобильного ШПД будет развиваться независимо от рынка фиксированного, но окажет существенное влияние на рынок мобильной голосовой связи: технологии 3G и 4G будут снижать объемы пользования голосовой мобильной связью.

Согласно данным агентства J'son & Partners Consulting, доминирование мобильных игроков на рынке широкополосного доступа станет реальностью в среднесрочной (3-5 лет) перспективе, а углубление процессов консолидации приведет к тому, что мобильные и фиксированные сети будут либо сосуществовать в рамках одной группы компаний, либо (менее вероятно) тесно взаимодействовать в процессе оказания услуг (концепция FMC).

По итогам 2009 года, доля доходов российских операторов «большой тройки» от услуг передачи данных в совокупных доходах по России составила около 5-6% (1,2% – по активным пользователям USB-модемов), в то время как у мировых лидеров этот показатель достигает 40-50%. Данный факт указывает на большой потенциал российского рынка мобильного Интернета, реализованного на базе технологий WCDMA/HSPA.

¹ Широкополосный или высокоскоростной доступ в Интернет – это передача данных по достаточно быстрому каналу, позволяющему, например, транслировать аудио и видео в реальном времени. Для этого требуется «полоса» не менее 128 кбит/с, что является ключевым отличием от коммутируемого (модемного) соединения, теоретическая максимальная скорость которого составляет 57,7 кбит/с.

Тенденции рынка

Доступ в Интернет — общевостребованная услуга, но в перспективе она станет еще более массовой. При этом около 75% пользователей ШПД в результате будут сочетать фиксированный и мобильный доступ, а 25% — использовать только мобильный. За комбинированный доступ потребители будут готовы платить в полтора раза больше.

Рынок находится на пути к новому этапу развития. И поэтому вполне ожидаемы и логичны все те процессы консолидации, которые сейчас происходят в телекоммуникационной отрасли: развитие технологий и перемены в потребительском поведении подталкивают операторов создавать альянсы и заключать партнерские соглашения.

По мнению J'son & Partners Consulting, в более долгосрочной перспективе появление более

«тяжелого» контента (например, телевидение высокой четкости, 3D-телевидение) будет способствовать дальнейшему развитию проводных сетей, которые будут опираться на оптические технологии (PON, FTTx). Однако для удаленных и сельских районов беспроводной доступ (прежде всего, спутниковый) будет оставаться единственно возможным способом выхода в Интернет.

В целом ситуация на российском рынке широкополосного доступа повторяет общемировые тенденции. Количество активных пользователей мобильного ШПД растет существенно быстрее, чем абонентская база фиксированного ШПД. К 2015 году в мире, по прогнозам, будет насчитываться порядка 2 млрд. и 1,74 млрд. пользователей, выходящих в Интернет через мобильные и фиксированные сети соответственно.

Статья подготовлена по материалам:

<http://cybersecurity.ru/telecommunication/97332.html>

<http://www.rg.ru/2010/06/22/telecom.html>

<http://www.bit.prime-tass.ru/news/show.asp?topicid=17&id=72622>

Централизованное управление абонентским оборудованием



Алексей Николаев,
руководитель отдела систем управления
компании «Инфосистемы Джет»

Рынок услуг широкополосного доступа (ШПД) является одним из наиболее быстрорастущих сегментов телекоммуникационного рынка. Полугодовой прирост ШПД в Российской Федерации в 2009 году составил 111%. И если раньше в сетях российских провайдеров насчитывались десятки тысяч абонентов ШПД, то сейчас речь идет о сотнях тысяч. Растет конкуренция, увеличиваются затраты на предоставление услуг.

Помимо борьбы за расширение абонентской базы, не менее важными стали вопросы увеличения выручки на существующей абонентской базе (ARPU) и обеспечения лояльности клиентов. Решение этих вопросов включает в себя реализацию задач:

- обеспечения качественной поддержки;
- продажи и подключения дополнительных услуг;
- обеспечения удобства использования услуг.

Помочь в этом и призвано то решение, о котором мы хотим рассказать в настоящем номере — система управления абонентским оборудованием (СРЕ).

Подобные системы не являются чем-то абсолютно новым, чем-то, что обеспечивает взрывной финансовый эффект. Но отказ от использования подобных систем становится одним из камешков, под лавиной которых может погибнуть бизнес оператора в будущей конкурентной борьбе за абонентов.

Система управления СРЕ поможет организовать качественную поддержку, предоставив службе поддержки инструменты диагностики и управления СРЕ. Она позволит повысить скорость подключения дополнительных услуг, обеспечив их удаленное (инициированное оператором) конфигурирование на универсальных СРЕ. И, наконец, система снимет с абонента заботу о настройке и контроле состояния его оборудования, как при первичном подключении к услугам, так и при их реконфигурации.

Отметим, что современные системы управления «смотрят» чуть дальше и включают в себя функции управления не столь типичным для нашего рынка ШПД оборудованием — сетевыми системами хранения, оборудованием femtocell. В перспективе подобная функциональность поз-

волит оператору предлагать новые комплексные услуги, приближающие эпоху «цифровых домов».

По опыту некоторых производителей подобных систем, окупаемость (в условиях регулярных массовых изменений в конфигурации СРЕ) составляет 5-6 месяцев. В особо серьезных случаях, по опыту компании Sagem Communications (производитель ПО управления СРЕ), использование системы позволяет экономить миллионы евро.

В первой части нашего номера мы определим предметную область, рассказав о рекомендациях по управлению абонентским оборудованием, организациях, иницилирующих и принимающих участие в разработке таких рекомендаций.

Во второй — рассмотрим практическую реализацию этих рекомендаций на примере решения по автоматизации процессов управления СРЕ от компании AVSystem.

TR-069¹

Спецификация TR-069, разрабатываемая некоммерческой организацией Broadband Forum (www.broadband-forum.org), начиная с 2004 года, описывает протокол управления абонентскими устройствами – CPE WAN Management Protocol (CWMP).

Основная цель создания CWMP – унификация средств и методов управления CPE² в сетях провайдеров, независимо от производителей и моделей CPE, централизация функций управления CPE, их передача со стороны абонента на сторону провайдера.

Достижение указанных целей позволило бы обеспечить качество предоставления массовых услуг, оптимизировать расходы на их сопровождение, упростить процедуру доступа к услуге со стороны абонентов.

Протокол CWMP определяет принципы взаимодействия между абонентскими устройствами (CPE) и сервером Auto-Configuration Server (ACS). ACS, согласно TR-069, является сетевым устройством и представляет собой сервер приложений, автоматизирующий реализацию основных методов управления абонентскими устройствами (CPE):

- Автоматическая настройка и динамическое реконфигурирование сервисов (услуг, пре-

доставляемых абонентам оператором, таких как доступ в интернет, VoIP, IPTV).

- Управление программным обеспечением (firmware) CPE.
- Мониторинг состояния и параметров производительности CPE.
- Диагностика.

Место ACS в сети оператора схематично представлено на рисунке 1 (стр.12).

«Южный» интерфейс (southbound) обеспечивает реализацию вышеперечисленных функций управления по отношению к CPE. Первоначально предполагалось управление CPE с использованием технологии DSL. В настоящее время усилиями как самого Broadband Forum, так и других организаций (Home Gateway Initiative, Digital Video Broadcasting), в состав управляемых по TR-069 CPE вошли интегрированные устройства доступа (IAD), PON и связанные с ними оптические устройства, VoIP-устройства, приставки IPTV, другие устройства домашних сетей.

«Северный» (northbound) интерфейс обеспечивает взаимодействие ACS с другими системами OSS/BSS провайдера в рамках реализации единых сквозных процессов управления услугами.

1 Необходимо отметить, что настоящая публикация не заменяет и не подменяет собой спецификацию TR-069, разработанную Broadband Forum и размещенную на сайте организации в Интернет.

2 CPE (от англ. customer premises equipment – оборудование в помещении клиента) – это все телекоммуникационное оборудование, расположенное в помещении клиента, находящееся в его собственности, арендуемое им или взятое в наем и соединенное с публичной или частной сетью через сетевой интерфейс любого вида. К CPE в первую очередь относится голосовое оборудование, включая телефонные устройства, настраиваемое оборудование, PBX (от англ. Private branch exchange – частная система обмена – офисная, учрежденческая автоматическая телефонная станция, УАТС), системы автоматического распределения сигналов (ACD), периферийное оборудование, а также терминальное оборудование, такое как терминалы данных, концентраторы, коммутаторы, маршрутизаторы (роутеры) и мультиплексоры, каждое из которых считается как конкретное CPE в данном контексте.

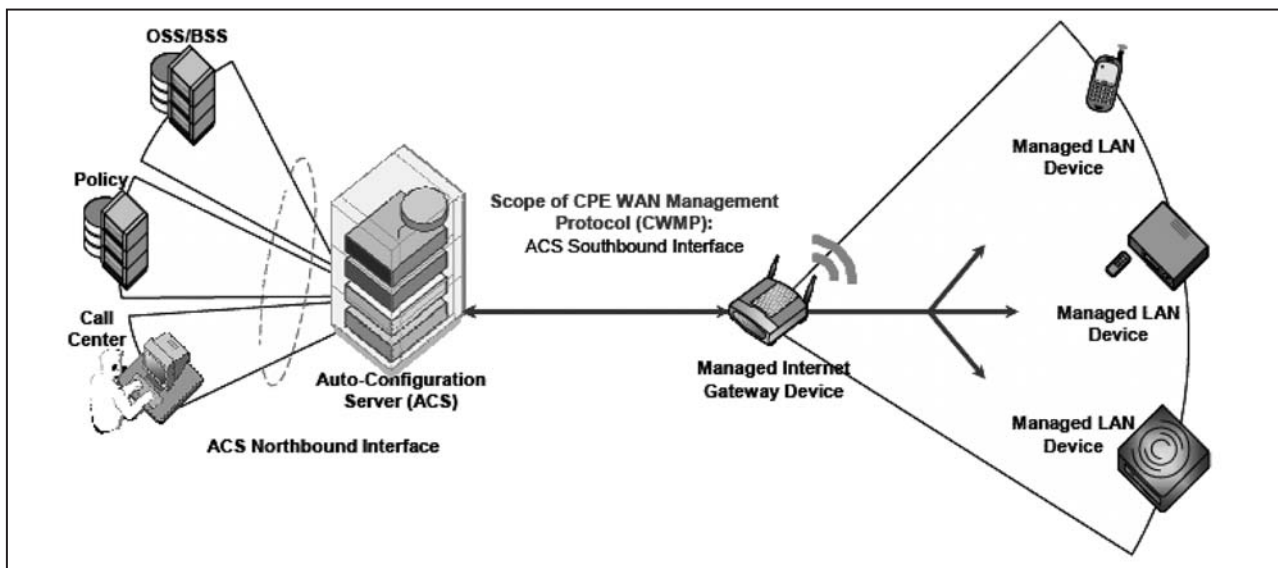


Рис. 1. Схема сети оператора

«Состав» спецификации TR-069

Под формулировкой TR-069 обычно понимают весь комплекс спецификаций, разработанных Broadband Forum в области управления CPE.

