ЗАКЛЮЧИТЕЛЬНЫЙ ОТЧЕТ

МСЭ-D 2-Я ИССЛЕДОВАТЕЛЬСКАЯ КОМИССИЯ

ВОПРОС 26/2

ПЕРЕХОД ОТ СУЩЕСТВУЮЩИХ СЕТЕЙ К СЕТЯМ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ ДЛЯ РАЗВИВАЮЩИХСЯ СТРАН: ТЕХНИЧЕСКИЕ, РЕГУЛЯТОРНЫЕ И ПОЛИТИЧЕСКИЕ АСПЕКТЫ

5-Й ИССЛЕДОВАТЕЛЬСКИЙ ПЕРИОД 2010-2014 Г.

Сектор развития электросвязи

СВЯЖИТЕСЬ С НАМИ

Веб-сайт:	www.itu.int/ITU-D/study_groups
Электронный книжный магазин МСЭ:	www.itu.int/pub/D-STG/
Электронная почта:	devsg@itu.int
Телефон:	+41 22 730 5999

ВОПРОС 26/2:

Переход от существующих сетей к сетям последующих поколений для развивающихся стран: технические, регуляторные и политические аспекты

Исследовательские комиссии МСЭ-D

Для обеспечения выполнения программы по обмену знаниями и созданию потенциала Бюро развития электросвязи исследовательские комиссии МСЭ-D оказывают поддержку странам в достижении ими своих целей развития. Выступая в качестве катализатора в создании, применении знаний и обмене знаниями в области ИКТ в целях сокращения масштабов нищеты и обеспечения социально-экономического развития; исследовательские комиссии МСЭ-D помогают стимулировать создание в Государствах-Членах условий для использования знаний для более эффективного достижения целей развития.

Платформа знаний

Результаты работы, согласованные в исследовательских комиссиях МСЭ-D, и соответствующие справочные материалы используются в качестве исходных документов при реализации политики, стратегий, проектов и специальных инициатив в 193 Государствах − Членах МСЭ. Эти виды деятельности служат также для укрепления базы совместно используемых знаний Членов МСЭ.

Платформа для обмена информацией и знаниями

Обмен темами, представляющими общий интерес, осуществляется путем участия в очных собраниях, на электронном форуме, а также путем дистанционного участия в атмосфере, благоприятной для открытого обсуждения и обмена информацией.

Хранилище информации

Отчеты, руководящие указания, примеры передового опыта и Рекомендации разработаны на основе вкладов, поступивших для рассмотрения членами комиссий. Информация собрана путем обследований, вкладов и исследований конкретных случаев и доступна для Членов, использующих средства управления информационными ресурсами и веб-публикаций.

2-я Исследовательская комиссия

ВРКЭ-10 поручила 2-й Исследовательской комиссии исследование девяти Вопросов в области информационно-коммуникационной инфраструктуры и развития технологий, электросвязи в чрезвычайных ситуациях и адаптации к изменению климата. Основными направлениями работы стали исследования методов и подходов, которые в наибольшей мере соответствуют предоставлению услуг при планировании, разработке, внедрении, эксплуатации, техническом обслуживании и поддержке услуг электросвязи/ИКТ и дают наилучшие результаты, а также повышают ценность этих услуг для пользователей. В этой работе особое значение придается широкополосным сетям, подвижной радиосвязи и электросвязи/ИКТ для сельских и отдаленных районов, потребностям развивающихся стран в управлении использованием спектра, использованию ИКТ/электросвязи для смягчения воздействия изменения климата на развивающиеся страны, электросвязи/ИКТ для смягчения последствий стихийных бедствий и оказания помощи, проверке на соответствие и функциональную совместимость и электронным приложениям, причем основное внимание уделяется приложениям, поддерживаемым сетями электросвязи/ИКТ. Кроме того, работа была сосредоточена на внедрении информационно-коммуникационных технологий с учетом результатов исследований, проводимых МСЭ-R и МСЭ-T, и приоритетов развивающихся стран.

2-я Исследовательская комиссия совместно с 1-й Исследовательской комиссией МСЭ-R участвует в работе по Резолюции 9 (Пересм. ВКРЭ-10) "Участие стран, в особенности развивающихся стран, в управлении использованием спектра".

Настоящий отчет подготовлен многочисленными добровольцами из различных администраций и организаций. Упоминание конкретных компаний или видов продукции не является одобрением или рекомендацией МСЭ. Выраженные мнения принадлежат авторам и ни в коей мере не влекут обязательств со стороны МСЭ.

Содержание

Стр.

Рисунки и таблицы

Стр.

ВОПРОС 26/2
Переход от существующих сетей к сетям последующих поколений для развивающихся стран: технические, регуляторные и политические аспекты

1 Переход к СПП

1.1 Почему необходим переход?

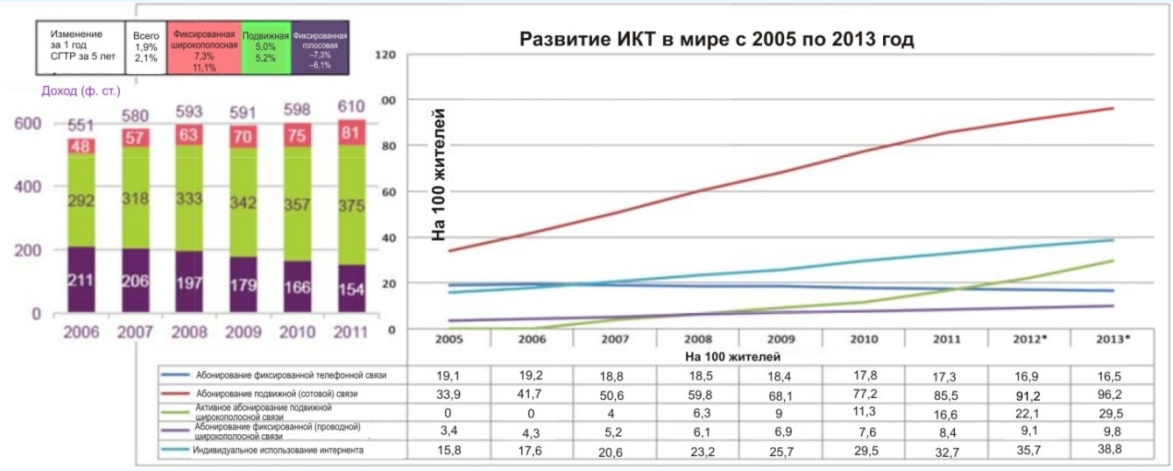
В этом разделе описываются причины для перехода от существующей сетевой инфраструктуры к новой сетевой инфраструктуре. Существует несколько причин, отражающих различные точки зрения, например деловые аспекты, технические аспекты и т. д.

1.1.1 Основная мотивация перехода

Одним из важных факторов, которые следует учитывать при переходе к новой сетевой инфраструктуре, такой как СПП, является следование тенденциям, вызываемым бизнес-процессами.

Одним из ключевых моментов бизнес-процессов является переход услуг голосовой связи от традиционных технологий фиксированной связи (на основе, например, КТСОП и ЦСИС) к технологиям на основе подвижной связи и межсетевых протоколов (IP). Как показано ниже на Рисунке 1-1, эта тенденция началась в 2003 году и продолжается до сих пор. Данная тенденция привела к двум направлениям развития: во-первых, к снижению доходов от услуг фиксированной голосовой связи (например, за период с 2006 по 2011 год доходы от услуг фиксированной голосовой связи упали примерно на 6%), во-вторых, к увеличению спроса на услуги, ориентированные на подвижную связь и передачу информации по IP-протоколу через сети фиксированной и/или подвижной широкополосной связи, что требует дополнительных инвестиций в существующую сетевую инфраструктуру (например, рост доходов от услуг подвижной связи на 5,2%, а широкополосной связи – примерно на 11% за период с 2006 по 2011 гг.).

