

Об эволюции телекоммуникационных сервисов на примере GIG

М.А. Шнепс-Шнеппе, Д.Е. Намиот

Аннотация— Рассмотрены трудности перехода от коммутации каналов к коммутации пакетов на примере информационной сети GIG Министерства обороны США -- крупнейшей в мире ведомственной сети. Опыт построения GIG поможет отечественным операторам связи в выборе путей перехода на "All-over-IP". Обсуждаются новые услуги связи, которые создаются на базе слияния коммутации каналов к коммутации пакетов, в том числе в условиях импортозамещения и в интересах ОАО «Ростелеком».

Ключевые слова— коммутация каналов, коммутация пакетов, SS7, интеллектуальная сеть, IP, софтверич, GIG, импортозамещение.

I. ИМПОРТОЗАМЕЩЕНИЕ – МОМЕНТ ИСТИНЫ ДЛЯ «РОСТЕЛЕКОМ»

Перед связистами всего мира стоит одна и та же задача – как перейти от коммутации каналов к коммутации пакетов. Главным, заинтересованным «игроком» на этом поле смены парадигмы телекоммуникаций является индустрия: производители оборудования коммутации пакетов собираются заработать многие миллиарды долларов и платят журналистам многие миллионы за популяризацию новой парадигмы.

Чем характерен текущий момент в российской отрасли связи, в отрасли народного хозяйства, важнейшей как для гражданских, так и специальных нужд [1]:

- 1) Полноценные системные исследования путей модернизации сетей связи не ведутся в России, как минимум, два десятилетия.
- 2) Операторы связи и Поставщики услуг копируют решения, принятые в других странах, без адекватной оценки их положительных и отрицательных сторон.
- 3) Не учитываются приемлемость иностранных решений для различных групп пользователей, прежде всего сетей специального назначения.

На Всероссийской конференции «Взгляд в электронное будущее», прошедшей в октябре 2014 г. в Сочи по инициативе «Ростелекома» и Правительства

России, обсуждался вопрос импортозамещения в области ИТ [2].

«Проектом импортозамещения мы занимаемся уже больше года, понимая, что национальный оператор должен иметь сегмент сети, построенный на национальном оборудовании, и управляемый национальным программным продуктом. Мы приняли решение, что как минимум 30 % оборудования, установленного на наших сетях, в ближайшем будущем должно быть поставлено российскими производителями и управляться российским софтом. Эта цель открывает большие возможности прежде всего для ИТ-компаний», -- заявил президент ОАО «Ростелеком» Сергей Калугин.

«Ростелеком» является партнером множества проектов: государственных инфраструктурных (устранение «цифрового неравенства», ЕГЭ, электронное правительство), отраслевых (медицина и образование, «112», «Безопасный город», КСЭОН) и инновационных (гео-информационные системы, ЖКХ). «Ростелеком» бесспорно является главным действующим лицом во многих ИТ-проектах, но не забудем, что около 90% сетей связи в России построено на импортном телекоммуникационном оборудовании, причем Cisco является основным поставщиком. И в этом таится угроза безопасности сети.

Повлияют ли санкции на бизнес «Ростелекома»? «Коммерсантъ» сообщает [3], что Cisco Systems и Juniper Networks с апреля 2014 г. не могут поставлять продукцию некоторым российским госзаказчикам, которые имеют отношение к оборонно-промышленному комплексу. Так, Juniper остановила поставки оборудования в силовые структуры, например МВД и Минобороны. Бюро по вопросам промышленности и безопасности (BIS) Министерства торговли США, отвечающее за исполнение законов в области экспорта коммерческих товаров, продукции двойного назначения, технологий и софта, с 1 марта 2014 г. приостановило выдачу лицензий на экспорт и реэкспорт в Россию сложного технологического оборудования.

Необходимость импортозамещения – это одна из сторон текущего момента в области телекоммуникаций. Другая, касается сути импортозамещения – на какую же технику направлять усилия: на традиционную коммутацию каналов или на новомодную коммутацию пакетов, которую агрессивно продвигают иностранные производители. Это очень сложный выбор, это своеобразное противостояние поколений, как «отцы и

Статья получена 10 декабря 2014.

Переработанный вариант – 20 декабря 2014

М.А. Шнепс-Шнеппе - профессор, главный научный сотрудник ЦНИИС. (email: sneps@mail.ru).

Д.Е. Намиот. - старший научный сотрудник лаборатории ОИТ, факультета ВМК МГУ имени М.В.Ломоносова. (email: dnamiot@gmail.com)

дети». Международные санкции стали, можно сказать, поворотным моментом в российской экономике новейшего времени, тем более для средств связи, которые, как правило, имеют двойное применение.

Цель настоящей статьи – изучить противоборство двух поколений техники связи: коммутации каналов и коммутации пакетов. Для этого воспользуемся новейшими методическими материалами по построению Глобальной информационной сети Пентагона – GIG (Global Information Grid) [4,5,6]. Сеть GIG представляет собой крупнейшую в мире ведомственную сеть, и разбор трудностей, которые выявляются при переходе от коммутации каналов к коммутации пакетов, на наш взгляд, может быть весьма поучительным.

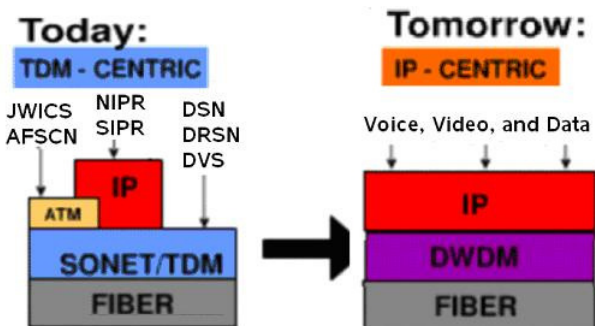


Рис. 1. Иллюстрация текущей проблемы GIG: как перейти от TDM сети к IP сети.

Рисунок 1 иллюстрирует главную проблему, которая стоит перед архитекторами сети GIG. Сегодня основу GIG составляет коммутация каналов, точнее, стандарт SONET (в Европе соответствующий стандарт SDH), по которому работают оптические кабели, а информация кодируется согласно телефонному стандарту TDM (Time Division Multiplexing). По этой сети коммутации каналов сегодня работают основные военные сети связи Пентагона:

- 1) телефонная сеть DSN (Defense Switched Network),
- 2) закрытая коммутируемая сеть DRSN (Defense Red Switched Network),

- 3) сеть видеоконференсвязи DVS (DISN VIDEO).

Кроме того, на рис. 1 указаны четыре закрытые сети JWICS, AFSCN, NIPRNet и SIPRNet, которые используют выделенные магистральные каналы:

- Объединённая глобальная сеть разведывательных коммуникаций (Joint Worldwide Intelligence Communications System, JWICS) — для передачи секретной информации по протоколам TCP/IP.
- Сеть управления спутниками AFSCN (Air Force Satellite Control Network),
- NIPRNet (Non-classified Internet Protocol Router Network) — сеть, используемая для обмена несекретной, но важной служебной информацией между «внутренними» пользователями,
- SIPRNet (Secret Internet Protocol Router Network) — система взаимосвязанных компьютерных сетей, используемых МО для передачи секретной информации по протоколам TCP/IP.

Первые две сети (JWICS и AFSCN) построены на базе

коммутаторов ATM (техника ATM в настоящее время больше не производится). Все эти сети (и другие, непоказанные на рисунке) следует перевести на IP технологию (рис. 1 справа).

Такая же задача стоит перед ОАО «Ростелеком» - как осуществить стратегию „All-over-IP”. Начнем статью с изложения краткой истории развития российских сетей связи (раздел 2). Далее обсудим особенности современной сети GIG (раздел 3), средства перехода на IP технологию (раздел 4) и новые услуги GIG (раздел 5). Раздел 6 посвящен задачам «Ростелекома».