Прилагаемая таблица определяет состав указанных спецификаций. Актуальные версии соответствующих документов приведены на сайте www.broadband-forum.org.

Наименование	Наименование документа (актуальная версия)	Краткое описание
TR-046	Auto-Config: Architecture & Framework	Определяет основные принципы автоматизированного конфигурирования оконечных устройств, подключенных по технологии DSL
TR-069	CPE WAN Management Protocol v1.1	Спецификация протокола CWMP
TR-098	Internet Gateway Device Data Model for TR-069	Описывает модель данных CWMP для шлюзов доступа в интернет
TR-104	DSLHome™ Provisioning Parameters for VoIP CPE	Описывает модель данных CWMP для устройств VoIP
TR-106	Data Model Template for TR-069-Enabled Devices	Определяет объектную структуру и требования к модели данных CWMP
TR-111	DSLHome™ Applying TR-069 to Remote Management of Home Networking Devices	Определяет функции управления устройствами локальных сетей, в том числе за NAT
TR-135	Enabling Network Throughput Performance Tests and Statistical Monitoring	Определяет объекты CWMP, обеспечивающие решение задачи мониторинга производительности и контроля доступности CPE
TR-140	TR-069 Data Model for Storage Service Enabled Devices	Описывает модель данных CWMP для устройств хранения
TR-142	Framework for TR-069 enabled PON Devices	Описывает модель данных CWMP для устройств PON и подключенных к ним оптических устройств
TR-143	Enabling Network Throughput Performance Tests and Statistical Monitoring	Определяет объекты CWMP, обеспечивающие решение задачи мониторинга производительности и контроля доступности CPE
TR-157	Component Objects for CWMP	Расширение объектной модели CWMP в соответствии с новыми технологиями и возможностями домашних сетей
TR-181	Device Data Model for TR-069	Определяет единую модель данных для всех устройств, поддерживающих TR-069
TR-196	Femto Access Point Service Data Model	Описывает модель данных CWMP для устройств femto-cell

Функции управления

Ключевая и одна из наиболее востребованных бизнесом функций управления CPE, определяемых TR-069 — автоматическая настройка и динамическое реконфигурирование сервисов. Спецификация определяет возможность как первоначально, так и повторного конфигурирования CPE, например, по запросу абонента или при изменении тех или иных параметров услуги.

TR-069 определяет возможность выполнения операций конфигурирования как по отношению к одному конкретному CPE, так и к группе, объединенных одним или несколькими общими признаками, такими как производитель CPE, модель, версия firmware и т.д.

Поддерживается возможность работы с опциональными наборами параметров услуг (например, с параметрами, определяющими платежи, функции Родительского контроля), включение которых требует относительно более высокого уровня доступа, в том числе с использованием механизма цифровой подписи.

Функция управления программным обеспечением CPE обеспечивает выполнение загрузки ПО на устройство. Протокол определяет механизмы идентификации версий управляемого ПО, инициации (по инициативе ACS или по запросу CPE), выполнения и завершения загрузки файлов образов, логирования и оповещения службы эксплуатации о результативности выполнения загрузки.

Помимо функций непосредственного управления конфигурацией CPE, протокол CWMP определяет методы предоставления доступа к информации, которая может быть использована сервером ACS для мониторинга статуса и производительности CPE. Протокол CWMP также определяет набор механизмов, которые позволяют CPE самостоятельно оповещать ACS об изменениях своего состояния.

Помимо возможностей мониторинга CPE, CWMP предоставляет также механизмы диагностики, в том числе состав параметров, которые могут содержать диагностическую информацию, методы предоставления диагностической информации. Существенным отличием от SNMP-протокола является возможность для ACS (исполняющего роль менеджера) не только запросить диагностическую информацию с CPE, но и получить ее в необходимом объеме от самого CPE (в случае SNMP возможно получение только SNMP- трапа, всю остальную информацию менеджер должен самостоятельно запрашивать у агента).

В дополнение к вышеперечисленным функциям CWMP предоставляет механизмы автомати-

ческой аутентификации и авторизации на веб-сайтах оператора в зависимости от идентификатора и типа используемого для доступа CPE (подробнее соответствующий механизм описан в приложении D к спецификации TR-069).

Архитектура CWMP

Архитектура протокола CWMP включает в себя:

- Стек протоколов CWMP, используемый для организации взаимодействия между ACS и CPE.
- Параметры CWMP.
- Процедуры CWMP.

Стек протоколов

Протокол CWMP реализован как комплекс стандартных и специально разработанных протоколов. Структура стека представлена на рисунке 2:

CPE/ACS Management Application
RPC
SOAP 1.1
HTTP
SSL/TLS
TCP/IP

Параметры CWMP

Параметры CWMP представляют собой модель данных, структура которой определена другим документом Broadband Forum — «TR-106: Data Model Template for TR-069-Enabled Device». Основное назначение параметров — предоставление данных ACS о характеристиках и состоянии CPE, управление их конфигурацией. Параметры могут быть определены как read-only или read-write. Параметры read-only могут использоваться сервером ACS для определения специфических характеристик CPE, текущего состояния CPE или получения накопленной статистики. Параметры read-write позволяют серверу ACS изменять конфигурацию CPE.

CPE/ACS Management Application — приложение, запускаемое на CPE или ACS, реализующее функции CWMP. Приложение не специфицируется CWMP и может представлять собой сервисы, GUI приложения и т.п.

RPC — набор методов RPC, используемых при взаимодействии между ACS и CPE, описанный в спецификации CWMP.

SOAP — все сообщения, передаваемые между ACS и CPE, конвертируются в формат XML. Использование SOAP позволяет обеспечить платформонезависимость решения, уйти от специфики реализации конкретных приложений.

HTTP — выбран в качестве транспортного протокола для запросов SOAP за его распространенность. Предполагается, что в большинстве случаев настройки межсетевых экранов предпо-

лагают пропуск трафика по портам http, соответственно, при внедрении CWMP не потребуются существенного пересмотра корпоративных политик информационной безопасности

SSL/TLS — при передаче данных между CPE и ACS используются соответствующие методы шифрования трафика, обеспечивающие конфиденциальность и целостность передаваемых данных. Используется аутентификация взаимодействующих по протоколу CWMP сторон с использованием сертификатов.

TCP/IP — все сообщения, передаваемые между ACS и CPE, в соответствии с TR-069 должны передаваться с использованием протокола TCP для обеспечения их гарантированной доставки. Использование TCP также определяется необходимостью работы в условиях использования NAT.

В CWMP все параметры объединены в иерархическую структуру. Эта структура данных в CWMP представлена в виде объекта. Каждый объект содержит один параметр или набор параметров. Каждый CPE имеет только один главный объект (root), в зависимости от типа устройства принимающий значение Device или InternetGatewayDevice.

В большинстве случаев, главный объект включает в себя три элемента:

- Common Objects;
- Components;
- Service Objects.

CommonObjects содержит параметры, которые определяют тип CPE. Параметры ветки CommonObject используются для идентификации CPE на ACS и включают в себя:

- DeviceInfo;
- ManagementServer;
- GatewayInfo;
- Time;
- Config;
- UserInterface;
- LAN.

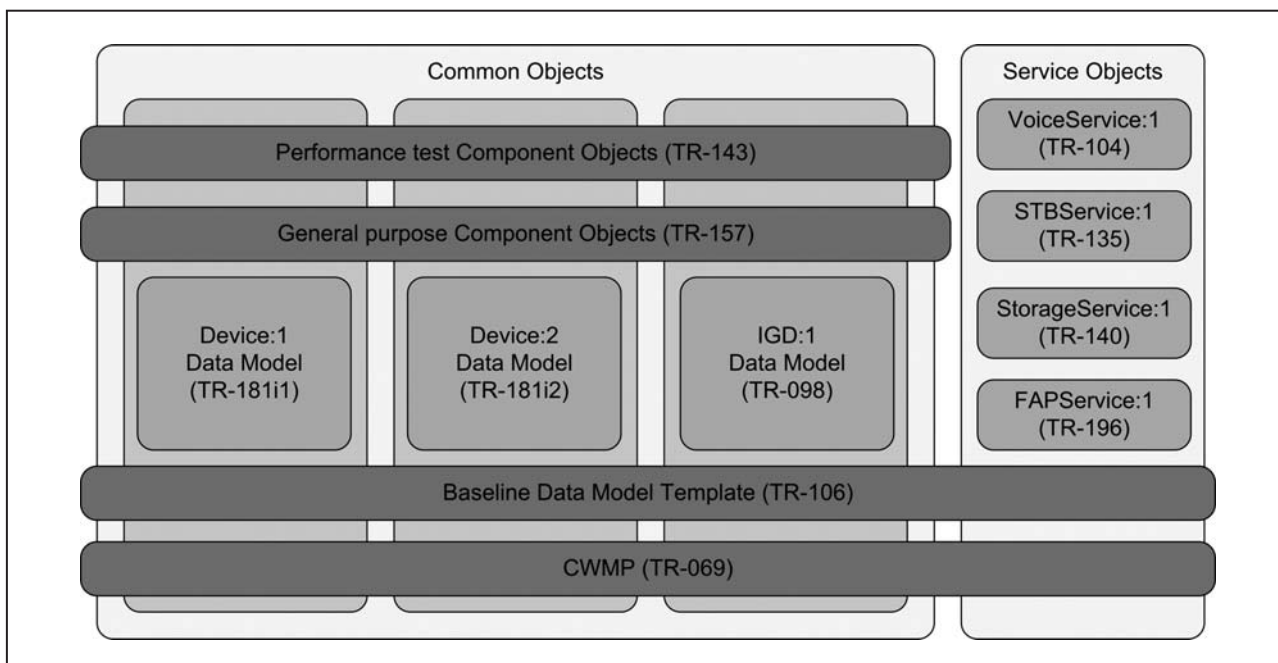


Рис. 3. Схема структуры параметров CWMP

Объект Components содержит параметры, обеспечивающие различные функции TR-069. Их спецификация приведена в отдельных документах BroadBand Forum.