Рисунок 1-1: Текущее состояние развития ИКТ



Источник: IDATE/данные отрасли/Ofcom 2012

Существует несколько путей, позволяющих следовать этим тенденциям, которые можно разделить на два направления: компенсация уменьшения доходов и изыскание новых источников дохода.

При компенсации уменьшения доходов наиболее важным элементом, помимо снижения затрат на развертывание сетевой инфраструктуры и инфраструктуры предоставления услуг, должно стать уменьшение затрат за счет совместного использования систем и инфраструктуры сети. Исходя из этого ниже приводятся соответствующие требования, которые должны быть учтены при переходе к СПП:

- снижение эксплуатационных расходов и дальнейшая рационализация операций;
- внедрение интегрированных платформ для обеспечения различных видов услуг и приложений;
- внедрение интегрированных эксплуатационных платформ, включая объединение технического обслуживания и обучения;
- использование централизованного управления и контроля.

Вообще говоря, предоставление экономичных мультимедийных услуг на коммерческой основе с точки зрения поиска новых источников дохода должно стать одним из важнейших элементов. В этой связи при оказании мультимедийных услуг перечисленные ниже задачи следует рассматривать как требования высокого уровня, которые будут служить основными причинами перехода к СПП:

- компенсация уменьшения доходов от услуг голосовой связи и расширение коммерческих операций, связанных с использованием услуг широкополосной связи;
- введение инноваций в сфере обслуживания (например, виртуальные частные сети (VPN));
- вывод на рынок в сжатые сроки каких-либо новых видов услуг и приложений.

1.1.2 Мнение операторов в отношении перехода

Следование тенденциям в предпринимательской деятельности также является очень серьезным вопросом для операторов, поскольку они находятся в центре этих процессов. Иными словами, операторы должны в кратчайшие сроки обеспечить, чтобы их деятельность по предоставлению услуг была достаточной для компенсации уменьшения доходов. А любые виды новых систем и элементов, вводимые в инфраструктуру операторами, будут достаточным дополнением для своевременного получения новых доходов.

Операторы, которые планируют введение новых элементов инфраструктуры, должны обеспечивать выполнение следующих требований:

- поддержку непрерывной деятельности, необходимой для бесперебойного предоставления основных услуг и обслуживания клиентов, которым требуются услуги связи операторского класса;
- гибкость при подключении существующих новых услуг и быстрое реагирование на те услуги, которые появляются в реальном времени (в полной мере используя преимущества режима IP);
- прибыльность, позволяющую получать реальный доход на вложенные инвестиции и по наиболее оптимальным рыночным ценам;
- живучесть, позволяющую гарантировать предоставление услуг в случаях возникновения сбоев и непредвиденных внешних обстоятельств;
- качество предоставления услуг, гарантирующее выполнение условий соглашения об уровне обслуживания для различных сочетаний, условий и перегрузки трафика;
- функциональную совместимость сетей, позволяющую предоставлять сквозные услуги для потоков данных в различных сетевых доменах.

В целом признается, что СПП должна стать одной из преобладающих структур, удовлетворяющих указанным требованиям. По этой причине многие из операторов начинают переходить от существующей сетевой инфраструктуры к СПП, а некоторые из них уже осуществили этот переход.

1.1.3 Переход с технической точки зрения

В настоящее время существует множество технических вопросов, которые касаются равномерного использования в интернете IP-технологий, применяемых в том числе и в сетях СПП. Эти технические вопросы создали определенные трудности при удовлетворении требований операторов сетей и поставщиков услуг. Кроме того, эффективная эксплуатация таких средств, как телевидение по IP-протоколу (IPTV), также сопряжена с дополнительными техническими проблемами. Следовательно, необходимо разработать совершенно новые технологии либо задействовать дополнительные возможности в дополнение к существующему IP-протоколу в тех случаях, когда он используется.

Краткий перечень основных технических вопросов представлен в таблице 1.

Согласно определению, приведенному в Рекомендации МСЭ-Т Y.2001, сети последующих поколений (СПП) позиционируются как одно из основных средств, с помощью которых можно решить многие (а возможно и все) указанные технические проблемы. Таким образом, в большинстве отраслей экономики разрабатываются системы СПП, а операторы осуществляют переход существующей инфраструктуры к электросвязи на основе СПП.

Таблица 1-1: Технические вопросы, связанные с переходом

Техническая область	Вопрос
Управление	Масштабируемость Выставление счетов
Качество обслуживания (QoS) и безопасность	Повышение надежности Повышение отказа устойчивости Безопасные системы Помехоустойчивость Функциональные характеристики Функциональные характеристики приложений Аутентификация, авторизация и учет
Повсеместная доступность	Повсеместно распределенная сеть, позволяющая пользователю иметь соединения – всегда, в любое время, в любом месте, любым способом Информированность о наличии услуг
Контент	Управление цифровыми правами (DRM) Условный доступ Безопасная и эффективная доставка
Оптимизация сети	Общая инфраструктура услуг Меньшее количество сетевых услуг Меньшее количество операций переключения Упрощенный процесс развертывания услуг Более высокая пропускная способность
Функциональная совместимость	Функционально совместимое оборудование от всех поставщиков
Многообразие сетей доступа	Фиксированные, подвижные, медные, волоконно-оптические, беспроводные… Поддержка множественных соединений "Прозрачная" мобильность в проводных и беспроводных сетях
Совместно используемые ресурсы	Совместно используемые ресурсы передачи как голоса, так и данных Максимально возможное совместное использование платформ обслуживания
Сочетание традиционных услуг и услуг интернета	Возможность сочетания традиционных существующих услуг связи с услугами на основе IP-протокола

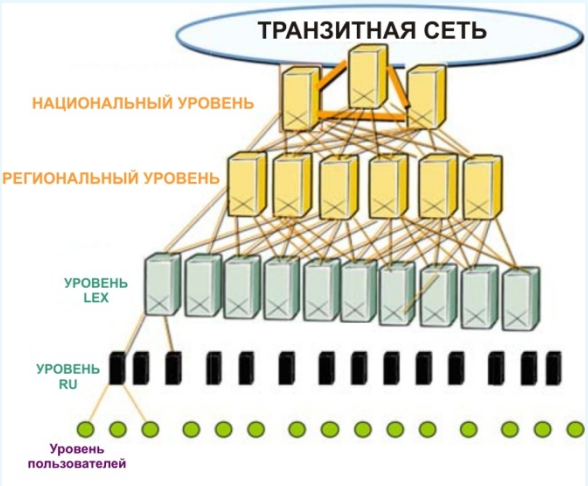
Техническая область	Вопрос
Интерактивность	Сквозная интерактивность (например, персонализированная интерактивная мультимедийная связь и т. д.) Интерактивность "клиент–сервер" (например, для игр: высокая производительность и небольшое время ожидания) Интерактивность, управляемая пользователем (например, передача информации любым устройствам, интерактивность типа от "m" к "n" и т. д.)
Хранение данных	Непрерывность процесса Совместное хранение данных как общественных (например, NPVR и "облачные" вычисления), так и частных (например, PVR) Сохранение данных
Соответствие стандартам	Введение в действие устройств, соответствующих действующим стандартам Стандартизированные протоколы и интерфейсы

1.1.4 Соображения, связанные с архитектурой

Один из традиционных существующих видов электросвязи построен с несколькими уровнями иерархии. Рассматриваются два аспекта: один из них касается технических основ, таких как физическая сеть, транспортная сеть, сеть обслуживания и т. д., а другой отражает основу геометрического распределения, например сеть удаленного доступа, региональную сеть, национальную сеть и т. д. Эти уровни иерархии, как правило, весьма полезны не только для установки и функционирования, но и для совершенствования систем. Кроме того, эти уровни иерархии хорошо согласуются с предоставлением услуг на основе традиционной телефонной связи и работой сети в части идентификации, т. е. на основе E.164.