II. СИГНАЛИЗАЦИЯ ОКС-7 И ИНТЕЛЛЕКТУАЛЬНЫЕ СЕТИ: РОССИЙСКИЙ ОПЫТ

Из истории разработки АТС. Рассмотрим развитие отечественных сетей связи с точки зрения технологий. Каковы основные достижения российских связистов постсоветского периода? На ум, прежде всего, конечно, приходят мобильная связь и Интернет. Но следовало бы назвать систему телефонной сигнализации ОКС-7 (SS7), которая является связующим звеном интеллектуальной сети (IN). Ныне много говорят о переносимости телефонного номера и обслуживании экстренных вызовов. Это всего лишь две услуги интеллектуальной сети. Но так как в России интеллектуальная сеть осталась недостроенной, то сейчас для внедрения этих двух услуг приходится городить специальные сети.

Разработка советской системы ОКС-7 началась в 1970х с созданием квазиэлектронных междугородных АТС. В квазиэлектронных АТС коммутация осуществляется герконами, а управление – электронное. В качестве прототипа для КЭАМТС «Кварц» использовалась станция 1ЕСС, разработанная в Bell Labs; первый экземпляр 1ЕСС был установлен в 1965 г. В разработке КЭАМТС «Кварц» принимали участие многие коллективы, в том числе:

- координацию работ и разработку прикладного ПО осуществлял ЦНИИС (Москва),
- операционную систему центрального процессора делал Институт кибернетики АН Украины (Киев),
- сам центральный процессор производил завод Роботрон (Дрезден, ГДР),
- периферийный процессор разрабатывал ЛОНИИС (Ленинград),
- коммутационное оборудование производилось на заводе ВЭФ (Рига, Латвия).

КЭАМТС «Кварц» успешно производилась и эксплуатировалась до распада СССР.

С начала 1980х разрабатывались следующее поколение телефонных станций - электронные АТС. Это был проект ЕС СКТ (Единая Система Средств Коммутационной Техники), о нем сейчас мало кто помнит. Этот проект был аналогом ЕС ЭВМ – другого, хорошо известного проекта, целью которого было копировать IBM 360. Система телефонных станций ЕС СКТ разрабатывалась с широкой кооперацией между странами-членами стран СЭВ. Координирующей организацией выступал НИИ ВЭФ (Рига). В качестве прототипа была выбрана система телефонных станций

System 12 компании IT&T. Следует признать, что выбор прототипа был неудачен, хотя, по замыслу, System 12 обладала многими положительными свойствами. Первая АТС System 12 была установлена в 1982 в Бельгии. Но полноценное серийное производство не удалось наладить, и в преддверии банкротства в 1986 компания IT&T продала всю разработку System 12 (включая заводы) франко-голландской компании Alcatel Alsthom, наследницей которой сегодня является Alcatel-Lucent. Было несколько причин, почему провалился проект IT&T, в том числе: высокая интеграция микросхем (опережающая уровень развития микроэлектроники того времени), недоработки программного обеспечения. Естественно, что даже широкая кооперация не могла спасти самый сложный проект ЕССКТ, хотя бы потому, что в социалистическом лагере отставала микроэлектронная промышленность, и проект ЕССКТ перестал существовать с распадом СССР и СЭВ.

Как проходило внедрение ОКС-7 в России. Обратимся к статье Н. С. Мардера и А. С. Аджемова от 1997 г. [7]:

«В настоящее время заканчивается реализация схемы опытной зоны внедрения. В рамках этой зоны по ОКС № 7 взаимодействует между собой следующее коммутационное оборудование: EWSD фирм Siemens и Iskratel, Alcatel 1000 S12 фирмы Alcatel Telecom, AXE-10 фирм Ericsson и Ericsson-Nikola Tesla, 5ESS фирмы Lucent Technologies, ODEX-100 фирмы Hanwha, Linea UT фирмы Italtel и др.»

Эти станции были использованы в качестве междугородных станций АМТС и узлов автоматической коммутации УАК на междугородной сети России. Согласно структуре междугородной сети России каждая АМТС страны включена в два УАК и общается по протоколу ОКС № 7 [8].

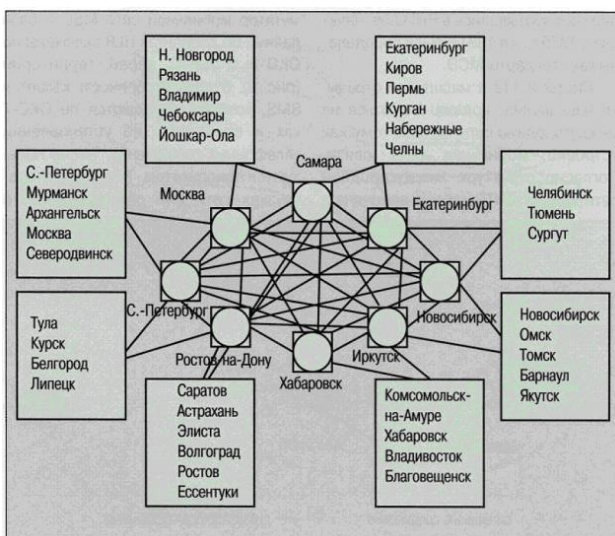


Рис. 2. Структура междугородной сети ОКС № 7.

На территории России размещены восемь УАК, имеющие важное стратегическое значение (рис. 2).

Заметим, что все они построены на базе цифровых АТС типа AXE шведской фирмы Ericsson¹.

При построении сети АМТС требовалось обеспечить их взаимодействие по протоколу ОКС-7, что было нелегко, так как сама реализация протокола SS7 на станциях разных производителей в деталях различалась. Тем более различались системы управления сетью SS7.

Оказывается, что уже изначально сеть ОКС № 7 не планировалась на охват всех АТС страны, так как для нумерации пунктов сигнализации ОКС № 7 выбраны 14-битные номера (т.е. $2^{14} = 16384$). В США же для сети SS7 выбраны 24-битные номера. Как замечает Н.С. Мардер [9], «требуется разработка нового плана нумерации национальной сети сигнализации ОКС-7».

На интеллектуальной сети России были установлены АТС разных производителей: EWSD фирмы Siemens (в Москве), Alcatel S12 фирмы Alcatel (в Перми), платформы китайской фирмы Huawei, отечественные платформы компаний Светец, Протей, Беркут и другие. Требовалось, чтобы все они работали по единому протоколу INAP-R. Это требование для отечественных производителей было чрезмерным, так как для этого пришлось бы переработать программное обеспечение множества станций. Тем самым единая интеллектуальная сеть России осталась недостроенной, что и сказывается ныне, например, на построение Системы-112.

В настоящее время «Ростелеком» взял курс на стратегию «All-over-IP», т.е. перестраивает сеть под IP протокол. Эти планы иллюстрирует презентация «Развитие сети IP телефонии Ростелекома» [10].

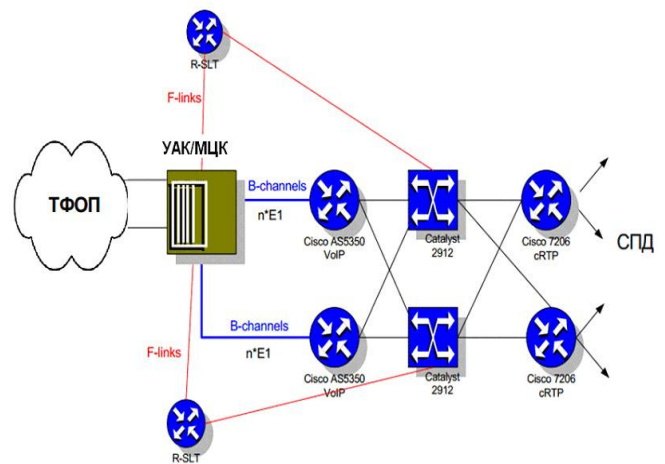


Рис. 3. Проектируемый типовой узел IP сети «Ростелекома».

На рис. 3 показан типовой узел новой IP сети. Узел предполагается построить на оборудовании Cisco.