ServiceObjects содержит объекты для каждого типа услуг, обеспечиваемых конкретной моделью CPE. Соответственно, для мультисервисных CPE определяется несколько объектов соответствующего типа. Для основных типов услуг параметры формализованы и оформлены в виде соответствующих рекомендаций BroadBand Forum.

Общая схема структуры параметров CWMP и соответствующих рекомендаций приведена на рисунке 3.

Для упрощения операций массового управления CPE, в соответствии с TR-069, для ACS определяется понятие профиля. Под профилем понимается набор требований, которым должны удовлетворять значения параметров одного или нескольких CPE. Параметры конфигурации сервиса, его подключения или отключения могут быть собраны в единый профиль. Каждый CPE может иметь более одного профиля — в зависимости от количества и типа предоставляемых абоненту сервисов. Обычно для каждого типа CPE

О Broadband Forum

Broadband forum является некоммерческим консорциумом, объединяющим провайдеров, производителей аппаратного и программного обеспечения, работающих на рынке широкополосных услуг. Форум основан в 1994 году как ADSL Forum, затем название было изменено на DSL Forum. В 2008 форум был переименован в Broadband Forum.

В качестве основной задачи форум видит создание спецификаций для широкополосных мультисервисных сетей, направленных на обеспечение совместимости решений различных производителей, оптимизацию архитектуры и управления.

Деятельность форума сконцентрирована в нескольких тематических областях, представленных соответствующими рабочими группами:

- Architecture & Transport
- Broadband Home
- Fiber Access Network
- IP/MPLS & Core
- Metallic Transmission
- Operations & Network Management
- End-to-End Architecture

Разрабатываемые участниками форума спецификации публикуются в виде технических отчетов на сайте форума.

выделяется один базовый профиль, определяющий основные параметры его работы, а также несколько дополнительных, полученных на основе базового и включающих в себя специфические для типов сервисов параметры.

Завершая краткий рассказ о параметрах, необходимо отметить, что CWMP не регулирует число параметров, поддерживаемых конкретной реализацией CPE. Каждый производитель может добавить свои, специфические параметры, наилучшим образом реализующие функции управления конкретным типом и моделью оборудования. Протокол CWMP в свою очередь определяет лишь набор основных параметров, позволяющих реализовать функции унифицированного управления гетерогенной сетью оператора.

Процедуры CWMP

Спецификация TR-069 определяет следующие основные процедуры, выполняемые в процессе управления CPE:

- Автообнаружение CPE;
- Установление соединения и передача информационно-формационных сообщений;
- Передача файлов;
- Завершение соединения.

Как видно из перечня, рекомендациями TR-069 покрываются все аспекты взаимодействия между ACS и CPE в процессе реализации заявленных функций CWMP.

Автообнаружение CPE

Спецификация TR-069 определяет два основных варианта первичного (или повторного — в случае потери связи с действующим ACS) подключения CPE к ACS (обнаружения CPE):

- При первичном локальном конфигурировании (Web GUI, CLI) CPE информация о значениях параметров доступа к ACS может быть непосредственно задана оператором.
- При наличии и возможности использования DHCP, параметры доступа к ACS (ip, код) могут быть переданы на CPE сервером DHCP. В этом случае, в процессе подключения к сети, CPE получит не только собственный динамический IP-адрес, но и адрес (ip), и код доступа на сервер ACS.

В последнем случае, для определения параметров CWMP обычно используется опция 43 протокола DHCP³.

Информация о сервере ACS хранится на CPE в виде значения параметра ...Management-Server.URL (где ... – путь к объекту в соответствии с вышеописанной иерархией). Существующая версия спецификации TR-069 предполагает привязку каждого CPE только к одному ACS. Соответственно, при потере связи с сервером ACS, указанным в качестве значения параметра ...ManagementServer.URL, CPE инициирует повторную операцию поиска ACS.

При этом в случае выполнения плановых операций по переключению CPE на новый ACS возможен также и третий вариант конфигурирования CPE для работы с конкретным ACS – установка соответствующего значения параметра с функционирующего (отключаемого) сервера ACS.

Установление соединения

Как свойственно многим видам двухсторонних коммуникаций, доступны два варианта установления соединения:

- По инициативе CPE.
- По инициативе ACS.

CPE, в соответствии с TR-069, может инициировать сессию взаимодействия с ACS в одном из следующих случаев:

- Первоначальная установка и конфигурирование CPE.
- Включение питания или перезагрузка CPE.
- По расписанию, в соответствии с заданными значениями соответствующих параметров.
- В случае получения от ACS запроса на подключение.
- При изменении адреса ACS.
- При изменении значений ряда ключевых параметров, для которых определена функция отслеживания их значений.
- В случае нештатного завершения предыдущей сессии.

Для ряда случаев, таких как организация сессии в случае изменения значений «наблюдаемых» параметров, спецификация TR-069 определяет требования по реализации механизма защиты ACS, например, за счет установки максимально возможной частоты оповещения об изменениях.

В случае успешного установления соединения с ACS, CPE инициирует запрос INFORM и, в случае успешности его прохождения, завершает процедуру установки сессии.

Открытие сессии по инициативе ACS осуществляется методом отправки соответствующего запроса на требуемый CPE. Для передачи подобных запросов выделен специальный порт – 7547. Запрос формируется в виде HTTP GET к конкретному url CPE. Никакие данные при этом от ACS на CPE не передаются. Полученный запрос анализируется CPE на предмет проверки подлинности и, в случае успешного прохождения проверки, формируется ответ и выполняется инициирование сессии с ACS.

Спецификация TR-069 описывает также различные требования по возможности ограничения факта и интенсивности сессий между CPE и ACS.

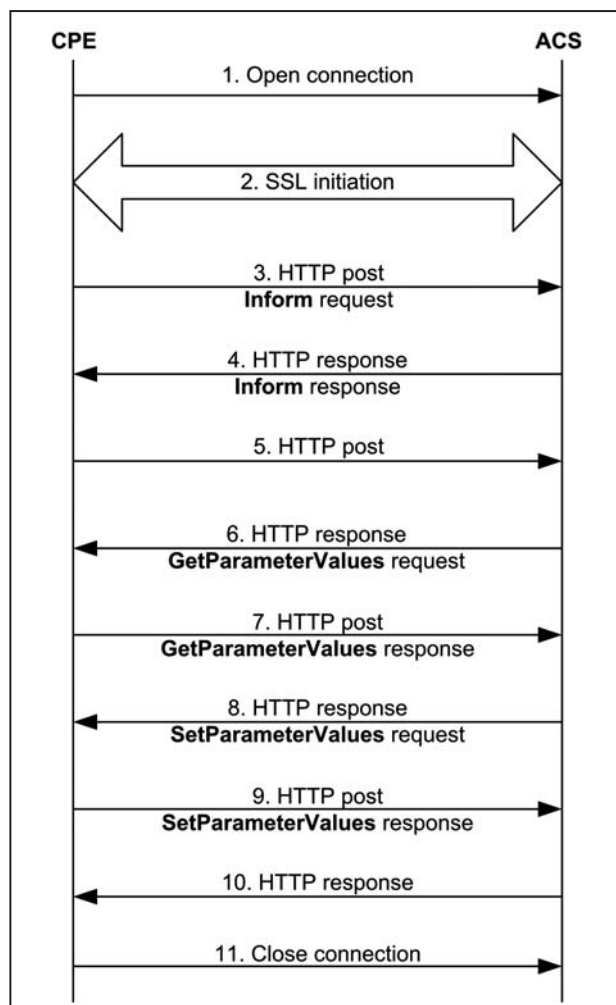


Рис. 4.

³ DHCP (англ. Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) – это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

Передача файлов

Ряд функций управления CPE связан с передачей на них файлов (образов firmware, например). Передача файлов осуществляется с использованием Unicast (HTTP/HTTPS, FTP, SFTP, TFTP) и Multicast (FLUTE, DSM-CC).

В качестве необходимого требования для инициирования процедуры передачи файла спецификация TR-069 определяет наличие активной сессии между ACS и CPE.

Передача файлов может быть организована одним из следующих способов:

- CPE может направить HTTP GET / PUT в рамках уже установленного соединения. После того как файл передан, CPE может перейти к отправке дополнительных сообщений в ACS, продолжая сессию.
- CPE может открыть вторую сессию для передачи файла при сохранении первичной сессии с ACS.
- CPE может прекратить текущую сессию с ACS, а затем инициировать отдельную сессию для передачи файла.

В случае если адрес ACS и адрес источника файла не совпадают, применимы только два последних способа передачи файлов.

Заккрытие соединения

Спецификация TR-069 определяет следующие условия, выполнение которых необходимо для закрытия сессии:

- Последний полученный CPE от ACS запрос пуст.
- CPE не имеет актуальных задач (запросов, ответов) взаимодействия с ACS.
- CPE получил все ответы на запросы от ACS.
- CPE послал все ответы на запросы ACS.

Заккрытие соединения возможно лишь при одновременном выполнении всех вышеперечисленных условий. Подобное решение ориентировано на предупреждение возможности несвоевременного разрыва сессии и потери данных или сбоя сети.

Пример сессии взаимодействия между CPE и ACS приведен на рисунке 4. Комментарии по структуре взаимодействия приведены в прилагаемой таблице 1.

Табл. 1.