Однако эти уровни иерархии создают определенные ограничения, особенно при обеспечении надлежащего сквозного соединения и эффективном управлении маршрутизацией с учетом различных особенностей IP-протокола, таких как использование простой адресации и динамической маршрутизации. Поэтому традиционные иерархии являются основой для подготовки инфраструктуры на базе IP-протокола. Далее на Рисунке 1-2 показана модель архитектуры традиционных сетей электросвязи.

Рисунок 1-2: Общая модель архитектуры традиционных сетей электросвязи



Ниже приводится краткий перечень основных характеристик, присущих традиционной модели архитектуры:

- иерархическая топология с 4–5 уровнями, возможностью соединения со следующим более высоким уровнем, а также в пределах каждого уровня в зависимости от экономической оптимизации;
- то или иное количество узлов в зависимости от трафика выходных данных и пропускной способности узлов;
- обработка услуг для средств распространения информации, сигнализации, управления и администрирования на всех узлах коммутации;
- предоставление услуг с качеством операторского класса с четко определенными критериями качества обслуживания и стандартизированными техническими нормативами.

Для сохранения оптимальных характеристик существующей инфраструктуры необходимо улучшить определенные характеристики в соответствии с меняющимися тенденциями. В этой связи необходимо учитывать следующие аспекты:

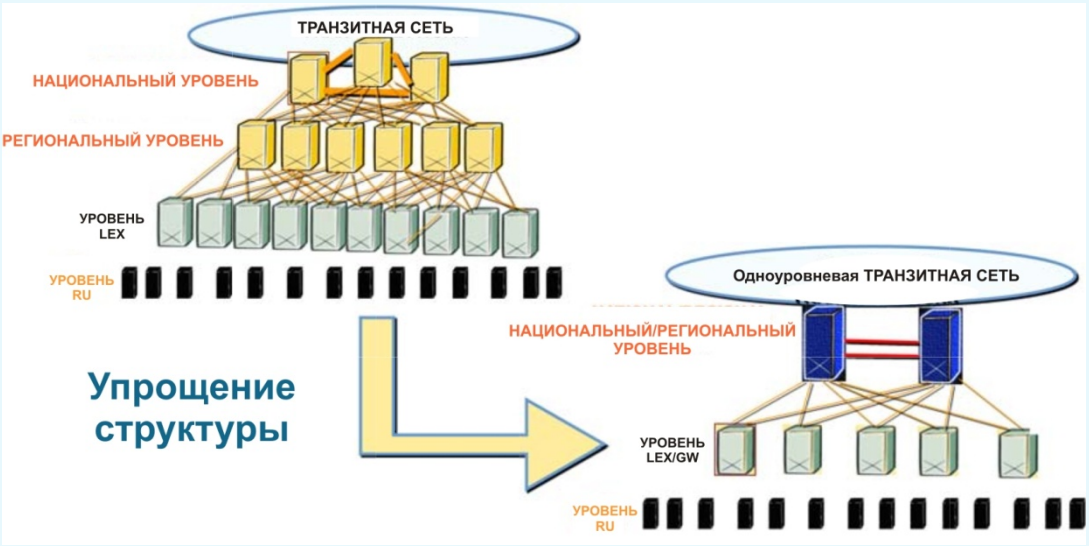
- меньшее количество сетевых узлов и линий благодаря более высокой (на порядок) пропускной способности систем;
- одинаковую капиллярность на уровне доступа благодаря идентичному местоположению клиента;
- более высокую топологическую возможность соединений для узлов и трактов с более высокой пропускной способностью благодаря требованиям безопасности.
- высокий уровень защиты и использование разнесенных трасс/источников во всех системах с высокой пропускной способностью как на функциональном, так и на физическом уровнях.

С учетом вышеупомянутого логического обоснования ожидается, что новая инфраструктура должна быть построена на основе более простой архитектуры, чем существующая. Один из примеров, подтверждающих подобное предположение, приведен на Рисунке 1-3.

Такого рода упрощенная архитектура помимо решения вопросов, присущих традиционной инфраструктуре электросвязи, позволит обеспечить множество преимуществ. Одно из важных преимуществ должно быть реализовано в сетях доступа, в которых решающую роль играют затраты на создание физической инфраструктуры и время развертывания. Это преимущество стало результатом использования абонентской линии связи меньшей протяженности, чем классические сети, и таким образом подготавливается почва для предоставления широкополосных мультимедийных услуг.

Такая упрощенная архитектура позволит быстро развертывать средства широкополосной связи путем использования технологии xDSL и/или волоконно-оптического кабеля ближе к клиентам при внедрении новых линейно-кабельных сооружений или модернизации существующих. Кроме того, это обеспечит большую гибкость при внедрении новых беспроводных технологий при низкой плотности клиентов. Все эти сети с улучшенным доступом, оснащенные средствами фиксированной и подвижной широкополосной связи, обеспечат очень гибкие возможности для оказания различных мультимедийных услуг в условиях конвергенции фиксированной и подвижной связи.

Рисунок 1-3: Способ улучшения в плане архитектуры



1.2 СПП как один из путей перехода

1.2.1 Основные характеристики СПП

Полное название СПП, расшифровываемое как "сети последующих поколений", само по себе не содержит достаточной информации для понимания общей картины. Благодаря МСЭ-Т разработаны четкое определение и ряд основных характеристик для более подробного определения СПП, включая аспекты СПП и их характеристики для более подробного определения СПП, включая аспекты эксплуатации и услуг. В Рекомендациях МСЭ-Т Y.2001 и Y.2011 приведены определения СПП и их характеристики, согласованные на глобальном уровне.

В Рекомендации МСЭ-Т Y.2001 приводится следующее общепринятое определение СПП: "Сеть с пакетной коммутацией, пригодная для предоставления услуг электросвязи и для использования нескольких широкополосных технологий транспортировки с включенной функцией QoS, в которой связанные с обслуживанием функции не зависят от примененных технологий, обеспечивающих транспортировку. Она обеспечивает свободный доступ пользователей к сетям и конкурирующим поставщикам услуг и/или выбираемым ими услугам. Она поддерживает универсальную подвижность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям".

Кроме того, в Рекомендации Y.2001 приводятся следующие основополагающие характеристики СПП:

- пакетная передача с пакетной коммутацией;
- разделение функций управления между пропускной способностью канала-носителя, вызовом/сеансом, а также приложением/услугами;
- развязка между предоставлением услуг и транспортировкой и предоставление открытых интерфейсов;
- поддержка широкого спектра услуг, приложений и механизмов на основе унифицированных блоков обслуживания (включая услуги в реальном масштабе времени, в потоковом режиме, в автономном режиме и мультимедийные услуги);

- возможности широкополосной передачи со сквозной функцией QoS (качества обслуживания);
- взаимодействие с существующими сетями с помощью открытых интерфейсов;
- универсальная мобильность;
- неограниченный доступ пользователей к разным поставщикам услуг;
- разнообразие схем идентификации;
- единые характеристики обслуживания для одной и той же услуги с точки зрения пользователя;
- сближение услуг между фиксированной и подвижной связью;
- независимость связанных с обслуживанием функций от используемых технологий транспортировки;
- поддержка различных технологий "последней мили";
- выполнение всех регламентарных требований, например для аварийной связи, защиты информации, конфиденциальности, законного перехвата и т. д.