¹ Цифровые АТС до сих пор господствуют в сетях связи, выдерживая жесткую конкуренцию с оборудованием коммутации пакетов. Наиболее известны АТС типа AXE шведской фирмы Ericsson, разработанные в 1970х. Они наследовали опыт разработки координатных АТС типа ARF, ARM, ARK и ARE (разработки 1950х), которые до сих пор находятся в эксплуатации. Второе место занимает франко-голландско-американский концерн Alcatel-Lucent. С его именем связаны АТС: Alcatel E10 (собственно разработка Alcatel), 1000-S12 (создана после приобретения ПТТ) и Western Electric 5ESS (после слияния с Lucent). В последние годы на телекоммуникационном рынке наблюдаем экспансию китайской фирмы Huawei.

Общение с узлом УАК/МЦК производится посредством системы ОКС-7 (по каналам F-links) и по В-каналам системы ISDN. Для общения с сетью ОКС-7 указан узел SLT (Cisco Signaling Link Terminal). Подобная IP сеть строится вокруг каждого УАК/МЦК (узел автоматической коммутации/международный центр коммутации), что показано на рис. 2. Вряд ли в условиях международных санкций подобные планы (на базе изделий Cisco или Juniper) удастся реализовать.

III. ОСОБЕННОСТИ СОВРЕМЕННОЙ СЕТИ GIG

Вспомним, как закладывались основы GIG, которые ныне являются тормозом ее модернизации? Оборонная информационная сеть DISN (Defense Information Systems Network) разрабатывается с начала 1990-х. Это – глобальная сеть. Ее назначение – предоставлять услуги по передаче различных видов информации (речь, данные, видео, мультимедиа) для эффективного и защищенного управления войсками, связью, разведкой и РЭБ. В 1996 г. состояние сети DISN было подвергнуто резкой критике. Прежде всего, это – низкий уровень интеграции сетей, входящих в состав DISN, что существенно ограничивает взаимодействие в рамках единой сети и препятствует эффективному единому управлению всеми ее ресурсами. В частности, отмечались сложности взаимодействия стационарной и полевой (мобильной) компонент базовой сети из-за различия в используемых стандартах, типах каналов связи (аналоговых и цифровых), предоставляемых услугах, пропускной способности (у мобильной компоненты она значительно ниже, чем у стационарной). Это порождает дополнительные трудности материального обеспечения боевых сил, технического обслуживания и подготовки специалистов. Кроме того, используемые сетевые технологии недостаточно масштабируемы и не в состоянии, в должной мере, предоставлять пропускную способность по требованию. Из-за отсутствия общей архитектуры и стандартов затруднена передача данных в интересах разведки и РЭБ. Несовместимость оборудования усложняет применение различных средств засекречивания и криптозащиты. Имеющаяся базовая архитектура DISN оказалась недостаточно гибкой и масштабируемой, особенно для мобильных сил, оперативно развертываемых в различных точках мира.

Поэтому при разработке принципов построения следующей очереди сети DISN агентство DISA пошло по пути использования готовых коммерческих продуктов (Commercial-Off-the-Shelf) в области новых информационных и сетевых технологий. Упор был сделан на открытые системы, которые основаны на национальных стандартах. Подобные требования действуют и сегодня, которые следует соблюдать поставщикам оборудования.

Эти требования нашли отражение в 15-летней программе развития вооружений «Joint Vision 2010», которую командование МО США (US Joint Chiefs of Staff) приняло в октябре 1996 г. В части средств связи основной выбор пал на интеллектуальные сети

(Advanced Intelligent Network, AIN), о чем представитель агентства DISA доложил в 1999 г. на международной конференции по военным коммуникациям MILCOM'99 [11]. Вот цитата из его выступления:

«Будущие сети DISA будут пользоваться преимуществами программных средств IN. Сервисы AIN станут ядром технологии развития, технологии оценки (assessment) и технологии передачи информации МО. Результаты сервисов AIN обеспечат командиров боевых действий способностью собирать, обрабатывать и передавать информацию без перерывов в работе сети. Возможности AIN станут краеугольным камнем информационного превосходства МО».

На той же конференции MILCOM'99 выступил представитель компании Lockheed Martin Missiles & Space [12], компании, которая является головным разработчиком глобальной информационной сети сил НАТО. В этом докладе подчеркивается, что AIN обеспечивает пользователей любыми сервисами, как то: голос, данные, e-mail, video, офисные приложения, вызовы «800». В докладе подробно описывается ключевая роль протокола SS7. Он обеспечивает множество сервисов, в том числе:

- занятие и освобождения канала (для телефонного разговора),
- передача номера вызывающего абонента,
- индикация занятости вызываемого абонента,
- индикация, что вызываемый абонент освобожден,
- управление подавлением эха,
- ограничение доступа к заданной группе абонентов.

Система SS7 составляет управляющее ядро сети AIN (рис. 4). Пользователями AIN могут быть как абоненты сети коммутации каналов, так и коммутации пакетов. До сих пор сигнализация SS7 сохраняет центральное место в сети DISN. Сеть SS7 является, образно говоря, нервной системой DISN.

Важная роль отводится интеллектуальной периферии (Intelligent Peripheral): в ее функции входит генерация тонов, распознавание голоса, сжатие речи и данных, распознавание набора номера и многое другое, включая тактические и стратегические сервисы по идентификации персонала.

Состояние сети DISN (на 2014 год) иллюстрирует рисунок 4 -- из документации по тестированию коммуникационных серверов Avaya [13]. (Более полные данные о состоянии сети GIG дают результаты тестирования сети SS7 [14].) Коммуникационный сервер Avaya S8300D выполняет функции учреденческой станции PBX с очень широким набором сервисов. Поддерживает IP-телефоны, цифровые и аналоговые аппараты. Один процессор может зарегистрировать до 50 медиа-шлюзов G450, соединенных по IP (H.248).

Распределенная структура коммуникационного сервера Avaya S8300D имеет следующие показатели: емкость процессора позволяет включать от 450 до 1000 IP-абонентов и от 450 до 4000 соединительных линий. Количество вызовов в час наибольшей нагрузки составляет 10 000. Дополнительно коммуникационный

сервер S8300D обеспечивает поддержку голосовой почты и поддержку операторских центров обработки звонков, что особенно важно.