	Сообщение	Описание
1	Open connection	CPE иницирует соединение. Протоколы нижнего уровня устанавливают соединение
2	SSL initiation	
3	HTTP post Inform request	CPE начинает каждую новую сессию путем передачи Inform RPC на сервер ACS, содержащего причины установления соединения и список необходимых своих параметров
4	HTTP response Inform response	ACS посылает ответное сообщение Inform посредством Inform RPC. Таким образом, Inform RPC закрывается
5	HTTP post	CPE сообщает серверу ACS, что не имеет других RPC для передачи серверу пустым сообщением. Такое сообщение может быть передано устройством в любое время, пока открыта TCP-сессия
6	HTTP response GetParameterValues request	ACS запрашивает информацию путем передачи GetParameterValues RPC
7	HTTP post GetParameterValues response	CPE передает ответное сообщение GetParameterValues, содержащее запрашиваемую информацию
8	HTTP response SetParameterValues request	ACS может посылать другие необходимые RPC устройству во время данной сессии. В данном случае, SetParameterValues RPC
9	HTTP post SetParameterValues response	
10	HTTP response	В заключение ACS посылает пустое сообщение для оповещения, что у сервера больше нет RPC для CPE
11	Close connection	С закрытием сессии CWMP, протоколы нижнего уровня закрывают свои соединения, и сессия успешно заканчивается

Информационная безопасность

В части обеспечения информационной безопасности разработчики спецификации TR-069 ориентировались на достижение следующих целей:

- Предотвращение фальсификации функций управления CPE или ACS, в том числе в ходе взаимодействий, выполняемых между CPE и АСУ.
- Обеспечение конфиденциальности соединений между CPE и АСУ.
- Предоставление возможности проверки подлинности для каждого типа транзакции.
- Предотвращение несанкционированного использования сервисов.

Для достижения указанных целей рекомендуется использовать уже упомянутые выше протоколы SSL 3.0 и/или TLS 1.0. Альтернативным способом является обычная http-аутентификация с использованием имени и пароля. Использование альтернативного способа не рекомендуется TR-069.

Спецификация определяет необходимость реализации на стороне ACS обоих протоколов — и SSL, и TLS. Это требование определяется необходимостью обеспечивать возможность поддержки наиболее удобного для CPE варианта аутентификации. Механизмы выдачи и отзыва сертификатов спецификацией TR-069 не определяются.

В заключении...

Приведенное выше краткое описание относится к основным положениям протокола CWMP, зафиксированным в спецификации TR-069. Как и любой другой протокол, CWMP имеет свои преимущества и недостатки. Основным его «конкурентом» в области массового управления CPE является протокол SNMP. Соответственно, при рассмотрении достоинств и недостатков CWMP обычно не удается избежать их сравнения. Поэтому в заключение разговора CWMP отметим его сильные и слабые стороны.

Основные преимущества:

- Унифицированное управление сервисами.
- Унифицированное управление по отношению к широкому спектру типов CPE.
- Возможность работы в сетях с использованием NAT.

TR-069 в России

В августе 2009 года по инициативе ФГУП ЛОНИИС создана рабочая группа по тематике систем автоконфигурирования и управления абонентскими устройствами по протоколу TR-069. Сайт рабочей группы — <http://tpark.loniis.org/tr069/>.

Основная цель рабочей группы, согласно Положению о ее создании — разработка и реализация мероприятий, обеспечивающих оптимальное техническое и экономическое внедрение решений по управлению CPE (на базе TR-069) на сетях связи Российской Федерации.

В настоящее время в состав рабочей группы входят представители семи крупнейших операторских компаний России и ближнего зарубежья, а также представители компаний производителей программных и программно-аппаратных средств ACS, таких как Cisco Systems, Alcatel-Lucent, Pirelli Broadband Solutions, Friendly Technologies, AVSystem Corporation и др.

Раздел «Общая информация» сайта рабочей группы содержит ссылки на маркетинговые документы по TR-069 и решениям отдельных производителей.

- Использование XML позволяет относительно легко расширять модель данных.
- Использование TCP в качестве транспортного протокола обеспечивает высокую надежность доставки информации.
- Обеспечивается более высокий, чем в SNMP, уровень информационной безопасности.

Недостатки:

- CWMP является относительно новым протоколом, рынок соответствующих программных средств еще не устоялся, ряд производителей CPE не поддерживает его в качестве протокола управления для своего оборудования.
- CWMP не является стандартом, что позволяет производителям CPE вносить в него собственные усовершенствования, существенно усложняющие достижение цели унифицированного управления CPE в сетях провайдеров.
- Обработка XML является достаточно ресурсоемкой операцией и предъявляет дополнительные требования к ресурсам:
 - к пропускной способности каналов между центром управления и CPE;
 - к производительности самих CPE.

Задача, которую нужно решать

В настоящее время на рынке средств автоматизированного управления СРЕ¹ работает достаточно много производителей ПО. Несложный анализ позволяет сгруппировать все решения в три основные группы:

- Решения компаний-производителей СРЕ.
- Решения независимых производителей.
- Решения на базе ПО с открытым кодом (Open Source Software).

В рамках первой группы представлены средства управления, разрабатываемые производителями СРЕ различного типа. Такие системы отличаются, в первую очередь, прекрасным знанием особенностей «своего» оборудования (моде-

лей СРЕ того же производителя) и, соответственно, обладают различными дополнительными возможностями управления, обеспечиваемыми их нестандартными особенностями. По отношению к СРЕ других производителей возможности управления ранжируются от полной поддержки всех функций управления до полного отсутствия поддержки «чужих» СРЕ.

Вторая группа решений включает в себя программные и программно-аппаратные решения, разрабатываемые независимыми, т.е. не имеющими собственных линеек телекоммуникационного оборудования, компаниями-производителями. Основное отличие подобных решений – полная поддержка рекомендаций TR-069, а также учет

Краткий (далеко не полный) перечень решений компаний-производителей:

Наименование компании-производителя	Наименование решения	Сайт производителя
Alcatel-Lucent	Motive Home Device Manager Motive WiMAX Device Manager	www.alcatel-lucent.com
Cisco Systems	Broadband Access Center	www.cisco.com
Pirelli Broadband Solutions	Pirelli Management Platform	www.pirellibroadband.com
Sagem Communications SAS	Gigaset Software Suite	www.sagemcom.com

¹ Необходимо отметить, что большинство перечисленных в разделе решений решают не только задачи непосредственного управления СРЕ в соответствии со спецификацией TR-069. Обычно поддерживаются и другие функции, ориентированные на облегчение и упрощение подключения и использования услуг для абонентов. Полную информацию о функциональных возможностях предлагаемых решений можно получить, обратившись в компанию-производителя или к ее партнерам.

Краткий перечень независимых производителей решений по управлению CPE:

Наименование компании-производителя	Наименование решения	Ссылка на описание решения
AVSystem Corporation	VoiceIP-ACS	voiceip.pl
Axiros	Axess Device Management Solutions	www.axiros.com
DrayTek	VigorACS	www.draytek.com
Fine Point Technologies	Reach5000	www.finepoint.com
Fiendly Technologies	FriendlyTR69 Solution	www.friendly-tech.com
Works Systems	One Network Management System	www.workssys.com

особенностей (расширяющих TR-069) CPE различных вендоров.

Поскольку TR-069 является открытой спецификацией, естественно ожидать появления решений на базе ПО с открытым кодом. Аналогией в данном случае может являться протокол SNMP, для работы с которым существует множество решений класса Open Source Software, в том числе свободно распространяемых, таких как Nagios, ZenOSS, MRTG и др. В настоящее время существует и развивается проект OpenACS, статус проекта — бета-тестирование. Информацию о OpenACS можно получить на сайте проекта — <http://openacs.sourceforge.net>.

Мы, в качестве примера решения автоматизации управления CPE, выбрали систему управления VoiceIP-ACS, предлагаемую компанией AVSystem Corporation. Мы не готовы выделить этот продукт как наилучший или наиболее универсальный, поскольку у каждого из предлагаемых на рынке решений есть свои достоинства. На его примере мы лишь постараемся проиллюстрировать реализацию протоколов BroadBand Forum и показать те особенности, которыми их дополняют производители ПО.

О компании AVSystem Corporation

Компания AVSystem Corporation основана в 2004 году. Головной офис компании находится в г. Краков, Польша. Область компетенции компании — программные решения собственной разработки для телекоммуникационного рынка. В первые годы своего существования, компания концентрировалась на разработке решений в области IP-телефонии: VoiceIP-PBX, VoiceIP-BX.lite, VoiceIP-CC Contact Center. В 2005 году началась разработка собственного решения по управле-

Система VoiceIP-ACS

Система VoiceIP-ACS представляет собой платформу для централизованного управления CPE. Система обеспечивает возможность управления как CPE, поддерживающими TR-069, так и CPE, без поддержки TR-069. В рамках управления реализуются все функции, определенные спецификацией TR-069. VoiceIP-ACS является масштабируемым, высокопроизводительным решением, обеспечивающим возможность управления (по результатам лабораторного тестирования) более 5 млн. CPE в рамках одной инсталляции.

Ключевые преимущества системы VoiceIP-ACS:

- Возможность виртуализации системы — т.е. возможность использования одной инсталляции несколькими операторами независимо друг от друга.
- Поддержка широкого спектра существующих протоколов управления.
- Высокая доступность и отказоустойчивость решения.
- Гибкий механизм настройки правил конфигурирования CPE.

нию CPE. В настоящее время в портфель решений по управлению CPE входят:

- VoiceIP-ACS, представляющий собой программный Auto-Configuration Server;
- VoiceIP-TR69.stack, представляющий собой комплект библиотек для реализации поддержки TR-069 в CPE различного типа.

Решения компании успешно используются в сетях операторов Европы (Польша, Финляндия, Бельгия) и Новой Зеландии.

- Мощная система определения и контроля прав доступа на любом этапе управления CPE в комплексе с гибкими механизмами журналирования действий пользователей системы.

Архитектура системы

Архитектура приложения

VoiceIP-ACS имеет трехуровневую архитектуру и реализована на базе технологии J2EE. В состав прикладного программного обеспечения системы входят следующие программные модули:

- VoiceIP-ACS Engine.
- VoiceIP-ACS Manager.
- VoiceIP-ACS Adapter.
- VoiceIP-SMG (Subscriber Manager).
- VoiceIP-Reporting.
- VoiceIP-Monitor.

Архитектура системы представлена на рисунке 1.

Для понимания работы решения, кратко рассмотрим входящие в него модули:

VoiceIP-ACS Engine представляет собой основной модуль системы, реализующий функции управления CPE, такие как обнаружение и классификация новых CPE по группам, управление их конфигурацией, управление ПО и мониторинг. Инициация управляющих воздействий осуществляется либо на основе внешней команды (другие модули системы – VoiceIP-ACS Manager, VoiceIP-Monitor, VoiceIP-SMG или внешние системы класса OSS/BSS²), либо в соответствии с предварительно заданным расписанием. Все операции, выполняемые модулем, журналируются.