Анализируя определения и характеристики СПП, можно выделить следующие ключевые характеристики СПП, которые должны стать основой для понимания и использования СПП.

- Открытая архитектура – открыта для поддержки создания услуг, обновления услуг и включения предоставления логики услуг третьими сторонами, а также поддерживает "Распределенное управление" и повышенную безопасность и защиту.
- Независимое предоставление услуг – процесс предоставления услуг должен быть отделен от работы сети путем использования распределенного механизма открытого управления для содействия развитию конкуренции.
- Поддержка многостороннего доступа – функциональная архитектура СПП обеспечивает гибкость конфигурации, необходимую для поддержки технологий многостанционного доступа.

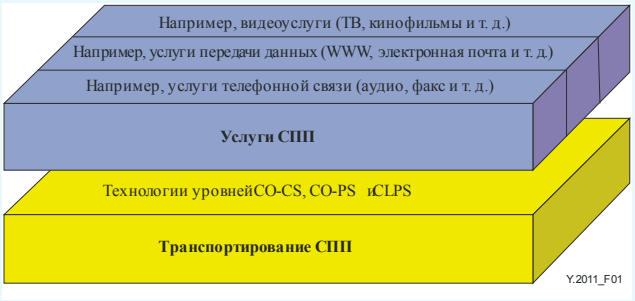
Сравнивая ключевые возможности, полученные из определения и характеристик СПП, приведенных в Рекомендации МСЭ-Т, следует признать, что эти возможности создадут определенные условия для решения проблем, возникающих при удовлетворении тенденциям предпринимательской деятельности, описанным в главе 1.

1.2.2 Эталонная модель архитектуры СПП

Одной из важнейших задач, которую предстоит решить СПП, является разделение услуг и транспортных технологий, на которых эти услуги базируются. Базовая эталонная модель для СПП показана на Рисунке 1-4 (Рекомендация МСЭ-Т Y.2011). На этой схеме показана ситуация, когда услуги отделены от базовой транспортной сети.

Вообще говоря все без исключения виды сетевых технологий могут быть развернуты в страте транспортирования, которая обозначается как "транспортирование СПП", включая технологии уровней, ориентированные на соединение сетей с коммутацией каналов (CO-CS), ориентированные на соединение сетей с коммутацией пакетов (CO-PS) и сетей с коммутацией пакетов без установления соединения (CLPS), согласно Рекомендациям G.805 и G.809. До сих пор считается, что использование протокола IP наиболее предпочтительно для поддержки услуг СПП, а также для поддержки услуг существующих. "Услуги СПП" – это услуги для пользователей, такие как телефония, веб-услуги и т. д. Таким образом, в состав "услуг СПП" может входить комплекс географически распределенных сервисных платформ услуг или, в более простом варианте, только сервисные функции со стороны двух конечных пользователей.

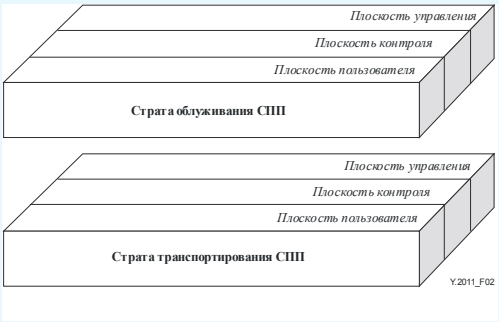
Рисунок 1-4: Разделение услуг и транспортирования в сетях СПП



В Рекомендации МСЭ-Т Y.2011 применяется особая терминология, согласно которой два важных понятия, показанные на Рисунке 1-5, получили названия "страта обслуживания СПП" и "страта транспортирования СПП". В этой Рекомендации также дается общее представление об этих понятиях следующим образом.

- **Страта обслуживания СПП**. Та часть СПП, которая обеспечивает функции пользователя по передаче связанных с обслуживанием данных и функции по контролю и управлению ресурсами услуг и сетевыми услугами таким образом, чтобы предоставить пользователям услуги и соответствующие приложения. Услуги для пользователей могут быть реализованы путем рекурсии нескольких уровней обслуживания в пределах страты обслуживания. Страта обслуживания СПП связана с приложением и его службами, которые функционируют между одноранговыми объектами. Например, услуги могут быть связаны с приложениями по передаче голоса, данных или видеоизображений, расположенными отдельно или в какой-либо комбинации в случае мультимедийных приложений. С точки зрения архитектуры считается, что каждый слой в страте обслуживания имеет свои собственные плоскости пользователя, контроля и управления.

Рисунок 1-5: Базовая эталонная модель СПП (NGN BRM)



- **Страта транспортирования СПП**. Это та часть СПП, которая обеспечивает функции пользователя по передаче данных и функции по контролю и управлению транспортными ресурсами и для передачи таких данных между оконечными объектами. Данные, передаваемые подобным образом, могут сами быть информацией пользователя, информацией для контроля и/или управления. Для контроля и/или управления передачей информации между такими объектами могут устанавливаться статические или динамические взаимосвязи. Страта транспортирования СПП реализуется путем рекурсии многоуровневых

сетей, как это описано в Рекомендациях МСЭ-Т G.805 и G.809. С точки зрения архитектуры считается, что каждый слой в страте транспортирования имеет свои собственные плоскости пользователя, контроля и управления.

На базе основных понятий об архитектуре СПП, приведенных выше, МСЭ-Т разработал модель архитектуры СПП с подробным описанием функций. Эта модель, опубликованная в Рекомендации МСЭ-Т Y.2012, показана на Рисунке 1-6.

В целях реализации следующих принципов в Рекомендации МСЭ-Т Y.2012 разработана архитектура СПП.

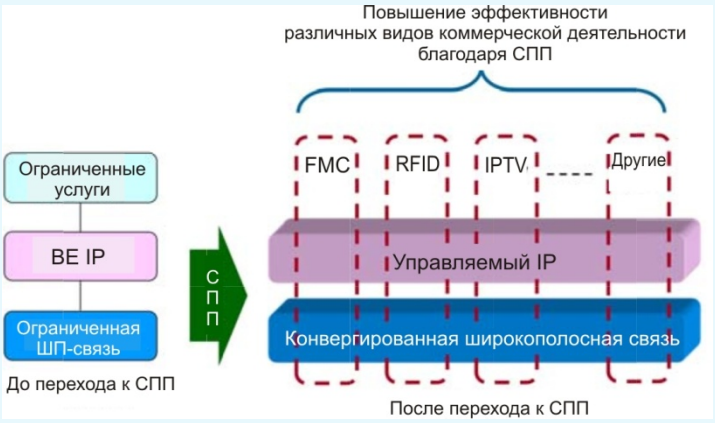
- Поддержка технологий многостанционного доступа. Функциональная архитектура СПП должна обеспечивать гибкость конфигурации, необходимую для поддержки технологий многостанционного доступа.
- Распределенное управление. Это позволит адаптироваться к распределенной обработке пакетных сетей и осуществлять поддержку прозрачности местоположения для распределенных вычислений.
- Открытое управление. Интерфейс управления сетью должен быть открытым для поддержки создания услуг, обновления услуг и включения возможностей предоставления логики услуг третьими сторонами.
- Независимое предоставление услуг. Процесс предоставления услуг должен быть отделен от функционирования транспортной сети путем использования вышеупомянутого распределенного механизма открытого управления. Этот принцип предназначен в целях содействия формированию конкурентной среды для развертывания СПП, что в свою очередь ускорит процесс предоставления разнообразных услуг СПП.
- Поддержка услуг в конвергированной сети. Этот принцип необходим для формирования гибких, простых в использовании мультимедийных услуг путем задействования части технического потенциала конвергированной функциональной архитектуры фиксированной и подвижной связи СПП.
- Повышенная безопасность и защита. Это является основным принципом открытой архитектуры, который необходим для защиты сетевой инфраструктуры путем обеспечения механизмов безопасности и живучести на соответствующих уровнях.
- Характеристики функционального объекта. Функциональные объекты должны соответствовать следующим принципам:
  - функциональные объекты могут не быть распределены между множеством физических модулей, но могут иметь много экземпляров;
  - функциональные объекты не имеют прямого отношения к многоуровневой архитектуре. Тем не менее похожие объекты могут быть расположены на различных логических уровнях.