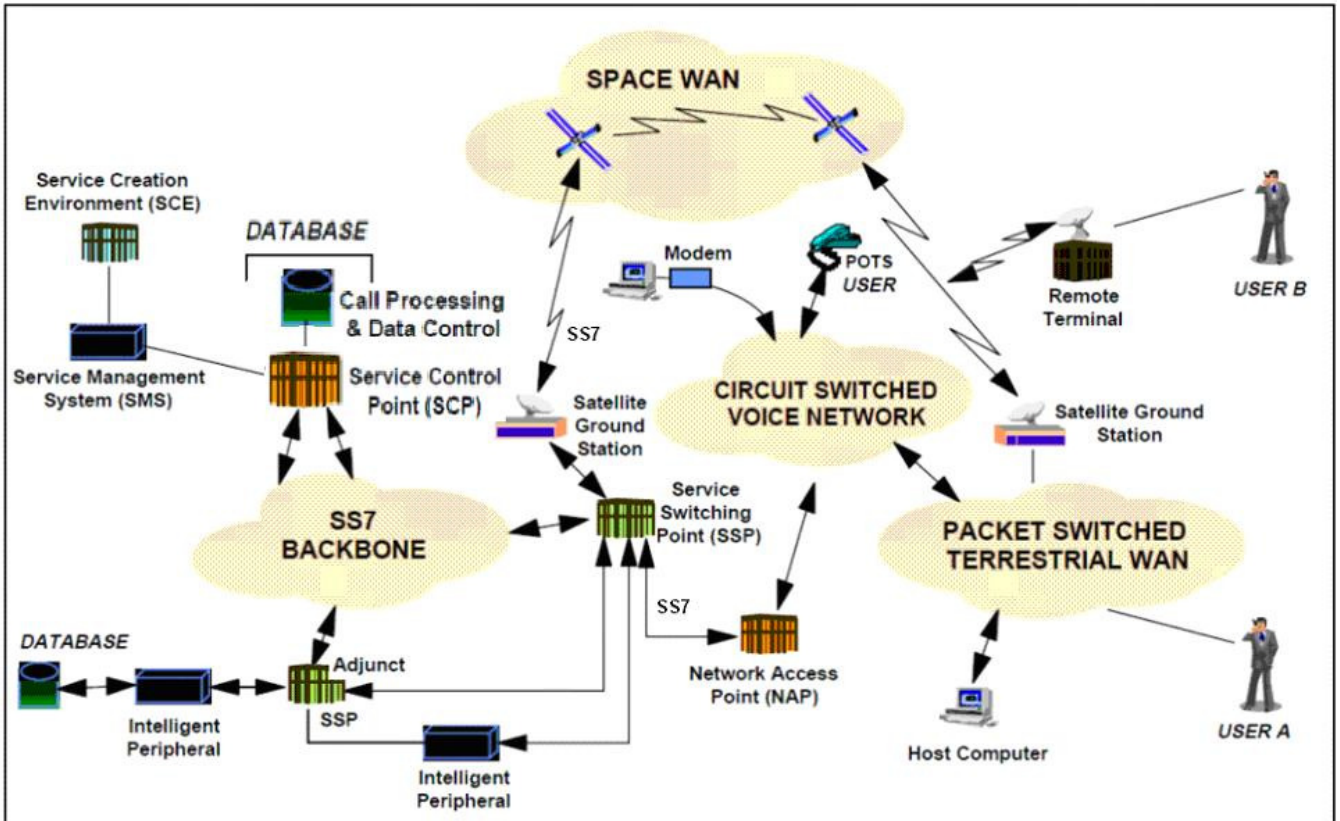


Рис. 4. Архитектура Advanced Intelligent Network (AIN).

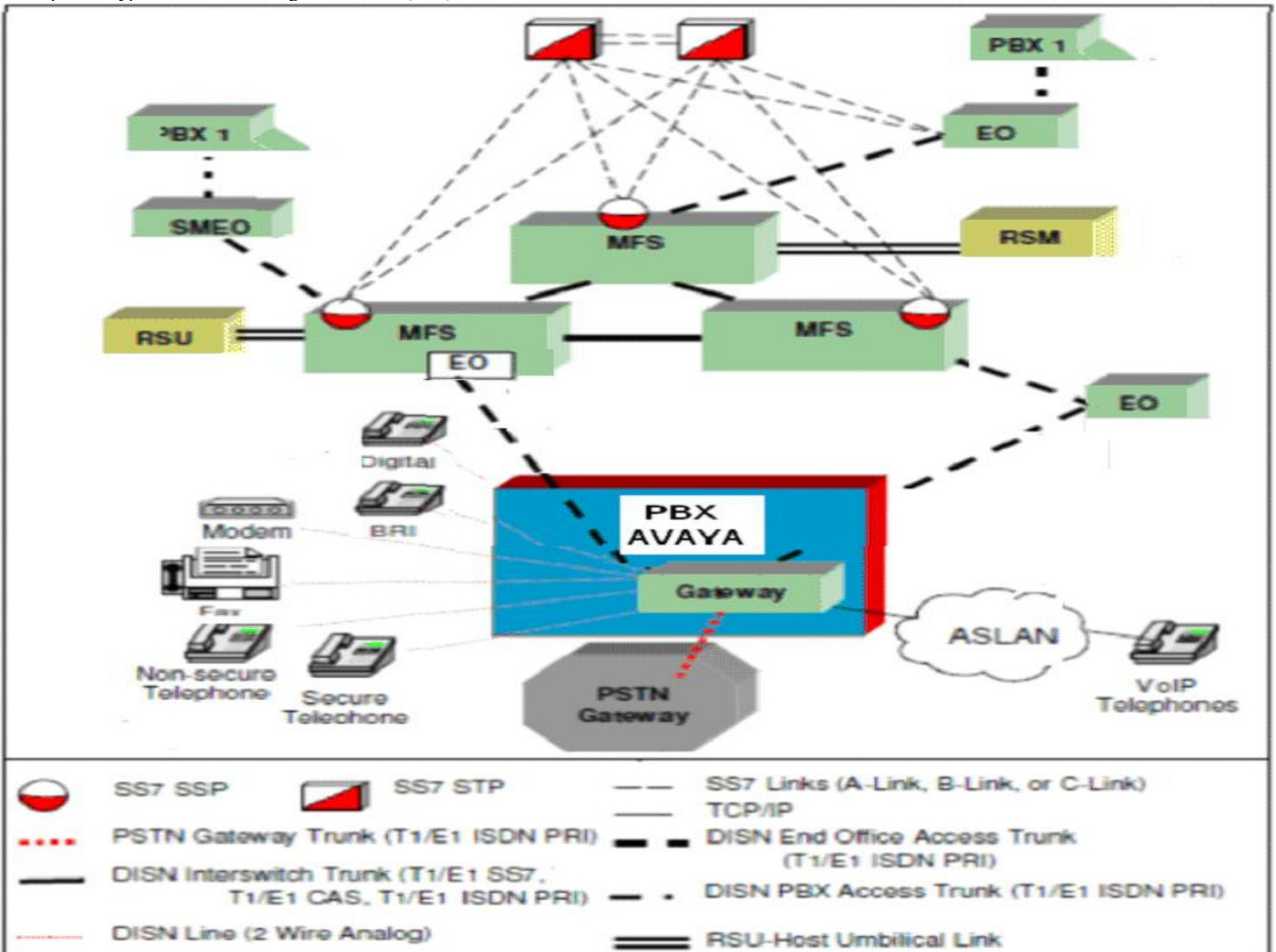


Рис. 5. Связь сервера Avaya S8300D (PBX1 SUT) с телефонными станциями MFS [13].

Коммуникационный сервер Avaya включен в электронную АТС (на рисунке 5 это MFS, Multi-Functional Switch), которая, по всей видимости, имеет функцию SSP (в составе интеллектуальной сети AIN). Обратите внимание на сеть, изображенную на рисунке 5 в центре сверху. Это сеть сигнализации SS7. То есть на оборонной сети DISN соединения до сих пор устанавливаются при помощи сигнализации SS7. Заметим, что пока неизвестно, когда планируется переход от сигнализации SS7 к протоколу AS-SIP. Тем самым не ясна судьба интеллектуальной сети AIN.

При обсуждении технической политики «Ростелеком» следовало бы учесть опыт построения AIN и ее дальнейшее развитие в условиях наступления IP технологии. Наибольшие усилия по стыковке сигнализация SS7 и интеллектуальной сети с протоколом SIP предприняты компанией Telcordia (США). Напомним, что Telcordia является продолжателем работ Bell Labs по интеллектуальным сетям. В начале 1990х Telcordia разработала несколько версий архитектуры AIN. Результаты двадцатилетних разработок объединяет группа документов AINGR Family of Requirements, FR-15 [15]. Эти документы подводят итоги работ по использованию SIP протокола, а также учет требований экстренных вызовов E9-1-1 в архитектуре AIN. На основе этих документов можно совершенствовать российскую интеллектуальную сеть и на ее основе строить, в частности, Систему 112..

IV. КАК ПЕРЕЙТИ НА IP СЕТИ

Можно выделить три этапа развития GIG. Первый этап относится к внедрению наиболее сложной части существующей сети GIG -- интеллектуальной сети AIN. Эту сеть стали строить после 1996 г. - согласно требованиям Программы развития вооружений МО США «Joint Vision 2010». Напомним, что перед выбором AIN как основы GIG сеть связи военного назначения строилась фрагментарно и подвергалась резкой критике. Сами же средства AIN к 1996 году имели длинную предысторию: они разработаны в Bell Laboratories, которые были ликвидированы аж в 1984 г. И вот сейчас – через 30 лет после разработки AIN перед строителями GIG стоит задача чем заменить AIN.

О наличии трудностей свидетельствует список вакансий на сайте компании Lockheed Martin [16]. На первом месте в длинном списке вакансий значится поиск аналитиков мультифункциональных информационных систем для DISA (рис. 6). Требуется умения разработки новых сервисов для AIN и опыт работы с оборудованием CISCO, Juniper, Promina, Safenet, Ciena, Sycamore, Ericsson. Уровень секретности работы – высший. То есть, нужны специалисты по усовершенствованию «старого» секретного ядра сети AIN (которому насчитывается уже лет 30) и его взаимодействию с новым разнородным оборудованием множества поставщиков.