Модуль содержит описание моделей данных протокола CWMP, включая описание параметров, шаблоны возможных значений. Реализован интерфейс для оперативной, без остановки системы, загрузки новых моделей, как разработанных BroadBand Forum, так и самим оператором. Управление CPE (возможность определения тех или иных услуг, параметров) осуществляется на основе информации о соотнесении CPE с од-

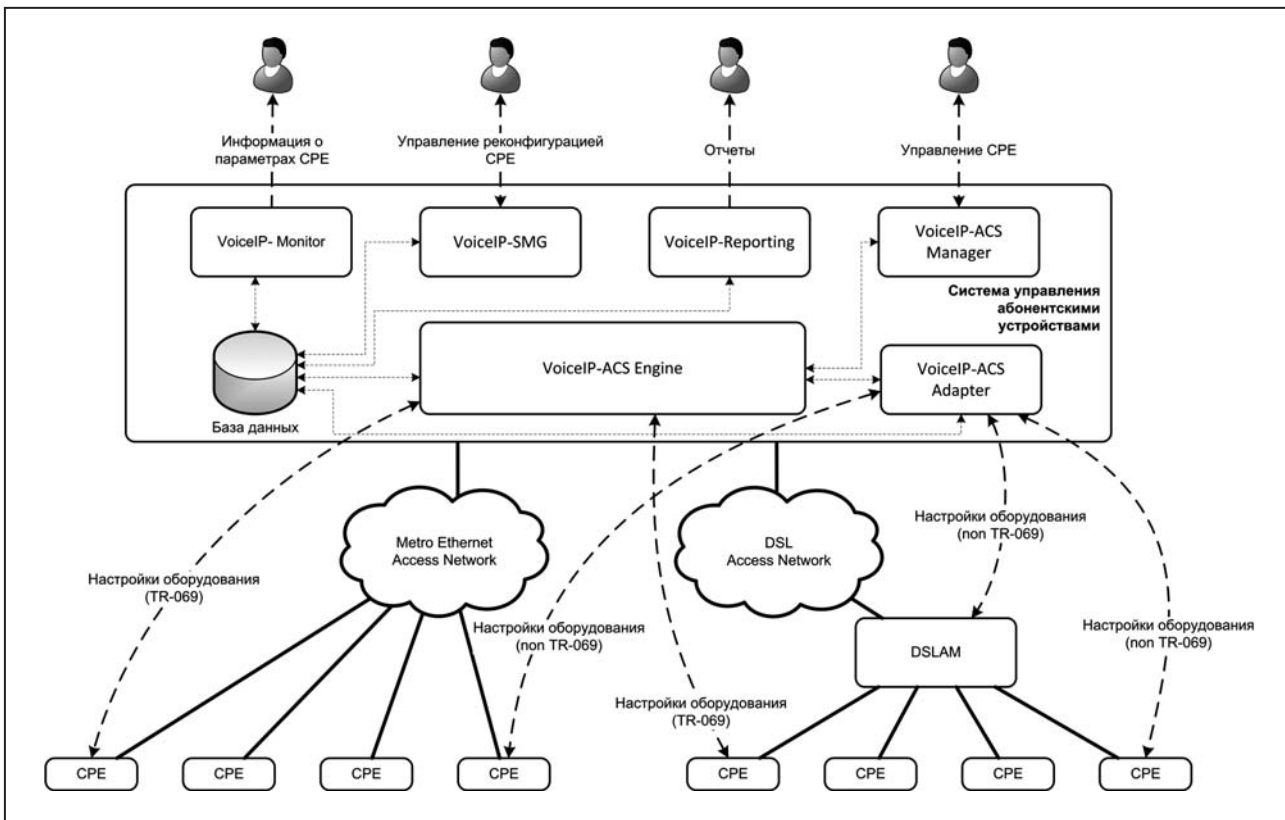


Рис. 1. Архитектура системы VoiceIP-ACS

² OSS/BSS системы (Operations Support Systems/Business Support Systems – системы поддержки операций/системы поддержки бизнеса) предназначены для комплексного управления телекоммуникационными ресурсами предприятия.

ной или несколькими моделями данных по одному или нескольким уникальным признакам CPE (IP, MAC и т.п.).

Управление последовательностью операций при выполнении тех или иных управляющих воздействий осуществляется либо с использованием скриптов VoiceIP-ACS Engine, либо за счет интеграции с модулями управления workflow (VoiceIP-SMG или внешние системы, интегрированные с использованием «северного» интерфейса).

В составе VoiceIP-ACS Engine реализован собственный разборщик XML, обеспечивающий необходимую скорость обмена данными с CPE в процессе выполнения управляющих воздействий. Также модуль VoiceIP-ACS Engine отвечает за аутентификацию и авторизацию пользователей в системе.

VoiceIP-ACS Manager – модуль представляет собой консоль администратора системы, обеспечивающий возможность ее тонкой настройки. Взаимодействие модуля с VoiceIP-ACS Engine осуществляется с использованием RMI³ (в целях безопасности используется SSL/TLS). Авторизация и аутентификация пользователей осуществляются на уровне VoiceIP-ACS Engine.

VoiceIP-ACS.Adapter – дополнительный модуль, позволяющий работать с CPE, не поддерживающими TR-069. Модуль содержит карты соответствия для преобразования CWMP-вызовов в вызовы других протоколов и обратно. Поддерживаются адаптеры к протоколам SNMP, TFTP, SSH, Telnet. Возможна разработка адаптеров к любым

другим частным протоколам. Реализованная схема позволяет полностью изолировать специфику работы с конкретным CPE от самой системы. Все CPE, представленные в сети, отображаются пользователю в качестве CPE с поддержкой TR-069. Преимущества такого подхода особенно хорошо проявляются при наличии планов миграции на CPE, поддерживающие TR-069. Изменения, производимые на системе при осуществлении подобной миграции – минимальны. Схема работы модуля VoiceIP-ACS.Adapter представлена на рисунке 2.

VoiceIP-SMG – модуль Subscriber Manager представляет собой пользовательский интерфейс системы для работников службы технической поддержки и call-centre. SMG представляет собой веб-портал и обеспечивает учет взаимосвязей между абонентами, принадлежащими им CPE и предоставляемыми им услугами. Взаимодействие с другими модулями системы осуществляется с использованием SOAP/RMI и JMS. SMG обеспечивает возможности удаленной реконфигурации CPE, подготовки профилей, обновления ПО CPE, загрузки и отслеживания журнальных файлов CPE. Все действия, выполняемые оператором в интерфейсе SMG, фиксируются в журнальных файлах, используемых в дальнейшем для диагностики проблем и контроля информационной безопасности. Модуль обеспечивает возможность резервного копирования конфигураций CPE. Поддерживается механизм возврата изменяемой конфигурации CPE к предыдущему состоянию, что позволяет оператору при решении проблем в предоставлении услуг вернуться к последней рабочей конфигурации CPE. Или выбрать любую другую конфигурацию из сохраненных.

Портал SMG может использоваться в двух режимах (в том числе одновременно) – в режиме портала технических служб оператора связи и в режиме портала самообслуживания для абонентов.

В режиме портала технических служб, SMG обеспечивает доступ к полному функционалу системы, в том числе:

- Первичная регистрация информации об абонентах, принадлежащих им CPE, соответствующих услугам (также возможна автоматизация регистрации этой информации за счет интеграции с системами класса OSS/BSS, например – CRM).
- Просмотр детальной информации о принадлежащих абоненту CPE, параметрах их конфигурации, текущем состоянии, событиях и т.д.

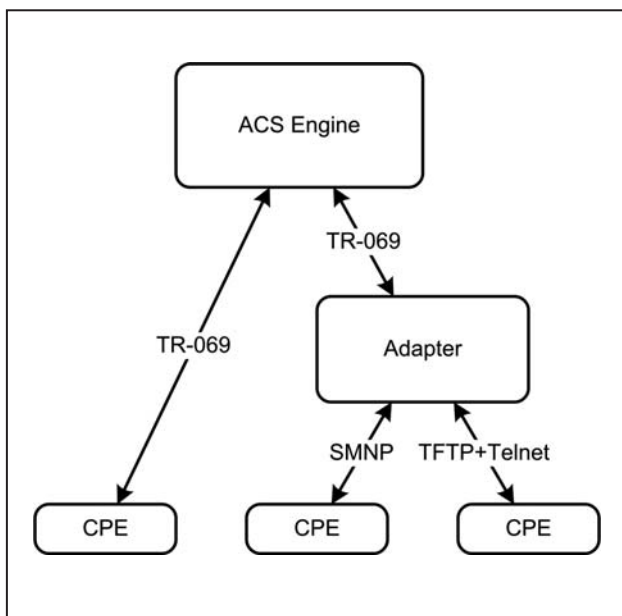


Рис. 2. Схема работы модуля VoiceIP-ACS

3 RMI (англ. Remote Method Invocation) – программный интерфейс вызова удаленных методов в языке Java.

- Выполнение операций по перезагрузке CPE, планированию и инициированию тех или иных задач управления конфигурацией CPE, загрузкой новых версий ПО на CPE.

В режиме портала самообслуживания для абонентов SMG может предоставлять пользователю ограниченный доступ к информации о принадлежащих ему устройствах, возможность конфигурирования тех или иных параметров, например — настройка функций родительского контроля. В принципе, доступ ко всем функциям управления CPE может быть перенесен в интерфейс портала SMG. В зависимости от настройки прав доступа, например, для корпоративных абонентов, пользователям могут быть предоставлены и расширенные функции управления CPE, такие как реконфигурация CPE, резервное копирование и восстановление конфигураций CPE и т.п.

SMG предоставляет возможности гибкой настройки прав доступа для самых разных категорий пользователей, таких как администраторы, сотрудники служб поддержки, абоненты и пр.

Интерфейс портала может быть локализован и адаптирован к имиджу оператора. За счет поддержки интеграционных интерфейсов, а также за счет наличия API, возможна тесная интеграция модуля SMG с существующими у оператора порталами и системами, такими как системы класса OSS/BSS, системы личных кабинетов и т.д.