Рисунок 1-6: Обзор архитектуры СПП

1.2.3 Преимущества архитектуры СПП

Одним из важнейших преимуществ архитектуры СПП является возможность предоставления различных услуг через общую транспортную платформу. А разнообразные технологии широкополосной связи через домены фиксированных и подвижных сетей доступа позволят эффективно использовать это преимущество, например, предоставляя различные услуги широкополосной связи и конвергенции по фиксированным и подвижным конвергированным транспортным сетям. Ниже, на Рисунке 1-7, показано, каким образом при помощи архитектуры СПП будет реализована поддержка различных услуг.

Рисунок 1-7: Преимущества архитектуры СПП



Одним из преимуществ использования протокола IP является обеспечение простой связи между уровнем 3 и уровнем 4, которая, как правило, является критической точкой разделения между обслуживанием и транспортированием. До перехода к СПП (показано в левой части Рисунка) протокол IP мог обеспечить всего один режим, называемый "оптимальный вариант", который не был способен поддерживать достаточный уровень качества и не отвечал требованиям безопасности. Кроме того, базовое транспортирование было основано на крайне ограниченных возможностях широкополосной связи xDSL, которые создавали определенные ограничения в плане соответствия коммерческим тенденциям. В данной ситуации невозможно было бы обеспечить достаточное количество платформ для эффективного использования конвергированных услуг и активизации коммерческой деятельности.

После перехода к СПП расширенные возможности протокола IP (под названием "Управляемый IP") и базовое транспортирование с функциональными возможностями конвергированной широкополосной связи смогут обеспечить поддержку различных услуг (например, IPTV, RFID, FMC и т. д.) через стандартную транспортную сеть, сохраняя при этом простую связь между уровнем 3 и уровнем 4. Как следствие будут созданы различные бизнес-модели, а участники рынка коммерческих услуг будут заинтересованы в формировании разнообразных и гибких деловых взаимоотношений.

1.2.4 Усовершенствование системы IMS для приложений СПП

Спецификации информационной управляющей системы (IMS) разработаны для применения в сотовых сетях доступа и основаны на определенных допущениях, относящихся к сети доступа, например доступная ширина полосы пропускания. Отличия, присущие различным видам сетей доступа, нашли вполне конкретное отражение в спецификациях IMS. Примеры таких отличий таковы.

- Для поддержки сетей доступа на базе xDSL системе IMS может также потребоваться сопряжение с функциями подсоединения к сети IP-CAN с целью получения информации о местоположении. В базовых спецификациях IMS подобный интерфейс отсутствует.
- Необходимо учитывать поддержку протокола IPv4, что в свою очередь требует поддержки функциональных возможностей NAPT. Для этого существуют по меньшей мере две причины:
  - некоторым операторам пришлось (или придется) столкнуться с нехваткой адресов IPv4;
  - говоря о конфиденциальности IP-адресов для потоков медиаданных, не следует полагаться на RFC 3041 (Расширения, обеспечивающие конфиденциальность для автоконфигурации адреса без запоминания в IPv6), как в случае с IPv6. Альтернативным решением, позволяющим скрыть адреса оконечных устройств, является функция NAPT.

В функциональную архитектуру СПП включена поддержка функций NAPT. В спецификациях систем IMS должны быть предусмотрены расширения к IMS для работы с конфигурациями, содержащими NAPT.

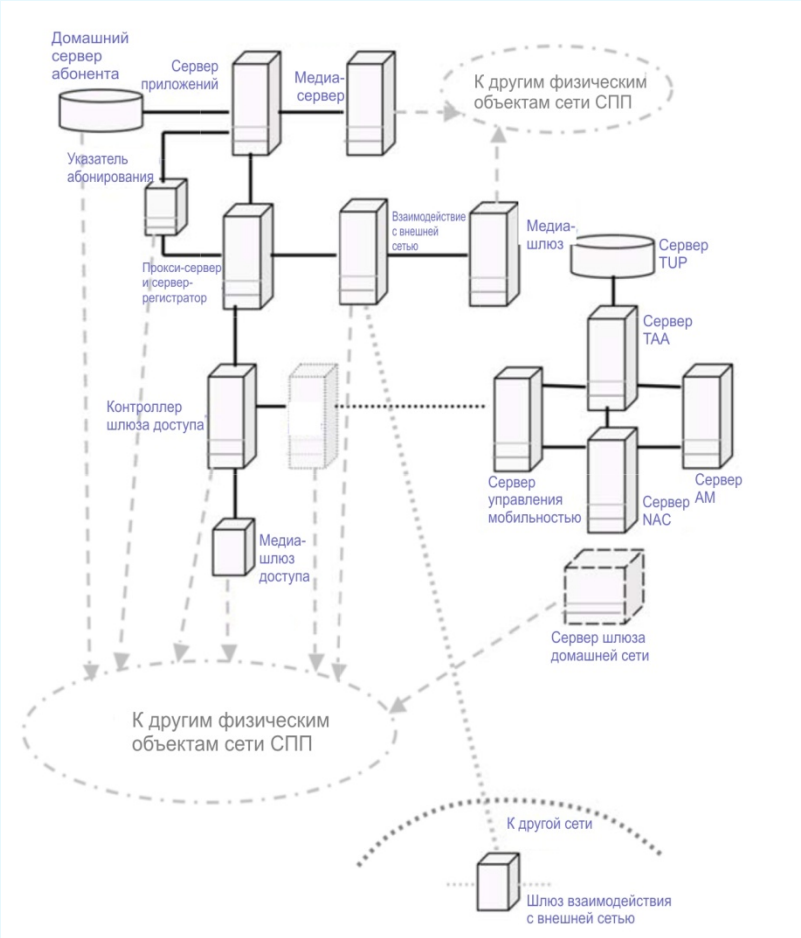
- Ослабление ограничений, связанных с недостаточной полосой пропускания, может привести к тому, что поддержка некоторых функций, которые в настоящее время являются обязательными, станет опциональной (например, сжатие сообщений SIP).
- Различия в управлении для определения местоположения повлияют на различные протоколы, при помощи которых передается данная информация как через интерфейсы сигнализации, так и через биллинговые интерфейсы.
- Различия в процедурах резервирования ресурсов в сетях доступа потребуют внесения изменений в процедуры авторизации и резервирования ресурсов IMS, поскольку процедуры резервирования ресурсов в сетях доступа xDSL должны инициироваться объектом сети (например, P-CSCF для услуг на базе SIP) от имени оконечных пользовательских устройств.

Упомянутые выше расширения изучаются различными организациями по разработке стандартов для обеспечения поддержки использования систем IMS в сетях СПП.

1.2.5 Физическая архитектура СПП

Физическая архитектура СПП идентифицирует физические объекты, соответствующие функциональному объекту или группе функциональных объектов, указанных в обобщенной функциональной архитектуре СПП. Физическая архитектура дает возможность идентифицировать точки функциональной совместимости между физическими объектами для обеспечения такой совместимости между различными физическими объектами в рамках сети СПП. В качестве примера на Рисунке 1-7 приведен один из вариантов реализации СПП с точки зрения физической архитектуры.