Второй этап начался в 2006 г., когда был принят новый план Пентагона «Joint Vision 2020» – на следующие 15 лет. В этом плане объявлена смена парадигмы сети DISN – переход от SS7 к IP протоколу. Предполагается, что IP протокол станет единственным средством общения между транспортным уровнем и приложениями. Заметим, что пока неизвестно, когда же планируют переходить от сигнализации SS7 к протоколу AS-SIP на всей сети GIG.

Третий этап наступил в 2010 году: появилась новая инициатива – кибервойна, что потребует кардинальной перестройки GIG. В октябре 2010 года была создано киберкомандование, 2-я армия США (US Army Cyber Command/2nd Army). Обсуждению кибервойны посвящены наши статьи [17, 18].

По программе МО США о переходе на IP технологию [6] было объявлено об установке к 2012 году 22 мощнейших софтверных MFSS и WAN SS компании Cisco на американских базах по миру (рис. 7).

Industry Job Title	Mult Functional Information Systems Analyst
Job Description	Provides engineering and technical expertise on all issues relating to the specified telecommunications networks/information systems within the DISN. Applies specialized knowledge of military unique features, specifically built into the network and its subtending hardware and software, to ensure appropriate support to the warfighter's requirements. Implements or extends advanced intelligent network features into the network/system. Applies systems engineering disciplines to the provisioning of new service offerings over the network/system, often specifically tailored with military unique features.
Basic Qualifications	Requires expertise in one or more of the following devices/vendors: CISCO, Juniper, Promina, Safenet, Ciena, Sycamore, or Ericsson.
Security Clearance	Top Secret

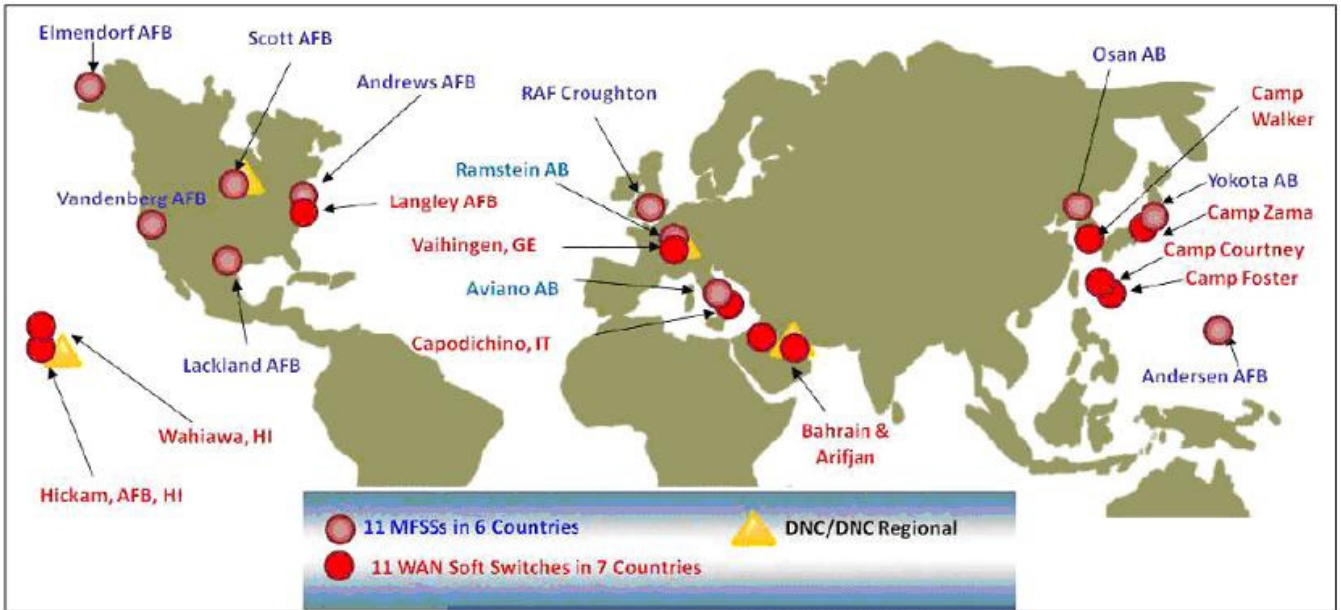


Рис. 7. Карта размещения 22 MFSS и WAN SS (2012) [6].

Напомним, что SoftSwitch (программный коммутатор) обеспечивает переход от коммутации каналов к коммутации пакетов (рис. 8). Он согласовывает протоколы сигнализации SS7 и SIP (посредством шлюза сигнализации SGW) и медиапоток IP и TDM (посредством медиашлюза MGW).

Более детальную архитектуру софтсвича показывает рис. 9. Контроллер сессии (Session Controller) – это самый сложный программный комплекс, который в сетях коммутации пакетов выполняет те же функции, что традиционные АТС. На сети GIG предполагается устанавливать три типа контроллеров (софтсвичей), в которых реализована функция контроля сессии: Wide Area Network SoftSwitch (WAN SS), Multifunction SoftSwitch (MFSS) и Local Session Controller (LSC).