VoiceIP-Reporting — дополнительный модуль, обеспечивающий возможность генерации отчетов в соответствии с расписанием или по требованию. Модуль построен на базе решения BIRT Project (Business Intelligence and Reporting Tool, <http://eclipse.org/birt/phoenix/>). Система обеспечивает возможность формирования отчетов на основе данных мониторинга, данных о резуль-

Техническая архитектура системы

Для хранения данных системы используется реляционная система управления базами данных. В настоящее время система поддерживает работу с PostgreSQL и Oracle.

В качестве платформы используются серверы под управлением ОС Linux Debian. Система может быть развернута и на других платформах, поддерживающих выполнение Java — Windows, Solaris, Linux и др.

Конфигурация комплекса технических средств определяется требованиями к производительности и отказоустойчивости системы.

Увеличение производительности системы достигается за счет выноса модулей VoiceIP-Reporting и VoiceIP-SMG на отдельные серверы. Отказоустойчивость — за счет дублирования сервера ACS системы и выноса СУБД на отдельный кластер.

Схема подобной конфигурации показана на рисунке 3.

Система поддерживает дублирование основного сервера. При этом оба сервера работают в режиме active-active. Распределение нагрузки между серверами

осуществляется программными или аппаратными балансировщиками нагрузки. Общая информация (журнальные файлы, файлы образов ПО CPE и т.д.) хранится на тех же или отдельных серверах и доступна по NFS. В процессе работы серверы обмениваются между собой контрольными информационными сообщениями (heartbeats). В случае выхода из строя одного сервера обслуживание всех CPE осуществляется вторым сервером. При этом все процессы управления CPE, начатые одним сервером, будут завершены вторым.

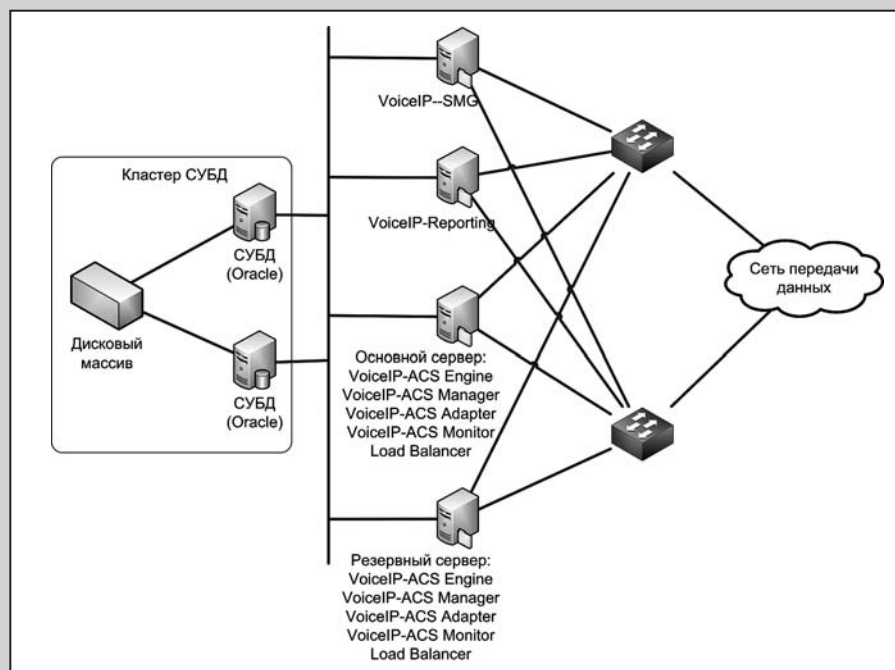


Рис. 3.

татах выполнения задач управления конфигурацией СРЕ. Существуют предустановленные формы отчетов, например, по конфигурации СРЕ, событиям реконфигурации, событиям на СРЕ, отчеты по активным (подключавшимся к ACS) СРЕ за период и т.д. Набор шаблонов отчетов может быть расширен пользователем.

Модуль поддерживает:

- Технологию OLAP, что обеспечивает возможность быстрого формирования сложных статистических отчетов.
- Язык Multidimensional Expressions, как инструмент создания сложных аналитических отчетов.

VoiceIP-Monitor — модуль, отвечающий за сбор в режиме реального времени событий о работе СРЕ. Реализована поддержка не только событий TR-069, но и трапов SNMP, записей syslog. Поддерживается функция автоматической группировки событий по заданным признакам. Возможен мониторинг значений параметров TR-069, контроль их пороговых значений. Информация мониторинга отображается в виде графиков и таблиц с возможностью просмотра исторической информации. Поддерживается возможность настройки оповещений о значимых событиях, в том числе, с использованием шины JMS для интеграции с внешними приложениями.

Как уже указано выше, система VoiceIP-ACS поддерживает взаимодействие с внешними системами. «Северный» (northbound) интерфейс

системы представляет собой API SOAP, RMI и .NET. Интеграция возможна как непосредственно с VoiceIP-ACS Engine, так и с VoiceIP-SMG. Компания-производитель рекомендует использовать API VoiceIP-SMG для интеграции с внешними системами класса OSS/BSS.

Функциональные возможности системы

VoiceIP-ACS обеспечивает автоматизацию всех функций управления, определенных TR-069. Не погружаясь в описание этих функций, остановимся на особенностях данной конкретной системы, позволяющих оптимизировать работу служб эксплуатации и повысить эффективность используемого решения.

Группировка СРЕ

Основным инструментом управления конфигурацией СРЕ и распространением ПО является механизм логической группировки СРЕ по различным признакам. Именно принадлежностью к той или иной группе определяется, какая конфигурация будет загружена на СРЕ. Каждый СРЕ может принадлежать к одной или нескольким группам. Для каждого СРЕ определяется одна домашняя группа. Все группы в системе организованы в иерархическую структуру. По умолчанию в системе определена группа root, являющаяся корнем иерархии и, соответственно, родительской группой для любой другой группы. С каждой группой ассоциированы следующие объекты:

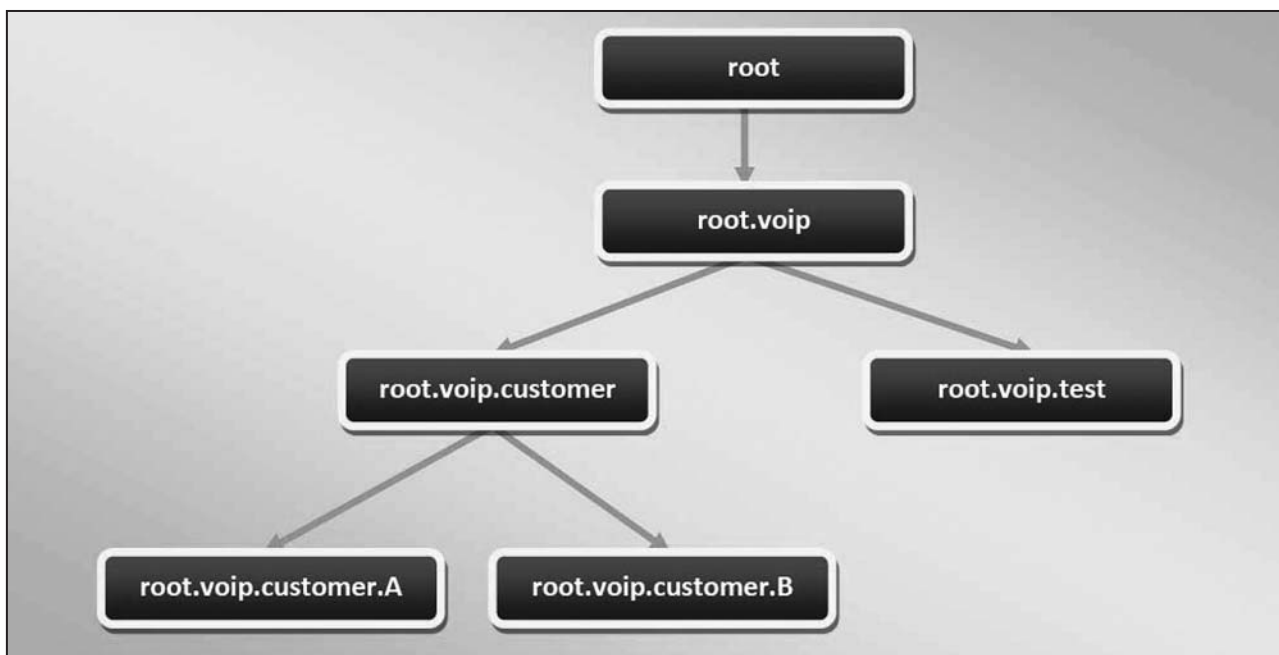


Рис. 4. Пример иерархии групп

- СРЕ — как уже упоминалось, каждый СРЕ должен принадлежать как минимум к одной группе (домашней группе). На любом этапе жизненного цикла СРЕ в системе количество групп, с которыми он будет ассоциирован, может быть увеличено.
- Пользователь — каждый пользователь в системе ассоциирован как минимум с одной группой, являющейся его домашней группой.
- Операции — для каждой группы определяется набор операций, которые должны быть выполнены на СРЕ, принадлежащих к этой группе. Примером таких операций может являться установка тех или иных параметров сервисов, обновление ПО СРЕ до определенной версии и т.д.

Поддерживается механизм наследования свойств (связанных объектов) группы вниз по иерархии.

Пример иерархии групп представлен на рисунке 4.

Представленная иерархия групп ориентирована на настройку на СРЕ сервиса VoIP. Состав групп учитывает различия в значениях параметров VoIP для основной и тестовой конфигурации СРЕ, а также, особенности настройки VoIP для разных абонентов (в примере — абонент А и абонент В). С точки зрения конфигурирования СРЕ логика работы групп выглядит следующим образом:

- Группа `root.voip` определяет параметры сервиса VoIP для всех СРЕ, входящих в эту группу или в одну из дочерних групп.
- Группа `root.voip.test` определяет (как вариант — переопределяет) параметры сервиса VoIP, специфичные для тестовой конфигурации СРЕ.
- Группы `root.voip.customer.A` и `root.voip.customer.B` определяют значения параметров, уникальные для каждого из абонентов с учетом, например, определенного с ним SLA.

Разработчики системы не накладывают никаких ограничений на принципы формирования групп и их количество, возможно, например, формирование групп по следующим критериям:

- Географический признак — группировка СРЕ в зависимости от их физического расположения (Россия, Англия, Москва, Санкт-Петербург, Екатеринбург, Владивосток и т.д.).
- Соответствие абоненту — СРЕ, используемые одним абонентом, могут быть объединены в отдельную группу. Такая группировка

необходима для реализации, например, механизмов самообслуживания.