Рисунок 1-8: Вариант физической архитектуры СПП



1.3 Пути для перехода к СПП

1.3.1 Рассмотрение вопросов перехода к СПП

В процессе разработки плана перехода к новой инфраструктуре необходимо учитывать множество точек зрения и соображений, так как этот процесс повлияет на многие аспекты, касающиеся соответствующих объектов, а также сообществ. Переход к СПП от существующей инфраструктуры, например КТСОП/ЦСИС, также окажет большое влияние на всю инфраструктуру связи.

Для того чтобы идти в ногу с техническим прогрессом и ожиданиями рынка, необходимо либо регулярное совершенствование систем, либо их замена новыми технологиями, не препятствуя при этом предоставлению услуг. Замена и усовершенствование существующего оборудования с использованием современных и продвинутых технологий требуется не только для предоставления новых услуг; часто время тратится на получение поддержки производителей аппаратного и программного обеспечения. Производители, как правило, предпочитают, чтобы подобные модификации удовлетворяли требованиям технического прогресса, когда устаревшие типы оборудования заменяются более эффективным, компактным и надежным оборудованием, которое должно также обеспечить повышение качества услуг для пользователей.

Предпочтительно, в особенности при расширении услуг в удаленных сельских районах, чтобы переход к СПП не был резким, т. е. и устаревшие, и новые технологии должны сосуществовать в течение некоторого обоснованного периода времени. Что касается потребителей, то они не должны вынужденно заменять оконечное оборудование только потому, что их поставщик услуг произвел "усовершенствование" системы для СПП.

С учетом сказанного в Рекомендации МСЭ-Т Y.2261 приведены руководящие указания по формированию плана перехода для оператора

Что касается перехода от КТСОП/ЦСИС к СПП, следует принимать во внимание аспекты, изложенные далее.

1.3.1.1 Сигнализация и управление

В сетях КТСОП/ЦСИС используются такие системы сигнализации, как сигнализация в аналоговом канале, сигнализация по выделенному каналу (CAS), например системы сигнализации R1 [Q.310–Q.332], R2 [Q.400–Q.490], а также системы сигнализации по общему каналу (CCS), типа SS7 или DSS1 [Q.931]. Все эти системы сигнализации предназначены для сетей с коммутацией каналов. Поскольку транспортировка в СПП основывается на пакетах (а вызов отделен от канала-носителя), могут потребоваться другие подходящие виды сигнализации (например, BICC, SIP-I [Q.1912.5] и т. д.). Кроме того, функция сигнализации и функция управления вызовами могут располагаться в нескольких элементах СПП.

Поскольку СПП должны работать совместно с сетями КТСОП/ЦСИС и другими сетями, необходимо обеспечить взаимодействие между системами сигнализации СПП и системами сигнализации существующих сетей. Аспекты сигнализации в рамках корпоративной сети последующих поколений должны оставаться независимыми от аспектов сигнализации в сети доступа или базовой сети СПП.

В дальнейшем ожидается, что аспекты сигнализации для сетей доступа и базовых сетей должны быть независимыми, для того чтобы обеспечить возможность поэтапного подхода для осуществления перехода к СПП.

1.3.1.2 Административное управление

Система управления СПП состоит из трех плоскостей, а именно: плоскость сетевого управления, плоскость сетевого контроля и плоскость управления услугами. Каждая из этих плоскостей реализует соответствующие управляющие функции для каждого уровня в многоуровневой модели СПП.

Переход системы управления КТСОП/ЦСИС (т. е. эксплуатации, администрирования и управления) требует обеспечения возможности перехода сетей КТСОП/ЦСИС через ряд промежуточных этапов по направлению к СПП.

1.3.1.3 Услуги

Услуги КТСОП/ЦСИС, которые традиционно предоставляются телефонными станциями КТСОП/ЦСИС, в сетях СПП могут предоставляться серверами приложений (AS). Как ожидается, в сетях СПП будут предоставляться некоторые или все существующие услуги. Так как качество голосовой связи в сети КТСОП считается "наилучшим", любой переход от подобной услуги "наилучшего" качества к сетям СПП на основе IP должен сопровождаться гарантией того, что

качество новых услуг будет сравнимо с качеством услуг существующей инфраструктуры класса 5 (или ВРК, т. е. с временным разделением каналов).

Однако при моделировании сетей КТСОП/ЦСИС нет гарантии того, что все услуги смогут быть предоставлены.

Для поддержки существующих сегодня услуг ожидается, что будут использоваться оконечные устройства традиционных типов, подключенные к СПП через адаптеры.

- Услуги передачи данных. При переходе от КТСОП/ЦСИС к СПП необходимо обеспечить непрерывность предоставления услуг передачи данных. Использование СПП для подключения сетей КТСОП/ЦСИС должно быть прозрачным для всех услуг передачи данных. В сетях СПП должно быть обеспечено такое же или более высокое качество обслуживания (QoS) для услуг передачи данных на базе КТСОП/ЦСИС.
  - Моделирование КТСОП/ЦСИС обеспечивает функциональные характеристики, которые схожи, но не идентичны существующим услугам передачи данных в сетях КТСОП/ЦСИС.
  - Эмуляция сетей КТСОП/ЦСИС должна давать возможность предоставления полного комплекса услуг передачи данных, предоставляемых сетями КТСОП/ЦСИС. Однако не требуется, чтобы сети СПП поддерживали все услуги передачи данных узкополосной сети У/ЦСИС, определенных в Рекомендациях МСЭ-Т серии I.230.
- Дополнительные услуги. При переходе от КТСОП/ЦСИС к СПП должна быть обеспечена непрерывность предоставления дополнительных услуг, насколько это практически возможно. Эмуляция сетей КТСОП/ЦСИС должна обеспечивать поддержку для всех дополнительных услуг, предоставляемых сетями КТСОП/ЦСИС, хотя моделирование КТСОП/ЦСИС обеспечивает функциональные характеристики, схожие, но не идентичные существующим услугам сетей КТСОП/ЦСИС. В целях СПП не обязательно должны поддерживаться все дополнительные услуги ЦСИС, определенные в Рекомендациях МСЭ-Т серии I.250. Сети СПП должны казаться прозрачными, когда они используются для подключения дополнительных услуг между сетями КТСОП/ЦСИС.
- Эксплуатация, управление и техническое обслуживание (OAM). Функции OAM используются для проверки качественных показателей сети, а также для сокращения эксплуатационных расходов за счет сведения к минимуму перерывов в обслуживании, улучшения качества обслуживания и сокращения периодов эксплуатационных простоев. При переходе от КТСОП/ЦСИС к СПП должна быть обеспечена, как минимум, возможность обнаружения неисправностей, дефектов и сбоев, таких как потерянные пакеты, пакеты с ошибками или неверно вставленные пакеты. Кроме того, должны существовать механизмы отображения статуса возможности подключения и обеспечиваться поддержка контроля качественных показателей.
- Наименование, нумерация и адресация. Схемы наименования, нумерации и адресации СПП в соответствии с Рекомендацией МСЭ-Т Y.2001 должны иметь возможность взаимодействия с существующей схемой нумерации E.164. В процессе перехода от КТСОП/ЦСИС к СПП необходимо обеспечить полную поддержку суверенитета Государств – Членов МСЭ в отношении планов нумерации, наименования, адресации и идентификации кодов стран. Кроме того, как минимум должна существовать поддержка схем IP-адресации интернета, включая телефонные унифицированные идентификаторы ресурса согласно E.164 (TEL URI), например тел.: +98 765 4321, и/или унифицированные идентификаторы ресурса SIP (SIP URI), например sip:my.name@company.org.
- Учет, начисление платы и выставление счетов. В течение переходного периода может потребоваться поддержка существующих процедур учета, начисления платы и выставления счетов, насколько это практически возможно. Переход от существующих сетей к СПП также предполагает замену существующих источников формирования данных учета. В сетях СПП должны поддерживаться механизмы начисления платы как в автономном режиме, так и в режиме он-лайн.