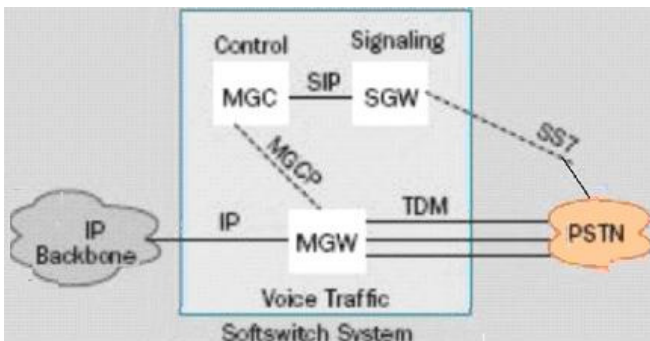


Рис. 8. Упрощенная схема софтсвича

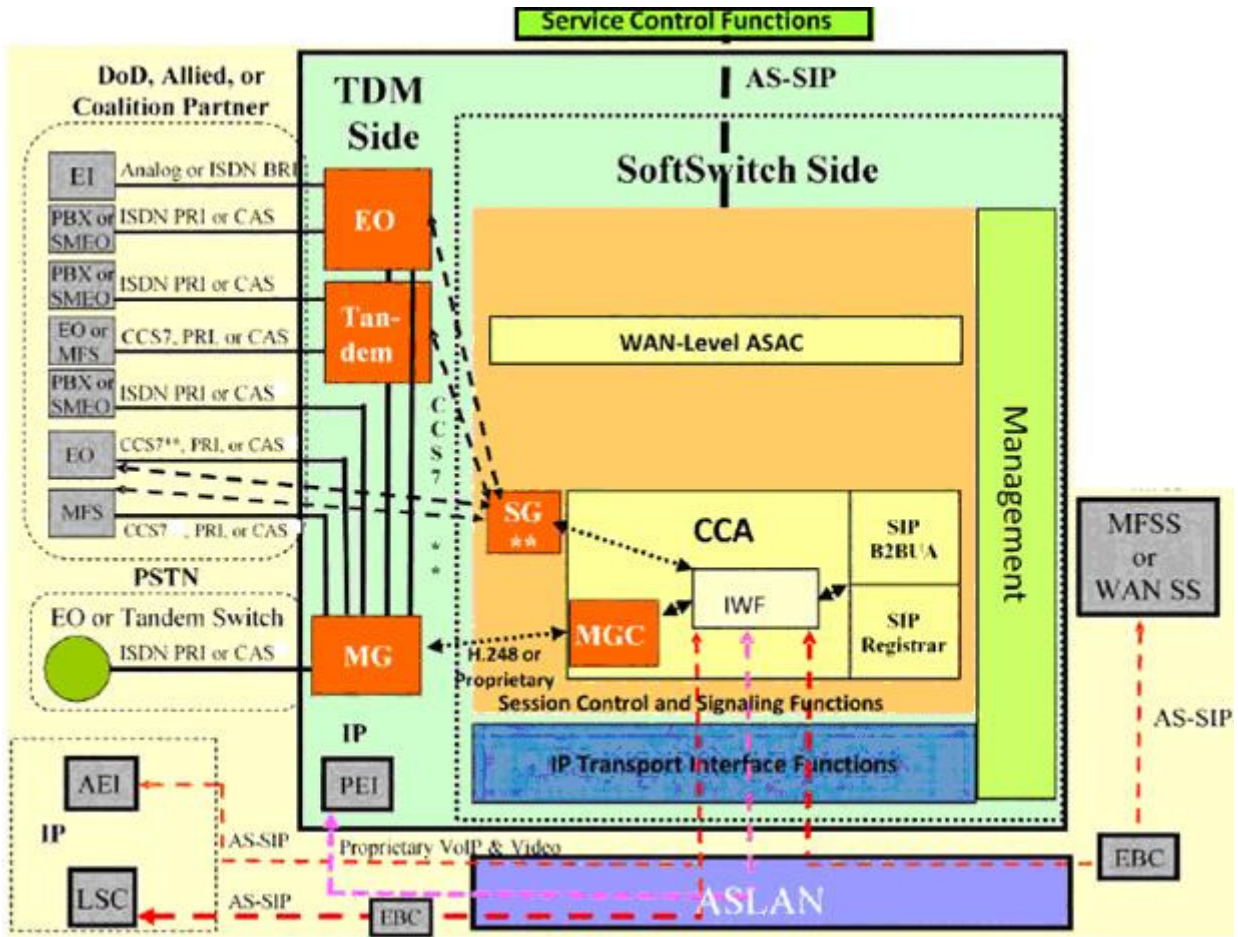


Рис. 9. Многофункциональный программный коммутатор (софтсвич) MFSS [6].

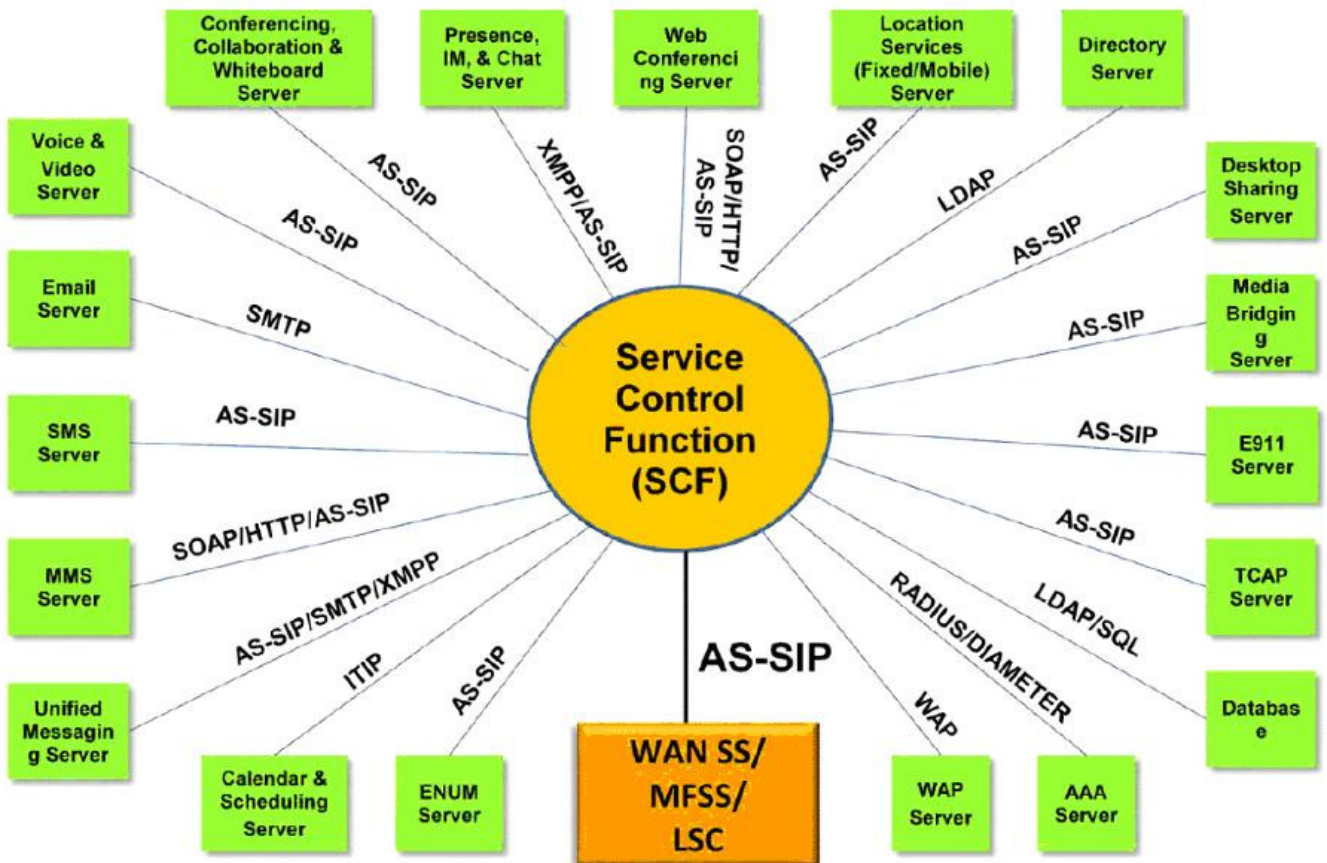


Рис. 10. Базовая модель функции контроля сессии

В настоящее время в армии США еще господствует традиционная коммутация каналов, т.е. TDM сети, и они долгое время будут сосуществовать со строящимися IP сетями. Рисунок 9 показывает, как многофункциональный софтверный MFSS управляет вызовами:

- В сторону внешней публичной сети PSTN или сети ISDN (Integrated Services Digital Network) используется функция IWF (ISUP-SIP interworking function).
- Контроллер MFSS обеспечивает «старые» сигнализации PSTN/ISDN, включая ISUP, CCS7/SS7 и CAS (Channel Associated Signalling).
- MFSS действует как медиашлюз (MG) между TDM каналами и IP каналами. Медиашлюзом управляет контроллер MGC посредством протокола H.248.
- Шлюз сигнализации SG (Signaling Gateway) обеспечивает взаимодействие между CCS7 и SIP.

На рис. 9 еще указаны оконечные устройства EO (End Office) в сети коммутации каналов и два типа IP устройств: AEI (Assured Services End Instrument), работающие по протоколу AS-SIP, и нестандартные устройства PIE (Proprietary Internet Protocol Voice End Instrument).

V. НОВЫЕ СЕРВИСЫ GIG

Состав сервисов в перспективной структуре GIG определяет блок „Service Control Function”, что показано на рис. 9 сверху и что раскрывает рис. 10. Для общения с контроллерами WAN SS, MFSS или LSC узел SCF использует единый протокол AS-SIP, а для общения с серверами разных сервисов используется множество других протоколов:

- SOAP = Simple Object Access Protocol,
- HTTP = HyperText Transport Protocol,
- LDAP = Lightweight Directory Access Protocol,
- SQL = Structured Query Language,
- RADIUS = Remote Authentication Dial In User Service,
- DIAMETER = расширенная версия RADIUS,
- WAP = Wireless Access Protocol,
- ITIP = iCalendar Transport Independent Interoperability Protocol,
- SMTP = Simple Mail Transfer Protocol,
- AAA = Authentication, Authorization, and Accounting,
- TCAP = Transaction Capabilities Application Part,
- ENUM = E.164 Number,
- IM = Instant Messaging,
- MMS = Multimedia Messaging Service,
- SMS = Short Message Service,

На рис. 10 по кругу изображены 19 серверов. Это могут быть 19 программ в составе софтверного физического объекта, а могут быть и 19 удаленных объектов. Среди них имеются 16 серверов, которые представляют 16 сервисов реального времени (Real-Time Communications, RTC), и еще три выделенных сервера:

- TCAP сервер - обеспечивает выход на базы данных интеллектуальной сети AIN,
- AAA сервер - обеспечивает услуги Authentication,

Authorization, and Accounting и пользуется протоколами RADIUS и DIAMETER,

- Database сервер - содержит данные, которые доступны по протоколам LDAP и SQL.