- Общность конфигурации — СРЕ группируются по возможности использования единых конфигурационных шаблонов. Этот механизм группировки используется наиболее часто, поскольку, в том числе с учетом механизмов наследования групп, обеспечивает основные возможности массового управления конфигурациями СРЕ.

Подобная реализация механизма группировки дает существенный выигрыш с точки зрения упрощения и увеличения скорости конфигурирования СРЕ. При первичном конфигурировании устройства задачей (кстати, автоматизируемой) пользователя системы является лишь корректный выбор нужной группы и уровня иерархии. Целевая конфигурация в этом случае собирается системой автоматически, на основе информации об операциях и параметрах вышестоящих групп.

При появлении новых типов устройств, внедрении новых услуг пользователь системы добавляет лишь новые группы на соответствующем уровне иерархии, не выполняя переопределение всех шаблонов конфигурации.

Указанные особенности существенно облегчают деятельность по управлению конфигурациями, позволяя оптимизировать ее и снизить расходы на эксплуатацию.

Управление конфигурацией СРЕ

Рассказав о механизмах группировки, перейдем к описанию реализации функций управления конфигурацией СРЕ.

В данной конкретной реализации функция управления конфигурацией СРЕ включает в себя функции определения конфигураций СРЕ и функции резервирования конфигураций с возможностью восстановления.

Определение конфигурации СРЕ, точнее — ее формирование и загрузка на устройство, строится на базе механизма группировки. Для каждой группы определяется профайл — набор параметров SWMP и их значений. За счет наличия механизма наследования, профайлы действительны не только для заданной группы, но и для всех дочерних групп. При определении параметров, составляющих профайл, поддерживаются следующие свойства наследования параметров:

- Блокирование — значения параметров, заданных в профайле не могут быть переопределены пользователями дочерних групп.

- Замена — пользователь дочерней группы может переопределить значения соответствующих параметров или сохранить их по умолчанию (т.е. заданные пользователем вышестоящей группы).
- Скрытие — соответствующие значения параметров не наследуются дочерними группами.

Определение целевой конфигурации CPE осуществляется помещением его в соответствующую группу на необходимом уровне иерархии групп.

Система поддерживает два режима распространения конфигурации на CPE — разовые операции (например, по запросу пользователя системы или внешней интегрированной системы), периодические операции по расписанию. Взаимодействие между системой и CPE в процессе определения конфигурации строится в соответствии с TR-069. В процессе распространения конфигурации на CPE система осуществляет сборку конечной конфигурации на основе профайлов всех групп, к которым принадлежит CPE, включая вышестоящие по иерархии. В случае выявления конфликтов осуществляется предупреждение администратора системы.

Резервное копирование конфигураций CPE может осуществляться также, как и их распространение: по запросу пользователя системы (например, перед выполнением каких-либо сложных вариантов реконфигурации) или по расписанию. Поддерживается резервное копирование конфигурации как одного CPE, так и всех CPE, входящих в группу. Конфигурация CPE хранится в виде файла формата .CSV на локальном сервере системы или на внешнем ftp-сервере. Для каждой копии конфигурации указывается версия ПО CPE (firmware), для которой она использовалась. Это позволяет избежать попытки автоматического восстановления конфигурации на новой версии firmware, не поддерживающей те или иные параметры предыдущей версии.

Количество копий конфигураций CPE ограничивается только размером дисковой памяти на сервере, выступающим в роли архива конфигураций. Поддерживается маркировка (например, «последняя рабочая конфигурация») и версияльность конфигураций.

Таким образом, благодаря наличию в данном решении функции резервирования конфигураций (сохранение копий конфигураций CPE) появляется возможность застраховаться от воздействия «человеческого фактора» на работу системы — повышается надежность сети.

Защита данных в системе

Выполняя вышеперечисленные функции управления, система непосредственно влияет на конфигурацию услуг, возможность и качество их предоставления. В связи с этим, важной задачей является обеспечение необходимого уровня информационной безопасности системы, защиты ее данных. Чуть более подробно остановимся на данных вопросах.

Защита данных системы реализована в следующих областях:

- В области защиты информационных потоков между компонентами системы.
- В области защиты системы от несанкционированного доступа пользователей к ее функциям и данным.
- В области защиты системы от подключения неавторизованных CPE.

Все взаимодействие между компонентами системы осуществляется с использованием RMI, работающего через сокеты SSL⁴, что обеспечивает защищенную транспортировку вызовов и данных. При работе через API доступны веб-сервисы, также защищенные SSL.

Доступ пользователей к ресурсам (функции и данные) системы определяется его правами. Информация об учетной записи пользователя хранится в БД системы в зашифрованном виде. Поддерживается интеграция с LDAP.

Права пользователя определяются по отношению к двум типам объектов системы:

- Группы CPE, по отношению к которым он может выполнять какие-либо действия.
- Состав операций, которые может выполнять пользователь в системе — около 100 атомарных операций (в том числе — изменение параметров CWMP), выполнение которых может быть разрешено или запрещено пользователю.

Каждый пользователь имеет одну домашнюю группу, в рамках которой определяются его полномочия, наследуемые для всех подгрупп домашней группы. По отношению к другим группам, не относящимся к домашней, пользователю могут быть назначены не наследуемые права. Например, может быть определен пользователь, имеющий права только на просмотр информации о конфигурации CPE домашней группы и ее подгрупп, но имеющий права на реконфигурацию CPE, входящих в какую-либо другую группу. Для удобства работы с назначением прав пользо-

⁴ Сокеты SSL -(Secure Socket Layer) является проверенным методом шифрования данных, передаваемых через Интернет.

вателям определены соответствующие роли, которые могут быть использованы как базовые типовые наборы прав.

Необходимо отметить, что в системе реализованы два уровня определения прав.

Первый уровень, являющийся основным, реализован в модуле VoiceIP-ACS Engine. Определены следующие типы ролей (в порядке убывания прав): superuser (root), root admin, group admin, group operator, group user.

Второй уровень, расширяющий первый, реализован в модуле VoiceIP-SMG. Определены роли (в порядке убывания прав): root, administrator, operator, subscriber. Пользователь SMG может иметь выделенную учетную запись в VoiceIP-ACS Engine либо несколько пользователей SMG могут работать с ресурсами системы под одной учетной записью VoiceIP-ACS Engine, имея отдельные учетные записи в SMG. Права, определяемые учетной записью VoiceIP-ACS Engine, являются определяющими и приоритетными для соответствующих учетных записей SMG.

Реализованная система назначения прав позволяет организовывать следующие схемы доступа:

- Самообслуживание — пользователю предоставляются права доступа только к принадлежащим ему CPE. При этом права в целом даны только на чтение. Исключение могут составлять только некоторые параметры, доступные для реконфигурации пользователем, такие как настройки DHCP сервера, параметры линии и т.д.
- Использование системы для работы нескольких виртуальных операторов — каждому виртуальному оператору может быть выделена домашняя группа в рамках которой, например, с учетом предоставляемых услуг, оператор имеет полные права на работу с соответствующими CPE и их параметрами. Владелец системы может определить базовые профайлы, параметры которых будут единственными и недоступными для изменения виртуальными операторами.
- Совместное использование системы несколькими операторами — каждый оператор может иметь полные права в рамках своей группы и входящих в нее подгрупп. При этом все другие группы для него недоступны.

Помимо защиты внутренних информационных потоков и разделения прав доступа, система обеспечивает возможность подключения CPE с их предварительной авторизацией. Реализуется подобная возможность одним из двух способов:

- Оператор заранее определяет те или иные уникальные параметры CPE в системе (например, при выдаче CPE в аренду или при продаже в комплекте с услугой). При обнаружении CPE и соответствии его предварительно заданным параметрам, VoiceIP-ACS Engine регистрирует информацию о CPE и соотносит его с одной или несколькими группами для загрузки на него соответствующей конфигурации.
- В случае обнаружения нового CPE, информация о котором предварительно в систему не загружалась, VoiceIP-ACS Engine регистрирует информацию об устройстве и включает его в группу неавторизованных CPE. При этом CPE не получит никакой конфигурационной информации для доступа к тем или иным услугам. По каждому CPE, входящему в эту группу, пользователь системы, наделенный соответствующими правами, должен принять решение о включении в систему или игнорировании. Этот процесс также может быть автоматизирован за счет интеграции с системами класса OSS/BSS.

В итоге, система обеспечивает высокий уровень защиты информации, предоставляя пользователям широкие возможности как ограничения доступа к функциям системы, так и контроля выполняемых пользователями и системой операций.

Сценарии работы системы

Рассказав о функциональных возможностях и особенностях решения, проиллюстрируем его работу на примере типовых сценариев. В этой статье мы подробнее остановимся на том, как же происходит подключение новых CPE, и сценариях активации новых сервисов.

5 Необходимо отметить, что особенностью большинства решений независимых производителей ПО ACS является достаточно гибкий подход к внедрению собственных решений (непосредственно производителем или его партнерами). В ходе таких внедрений решение может быть существенно адаптировано к сценариям подключения CPE, требуемым конкретным операторам — заказчикам системы. Степень возможной адаптации ограничивается лишь гибкостью платформы и финансовыми возможностями заказчика.

Подключение новых CPE

Система поддерживает два основных сценария подключения новых CPE⁵ – с участием абонента («one touch») и без его непосредственного участия («zero touch»). При любом из сценариев возможность использования DHCP при подключении CPE существенно упростит задачу абонента и технической службы оператора, поскольку позволит избежать предварительной установки параметров доступа к ACS на каждом CPE.

В первом случае, купив и установив CPE, абонент должен ввести в портале самообслуживания (SMG или другая система, интегрированная с VoiceIP-ACS) данные, уникальным образом идентифицирующие CPE (OUI – Organizationally Unique Identifier, MAC, Serial Number и т.п.).

Во втором случае, например, в случае аренды CPE абонентом или продажи CPE в комплекте с сервисом, возможен следующий сценарий работы, схематично представленный на рисунке 5.