- Взаимодействие. Термин "взаимодействие" используется для описания процесса обмена данными между сетями, между оконечными системами или между их частями с целью предоставления функционального объекта, способного поддерживать сквозную связь. При переходе от КТСОП/ЦСИС к СПП необходимо учитывать следующие аспекты:
  - возможность взаимодействия с существующими сетями, такими как КТСОП/ЦСИС и интернет;
  - возможность взаимодействия с сетями на базе IMS или с сетями на базе серверов вызова;
  - возможность междоменного, межзонового и межсетевого взаимодействия;
  - поддержка аутентификации и авторизации;
  - возможность осуществления управления допуском вызова;
  - способность поддерживать параметры качества работы сети, как определено в [Y.1541];
  - поддержка учета, начисления платы и выставления счетов.
- Маршрутизация вызовов. При сосуществовании СПП с КТСОП/ЦСИС схема маршрутизации должна обеспечивать операторам контроль данных о том, где их трафик входит и выходит из СПП. Это даст возможность оператору оптимизировать использование ресурсов своих сетей и избежать появления нескольких точек взаимодействия между СПП и КТСОП/ЦСИС на линии передачи данных.
- Требования по обслуживанию со стороны национальных регуляторных органов. В случае взаимодействия поставщик услуг СПП обязан соблюдать следующие требования, установленные национальными/региональными нормативными документами или законодательством:
  - базовые услуги телефонной связи с тем же или лучшим качеством и готовностью, как и в существующих сетях КТСОП/ЦСИС;
  - возможность точного начисления платы и учета;
  - возможность сохранения номера при смене оператора;
  - доступность телефонной справочной службы для пользователей сетей КТСОП/ЦСИС и СПП;
  - поддержка электросвязи в чрезвычайных ситуациях;
  - поддержка для всех пользователей, в том числе для лиц с ограниченными возможностями. Такая поддержка должна предоставлять по крайней мере те же возможности, что и в существующих сетях КТСОП/ЦСИС. Сети СПП обеспечивают возможности более продвинутой поддержки, например способность сети преобразовывать текст в речь;
  - механизмы поддержки законного перехвата и контроля сигналов различных медийных типов электросвязи, таких как передача голоса, данных и видео, электронная почта, обмен сообщениями и т. д. Такой механизм может потребоваться поставщику сетевых услуг для предоставления доступа органам охраны правопорядка (LEA) к контенту электросвязи (CT) и сведениям, полученным в результате перехвата данных (IRI), в целях удовлетворения требований администраций и международных договоров;
  - функциональная совместимость между СПП и другими сетями, например КТСОП/ЦСИС и сети сухопутной подвижной связи общего пользования (PLMN).

1.3.2 Общая процедура перехода

Переход от одной инфраструктуры к другой не является легкой или простой задачей, поскольку включает множество вопросов, которые необходимо рассматривать с различных точек зрения.

Переход к сетевой инфраструктуре следует планировать с особой тщательностью, исследуя различные аспекты. В качестве вывода можно отметить, что не существует единого или наилучшего пути перехода к СПП, поскольку переход должен основываться на ситуации в каждой стране и на условиях, определяемых каждым оператором.

Для разработки плана перехода от существующей сетевой инфраструктуры к СПП рекомендуется учитывать следующую процедуру.

1 Предоставление новых услуг связи для пользователей широкополосной связи в дополнение к услугам существующей сети.

2 Значительная часть пользователей переключается на эти услуги, что приводит к заметному реальному сокращению использования сетей КТСОП/ЦСИС.

3 Расходы на параллельное обслуживание обеих систем становятся важным фактором. **Решение о начале замены инфраструктуры**.

4 Замена части инфраструктуры (например, местного коммутатора) элементами новой инфраструктуры, **не вынуждая всех пользователей переходить на новую инфраструктуру**.

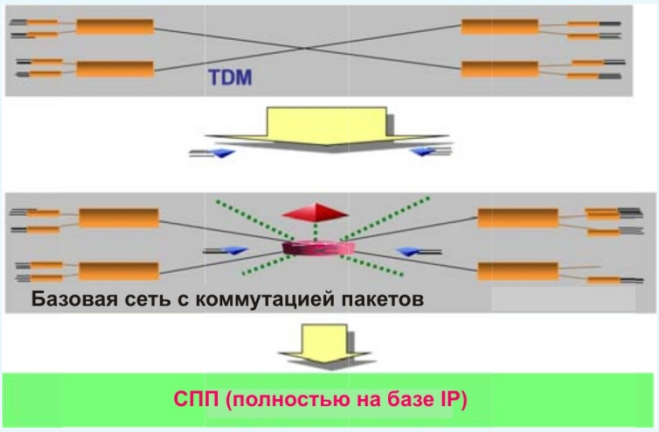
5 Полный переход на новую инфраструктуру.

6 Переход оставшихся пользователей на СПП.

1.3.3 Общий путь перехода

Результатом перехода должна стать "среда, полностью базирующаяся на IP", которая является ключевой технологией СПП, и поэтому с технической точки зрения переход должен рассматриваться как замена сетей "на базе технологии TDM" сетями "на базе IP". Учитывая, что каждая страна владеет участками между "доменом сети доступа" и "доменом базовой сети", процедура перехода должна в первую очередь применяться к одному из таких доменов. В целом считается, что проще разработать план перехода для "домена базовой сети". Базовый переход будет оказывать меньшее влияние на предоставление услуг по сравнению с переходом к "домену сети доступа". На Рисунке 1-9 приведен общий вид перехода базовой сети к СПП.

Рисунок 1-9: Общий вид перехода базовой сети к СПП

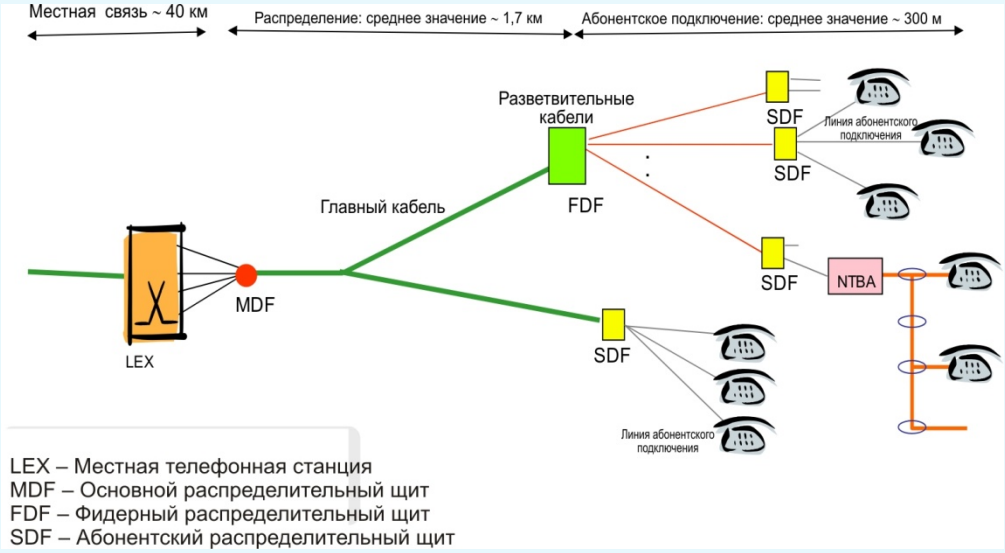


В случае с доменом сети доступа, при котором могут возникать довольно сложные ситуации не только из-за технических аспектов, но и из-за географических различий, не рекомендуется выбирать какую-то конкретную технологию для замены любых существующих систем сетей доступа. Вместо этого рекомендуется рассмотреть вопрос о согласованном использовании различных технологий в целях удовлетворения запросов клиентов более гибким и экономичным способом. Разрабатывается множество разнообразных технологий доступа, использующих фиксированную и подвижную связь с поддержкой широкополосных соединений. Большинство технологий также

обеспечивают возможность IP-соединений, что является важнейшей технической характеристикой, необходимой для удовлетворения требованиям СПП (например, передача на основе пакетов).