Приводим список 16 сервисов реального времени:

- Voice & Video,
- Web Conferencing,
- Conferencing, Collaboration & Whiteboard,
- Media Bridging,
- Presence, Instant Messaging (IM) & Chat,
- Unified Messaging,
- Calendaring & Scheduling,
- E.164 Number Mapping (ENUM),
- E.911 (Emergency Call),
- Transaction Capabilities Application Part (TCAP),
- Desktop Sharing,
- Short Message Service (SMS),
- Multimedia Message Service (MMS),
- Email,
- Wireless Application Protocol (WAP), and
- Location Services (Fixed/Mobile)

В завершении разбора возможностей создания новых услуг обсудим целевую инфраструктуру DISN. Воспользуемся новейшими методическими материалами по GIG (от 2013 г.), которые относятся к базовой архитектуре унифицированных сервисов (Unified Capabilities Reference Architecture) [5]. Эта новая архитектура унифицированных сервисов UC предлагает любому солдату и армейскому служащему богатый набор средств общения: e-mail, чат, голос, видео, поиск и многое другое, и все это доступно по единому адресу пользователя и в безопасной среде. Управление сеансом связи (Session Control) происходит по единому протоколу AS-SIP (Assured Service – Session Initiation Protocol). Сетевая архитектура унифицированных сервисов (рис. 11) базируется на широкополосной IP сети (wide area IP backbone network) и на протоколе MPLS (multiprotocol label switching protocol), который обеспечивает требуемое качество связи QoS в сети коммутации пакетов.

Наряду с этим в сети DISN используется традиционная технология SONET/TDM. Средства доступа построены на базе различных технологий: IP, LAN, PSTN/ISDN/TDM, Wi-Fi, DSL, спутники связи, медный кабель, оптоволокно, мобильная сеть 3G, WiMAX и LTE/4G. При использовании «старых» технологий PSTN/ISDN/TDM требуется устанавливать шлюзы стыковки с IP/MPLS сетью. В центре рис. 11 показаны три типа шлюзов (софтверных): MFSS, SS и LCS.

«Строительные блоки» новых услуг перечислены в верхней части рис 11 и на рис. 12. Там названы 16 сервисов реального времени и системные средства по управлению ресурсами: Content Management, Records Management, Team Collaboration, Business Process Management, Web 2.0, Applications, Portals, Profiles,

Search & Discovery, Information Assurance.

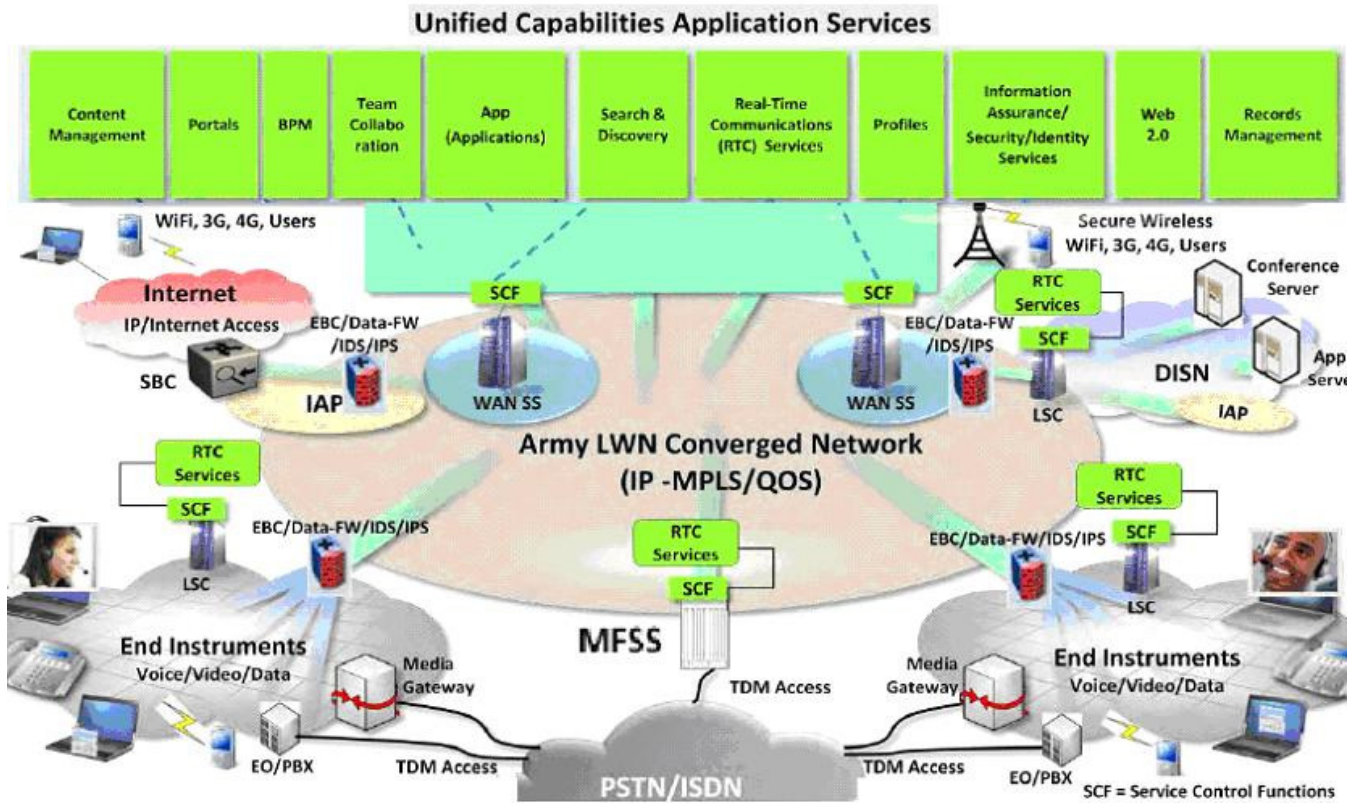


Рис. 11. Целевая единая инфраструктура DISN [5].

Portal	Team Collaboration	Web 2.0	Real-Time Communications
<ul style="list-style-type: none"> •Portlets •Personalization •Audience Targeting 	<ul style="list-style-type: none"> •Collaboration Sites •Project Sites •Business Intelligence Sites •Workflow •ECS Sites 	<ul style="list-style-type: none"> •WiKi •Blog (Team/Personal) •Social Network •Groups •Forums •Micro Blog 	<ul style="list-style-type: none"> •Voice & video •Web Conferencing •Conf, Collaboration, & WB •Media Bridging •Presence, IM, and Chat •Unified Messaging •Calendar & Scheduling •E.164 Number/ENUM •E.911 •CALEA •TCAP •Desktop Sharing •Short Msg. Service (SMS) •MM Msg. Service (MMS) •Email •Wireless App Protocol (WAP) •Location Services (Fixed/Mobile)
Profiles	BPM	Apps	
<ul style="list-style-type: none"> •Organizational Profiles •Team Profiles •Individual User Profiles 	<ul style="list-style-type: none"> •Large-Scale Process Automation •Forms Management •Orchestration •Delegation 	<ul style="list-style-type: none"> •Market •Code Repository •Rating •Certification •Accreditation •Code Scan •Distribution •Patching & Upgrading 	
Content Management	Search & Discovery	Records Management	
<ul style="list-style-type: none"> •Collection •Categorization •Organizational Drive (Team/Individual) 	<ul style="list-style-type: none"> •Indexing •Metadata Tagging (Org., Individual, Personal) •Contextual Results •Security Trimming 	<ul style="list-style-type: none"> •Scheduling •Disposition •eDiscovery •Legal Hold •Secure Destruction 	
Information Assurance			
<ul style="list-style-type: none"> •Public Key Infrastructure •Common Access Card Services •Claimed-Based Authentication •Attribute-Based Access Control 	<ul style="list-style-type: none"> •Policy Decision Service •Directory Service •EBC/Data-Firewall/IDS/IPS •AAA Services 		

Рис. 12. «Строительные блоки» новых услуг GIG.