Этапы сценария:

1. На этапе предоставления абоненту CPE идентифицирующая CPE информация (OUI, MAC, Serial Number) о нем заносится в соответствующую систему (CRM, Order Management и т.п.).
2. SMG получает от внешней системы информацию, идентифицирующую CPE, а также информацию о привязке CPE к учетной записи абонента. На основе полученной информации инициируются подготовительные операции: регистрация информации о CPE в VoiceIP-ACS Engine, осуществляется запрос и получение информации о сервисах, на которые подписан абонент, выполняется подготовка соответствующего конфигурационного профиля (соотнесение с существующими группами в случае, если сервисы являются типовыми).
3. Абонент, получив CPE, включает его в сеть. По DHCP или в соответствии с заранее заданным url CPE подключается к серверу ACS (VoiceIP-ACS Engine).
4. CPE инициирует сессию CWMP, распознается системой VoiceIP-ACS и получает подготовленный конфигурационный профиль.
5. По завершении сессии CWMP VoiceIP-ACS Engine формирует событие, содержащее информацию о результатах активации CPE. Со-

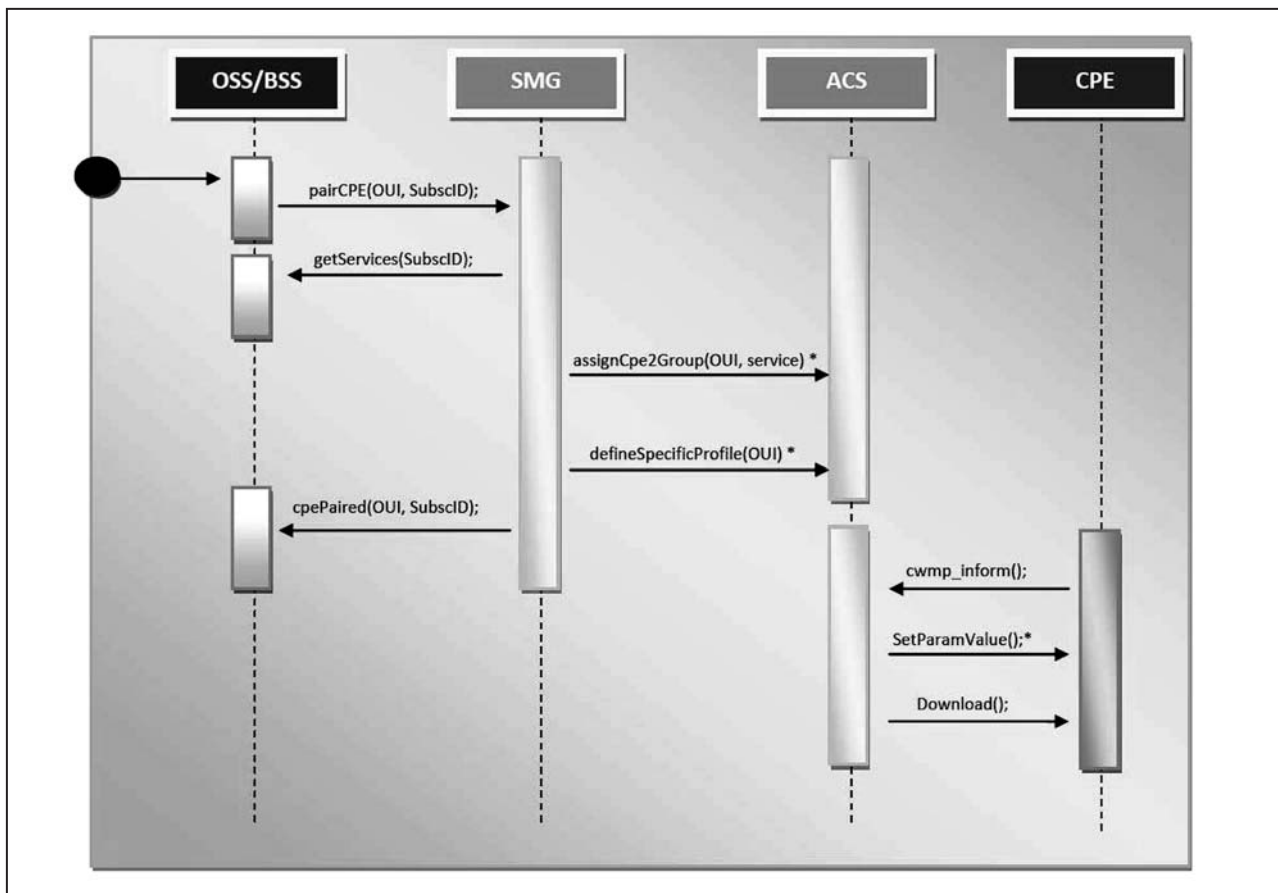


Рис. 5. Сценарий подключения новых CPE

ответствующие оповещения о результатах сессии могут быть получены пользователем системы для оперативной реакции в случае некорректного завершения сессии.

6. После завершения всех операций СРЕ настроен в соответствии с перечнем сервисов, заказанных абонентом, и готов к работе.

Таким образом, все, что требуется абоненту для подключения — купить или арендовать «коробку» у оператора и подключить ее к сети передачи данных. Все остальное система сделает автоматически. Так средства автоматизации позволяют экономить время как абонентов, так и сервисных служб. Они избавляют клиентов от необхо-

димости разбираться в особенностях настройки оборудования и параметров доступа к услугам.

Сценарий активации нового сервиса

Рассмотрим следующую ситуацию — абонент хочет подключиться к новой услуге. Для упрощения ситуации предположим, что у оператора нет системы активации сервисов, а портал самообслужи-

О выборе ACS

При выборе средства автоматизации задачи управления СРЕ по протоколу TR-069 каждый оператор определяет свой набор критериев. Тем не менее, по результатам анализа выполненных внедрений, а также запросов операторов на проработку решения можно сформулировать набор основных критериев, которые необходимо принимать во внимание при выборе системы:

- Совместимость используемых абонентами СРЕ с системой. Оценка соответствия реализованных на СРЕ интерфейсов TR-069 соответствующей спецификации может быть осуществлена с использованием программных средств, предоставляемых обычно производителем прикладного ПО системы. В случае выявления несовместимых (не полностью совместимых) СРЕ, а также в случае наличия СРЕ, не поддерживающих TR-069, необходимо принять во внимание способность системы адаптироваться к используемым СРЕ, степень сложности выполнения подобной адаптации на этапе внедрения и в процессе эксплуатации системы.
- Производительность системы. Необходимо оценивать количество СРЕ, подключаемых к одной инсталляции системы, скорость выполнения операций реконфигурирования и обновления ПО СРЕ. При оценке желательно соблюсти баланс между реальными и перспективными потребностями и возможностями системы, поскольку более производительная система при равной стоимости может оказаться не самой функционально насыщенной.
- Возможность интеграции с внешними системами класса OSS/BSS. ACS является ком-

понентом сквозных процессов конфигурирования услуг для абонентов. Его функционирование невозможно без интеграции с внешними системами. Учитывая изменчивость прикладной архитектуры операторов связи (модернизация существующих, внедрение новых прикладных систем), необходимо принимать во внимание не только готовность команды внедрения выполнить интеграцию на этапе развертывания, но и наличие у системы открытых, документированных интерфейсов.

- Адаптивность пользовательских интерфейсов. Возможность локализации интерфейса, изменения стилистики интерфейса в соответствии со стилистикой оператора. Возможность полностью отказаться от стандартных пользовательских интерфейсов за счет тесной интеграции с другими прикладными системами оператора. Соблюдение подобных условий позволит оператору интегрировать разворачиваемую систему не только на уровне данных, но и на уровне интерфейсов, что существенно повысит эффективность ее использования.
- Стоимость системы, которая складывается из собственно стоимости прикладного программного комплекса и соответствующего аппаратного обеспечения, стоимости работ по внедрению (независимо от того, будет ли осуществляться внедрение собственными силами или приглашенным подрядчиком), стоимости эксплуатации и сопровождения, включая стоимость доработки системы для поддержки новых СРЕ, интеграции с новыми прикладными системами.

вания абонентов реализован на базе входящего в состав решения модуля SMG.

Рассмотрим по какому сценарию происходит динамическое включение нового сервиса на CPE абонента:

1. Абонент формирует запрос на подключение нового сервиса в интерфейсе SMG.
2. SMG размещает запрос на подключение во внешних интегрированных системах (биллинг, управление заказами и т.п.) и ожидает подтверждения возможности включения новой услуги.
3. После получения подтверждения SMG формирует конфигурационный профиль, ассоциируя CPE с одной или несколькими группами.
4. SMG уведомляет VoiceIP-ACS Engine о необходимости отправки вызова типа «ACS connection initiation request» на каждое устройство, подлежащее реконфигурации.
5. CPE инициирует сессию с VoiceIP-ACS Engine.
6. VoiceIP-ACS Engine выполняет загрузку новой конфигурации на CPE.
7. Запрошенный сервис становится доступен абоненту.

Длительность выполнения подобного сценария (без учета специфики интегрируемых систем OSS/BSS, реализации TR-069 на CPE) составляет несколько секунд.

В окружении оператора данный сценарий может выглядеть иначе — например, размещение запроса на новую услугу может выполняться через «Личный кабинет» на портале оператора. В этом случае работа системы начинается с шага 3.

Заключение

В настоящее время, на фоне стремления к сокращению бюджетов, с одной стороны, и усиления конкуренции на рынке широкополосных услуг, с другой, задача автоматизации массового реконфигурирования и управления CPE становится особенно значимой. Благодаря внедрению подобных систем оператор может:

- Обеспечить оптимизацию операционных затрат (ОРЕХ) в условиях роста абонентской базы пользователей услуг.
- Снизить риски невыполнения маркетинговых планов по подключению новых абонентов.
- Обеспечить повышение своей конкурентоспособности на рынке широкополосных услуг фиксированной связи за счет увеличения скорости и качества предоставления услуг.

Практика внедрений подобных систем в Европе и мире показывает возможность их окупаемости уже в первые 6-8 месяцев (для сетей с большим количеством абонентов).

К тому же, не стоит забывать, что клиенты пойдут лишь к тем операторам, с которыми удобно и комфортно работать, поэтому использование средств автоматизации становится не просто технической потребностью, а бизнес-необходимостью.

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю.
Редактор: Слободчикова Т.А.
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
e-mail: JetInfo@jet.msk.su <http://www.jetinfo.ru>

Подписной индекс по каталогу Роспечати

32555