Таблица 1. Основные услуги GIG [5]

Услуги связи	Описание
Email and Calendaring	Обеспечивает передачу сообщений с указанием приоритета, условий доставки, цифровой подписи и криптоключей. Календарь позволяет планировать расписание встреч.
Instant Messaging and Chat	Обеспечивает обмен сообщениями в реальном времени. Чат отличается от Instant Messaging групповым общением в специальном чат-пространстве.
Rich Presence	Позволяет устанавливать контакты на базе разнообразной информации о доступности в данный момент времени (IM, телефон, мобильные устройства).
Unified Messaging	Обеспечивает доступ к голосовой почте через e-mail или доступ к e-mail через голосовую почту.
Video Conferencing	Обеспечивает общение многих пользователей средствами видео-конференции.
Voice and Video (Point-to-Point)	Обеспечивает двух пользователей средствами общения посредством голоса и видео с возможностью дополнительных сервисов голосовой почты, переадресации вызова, подключения телефонистки и местной справочной службы.
Voice Conferencing	Обеспечивает организацию голосовой конференции многих пользователей.
Web Conferencing and Web Collaboration	На основе web страницы обеспечивает многих пользователей средствами общения голосом, по видео и передачей данных.

Время покажет, как из этих «строительных блоков» (Unified Capabilities) будут строиться новые услуги, и какие услуги найдут применение. Попытку строительства новых услуг показывает Таблица 1. На основе унифицированных сервисов реального времени предлагается создать восемь услуг связи. В действительности новых услуг получается больше, так как ими можно пользоваться по отдельности и в разных комбинациях. Например, Unified Messaging обеспечивает перевод текста в речь для услуги Voice and Video (Point-to-Point), а услуга Voice and Video Services (Point-to-Point) обеспечивает запись голоса для услуги Unified Messaging. Наибольшее число связей имеет услуга Rich Presence Services: с услугами Email/Calendaring, Voice and Video Services, Video Conferencing, Instant Messaging (IM)/Chat и Web Conferencing and Web Collaboration.

VI. О ЗАДАЧАХ «РОСТЕЛЕКОМА»

Анализ опыта построения GIG и состояния отечественных систем связи позволяет сформулировать несколько предложений.

1. ОАО «Ростелеком» объявило курс на импортозамещение. Если действительно идти на строительство сетей связи собственными силами, то следует вернуться к тому состоянию знаний, которые были достигнуты ранее – лет 20 назад и развивать их далее. В данном случае такой точкой отсчета условно можно назвать систему ОКС-7. В России отставание от передового мирового уровня, конечно, большое, особенно по технике коммутации пакетов, где требуется мощная микроэлектроника. Поэтому коммутация каналов на данный момент предпочтительнее.

2. Для уточнения плана собственных разработок

следует провести системное исследование и сравнить особенности технологий коммутации каналов и коммутации пакетов, особенно с точки зрения интересов спец-потребителей.

3. О российской службе экстренных вызовов 112. На рис. 10 указан сервер экстренных вызовов E.911. В руководящем документе [5] по части архитектуры армейской службы экстренных вызовов (E-911) сказано, что она на долгое время останется в области TDM сети. Признано, что переход на IP сеть произойдет по мере построения гражданской сети экстренных вызовов нового поколения NG-911 и придется обеспечить работу будущей сети по протоколу AS-SIP. Так как в России до сих пор не разработан системный проект службы 112, охватывающей всю страну и сопредельные ведомства, то целесообразно поставить задачу разработки общего системного проекта службы 112 для гражданских и военных нужд и с учетом миграции в IP область.

4. О российской интеллектуальной сети. На рис. 10 указан сервер TCAP. Этот сервер должен обеспечивать общение с базами данных в интеллектуальной сети, точнее с контроллером услуг SCP (см. рис. 4). Заметим, что протокол интеллектуальной сети INAP работает поверх протокола TCAP. В руководящем документе [5] сказано, что существующая интеллектуальная сеть AIN в будущем будет переработана с учетом требований секретности по протоколу AS-SIP, а место протокола сигнализации SS7 может занять протокол SCTP (stream control transmission protocol), который является более эффективным. Задача российских связистов заключается в доработке отечественной интеллектуальной, сети с учетом особенностей протокола INAP-R.

5. Об индустрии программирования услуг. В руководящем документе [5] сказано, что среда разработки услуг SCE (service creation environment) должна входить в состав средств разработки армейских приложений, что позволит сократить время разработки новых услуг, указано на целесообразность привлечения сторонних программистов. Это предложение относится к весьма болезненному для связистов вопросу об открытых интерфейсах программирования (Open API). Если обеспечить открытый доступ к API, то многие сторонние программисты включатся в разработку, а дело армейских связистов будет состоять в тестировании предложенных услуг и включении их в состав сети GIG. В равной мере это предложение относится к «Ростелекому»: в России имеется множество web-программистов, которые включатся в работу по конструированию новых услуг на базе новых возможностей (см. рис. 12).

БИБЛИОГРАФИЯ

- [1] Соколов Н.А. Системные аспекты построения и развития сетей электросвязи специального назначения //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 9. – С. 4-8.
- [2] <http://servernews.ru/597356> Retrieved: Dec, 2014.
- [3] <http://www.kommersant.ru/doc/2520423> Retrieved: Dec, 2014.
- [4] Department of Defense. Unified Capabilities Framework. January 2013.
- [5] U.S. Army Unified Capabilities Reference Architecture. Version 1.0, October 2013
- [6] DISA. Global Information Grid (GIG) Convergence Master Plan (GCMP), Vol. 1, 02 August 2012.
- [7] Н. С. Мардер, А. С. Аджемов Развитие российской сети ОКС № 7 — основа современных услуг связи// Сети и системы связи, 1997, №9.
- [8] <http://www.gosthelp.ru/text/PolozhenieOsnovnyepolozhe2.html/> Retrieved: Dec, 2014.
- [9] Н.С. Мардер «Современные телекоммуникации», Москва, 2106.
- [10] http://support.comptek.ru/download/index.xhtml/255/rostelekom_burkov.pdf Retrieved: Dec, 2014.
- [11] B.T. Bennet. Information Dissemination Management/ Advanced intelligent Network services for department of Defence// MILCOM, 1999.
- [12] W.W. Chao. Emerging Advanced Intelligent Network (AIN) For 21st Century Warfighters// MILCOM, 1999/
- [13] http://www.avaya.com/usa/documents/avaya_8300_pbx1_apr12.pdf Retrieved: Dec, 2014
- [14] http://jtitc.fhu.disa.mil/tssi/cert_pdfs/tekeleceagle_tn1030701.pdf/ Retrieved: Dec, 2014.
- [15] Telcordia Roadmap to Advanced Intelligent Network (AIN) Documents, Issue 2, August 2008.
- [16] <https://sjobs.brassring.com/tgwebhost/jobdetails.aspx?partnerid=25037&siteid=5010&jobid=288372> Retrieved: Dec, 2014.
- [17] Шнепс-Шнеппе М.А., Намиот Д.Е., Цикунов Ю.В. Телекоммуникации для военных нужд: сеть GIG-3 по требованиям кибервойны//International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 10. – С. 3-13.
- [18] Шнепс-Шнеппе М. А., Намиот Д. Е. Телекоммуникации для военных нужд: от сети GIG1 к сети GIG2 //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 9. – С. 9-17.

On the evolution of telecommunications services on the GIG example

M.A. Sneps-Sneppe, D.E. Namiot

Abstract— This paper discusses the difficulties of transition from circuit switching to packet switching using as an example of an information network GIG from US Department of Defense - the world's largest private network. We think, the lessons from GIG development can help domestic telecom operators in their transition to "All-over-IP" networks. This article discusses the new communication services, which are based on merging circuit switching and packet switching. Also, we discuss the conditions of import substitution in the interests of JSC "Rostelecom".

Keywords— circuit switching, packet switching, SS7, Intelligent Network, IP, Softswitch, GIG, import substitution.