Что касается сетей доступа на базе фиксированной связи, в настоящее время для обеспечения широкополосной связи в основном используется технология xDSL. Конечной целью в сети фиксированной связи станет развертывание инфраструктуры на основе волоконно-оптических линий. xDSL дает возможность максимального использования существующей инфраструктуры доступа на основе медного кабеля для развертывания широкополосной инфраструктуры экономичным способом, но с ограниченной пропускной способностью (максимум несколько десятков мегабитов в секунду). Волоконная оптика является своего рода целевой технологией в области сетей фиксированной связи с неограниченной пропускной способностью не только для базовых сетей, но и сетей доступа, включая также домашние сети. Проблемы здесь связаны лишь с затратами и сложностью прокладки кабелей. Осуществляя быстрое развитие технологий, придется столкнуться с обеими проблемами. Поэтому рекомендуется использовать как xDSL, так и волоконную оптику совместно в сети доступа в качестве подготовки перехода к СПП, включая обеспечение достаточной для широкополосной связи пропускной способности. Ниже, на Рисунке 1-10, приведен пример построения сетей доступа с учетом географических расстояний.

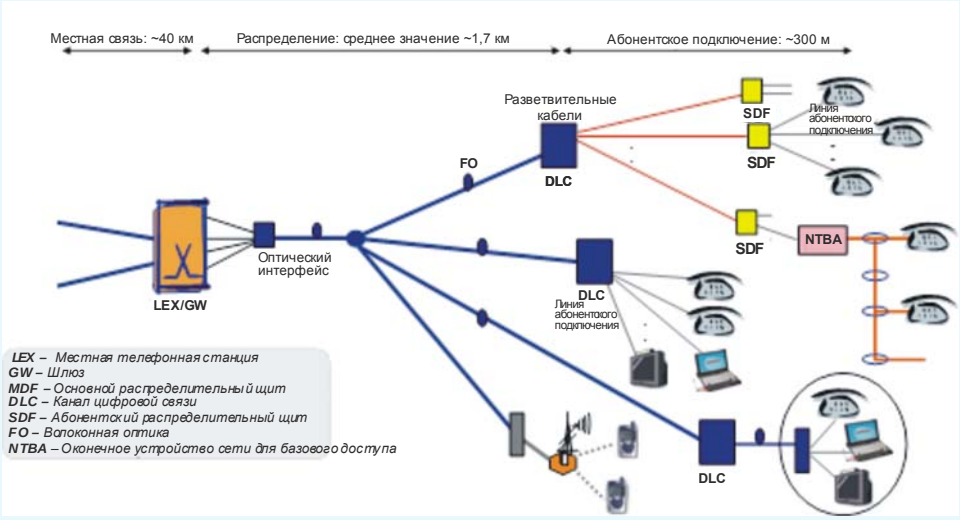
Рисунок 1-10: Общий вид перехода сети доступа (фиксированной) к СПП



Еще одним важным направлением должно стать использование технологий подвижной связи (в том числе беспроводных, таких как Wi-Fi и WiMAX) для обеспечения возможности широкополосных соединений. Этот аспект также очень важен, поскольку многие люди, особенно в развивающихся регионах, используют мобильные телефоны для связи в своей повседневной жизни, обеспечивая людям мобильность. Существует множество технологий, предоставляющих возможность широкополосных соединений в сетях мобильного доступа, включая IP-соединения, однако все еще имеются определенные ограничения по предоставляемой полосе пропускания (около 10 Мбит/с). Организации по разработке стандартов трудятся над созданием технологий для обеспечения большей пропускной способности, однако для этого потребуется время. Ниже, на Рисунке 1-11, приведена диаграмма с примером того, как различные технологии подвижной связи используются в сетях доступа, а на Рисунке 1-12 показана смешанная схема подвижной и фиксированной связи.

Рисунок 1-11: Применения различных технологий мобильного доступа

Рисунок 1-12: Общий вид перехода сети доступа (смешанной) к СПП



1.3.4 Технология СПП, предназначенная для поддержки перехода

Для поддержки перехода от существующих сетей к СПП, по крайней мере для голосовых услуг, сеть СПП предоставляет две возможности. Одна из них – это эмуляция, поддерживающая предоставление возможностей и интерфейсов услуг КТСОП/ЦСИС, используя адаптацию к инфраструктуре СПП при помощи IP. Другая – это моделирование, которое поддерживает предоставление возможностей услуг, подобных КТСОП/ЦСИС, с использованием управления сеансами связи через интерфейсы и инфраструктуру IP.

1.3.4.1 Сценарий эмуляции

Ниже, на Рисунке 1-13 приведена схема сценария эмуляции высокого уровня. Используя возможность эмуляции СПП, которая обеспечивает функцию адаптации (ADF), существующие оконечные устройства, такие как "черные телефоны", подключаются к сети СПП и пользуются их услугами с учетом следующих аспектов:

- процесса инкапсуляции;
- всех услуг, доступных для пользователей КТСОП/ЦСИС;
- опыта, присущего пользователю, не изменяющегося в результате преобразования сети.

Рисунок 1-13: Эмуляция КТСОП/ЦСИС в сетях СПП

1.3.4.2 Сценарий моделирования

Моделирование служит для предоставления пользователям СПП услуг наподобие КТСОП/ЦСИС. Поэтому используя возможности моделирования, пользователи СПП будут связываться с пользователями КТСОП/ЦСИС.

Ключевые особенности моделирования СПП формулируются следующим образом:

- наличие услуг, подобных КТСОП/ЦСИС;
- возможное наличие новых услуг;
- опыт, присущий пользователю, не изменяется в результате преобразования сети.

Рисунок 1-14: Сценарий 1 моделирования КТСОП/ЦСИС в сетях СПП

Рисунок 1-15: Сценарий 2 моделирования КТСОП/ЦСИС в сетях СПП

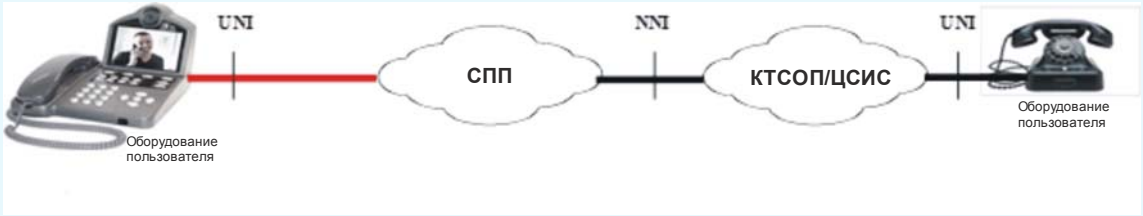
1.3.4.3 Взаимодействие с использованием эмуляции и моделирования

С учетом важности услуг передачи голоса услуги СПП, ориентированные на передачу голоса, должны быть связаны с услугами передачи голоса в среде КТСОП/ЦСИС. Для поддержки этого требования эмуляция и моделирование используются совместно в целях взаимодействия между СПП и существующими сетями, такими как КТСОП/ЦСИС. В зависимости от ситуации с взаимодействием будет принято решение о том, в какой области какая технология будет использована.

На Рисунке 1-16 приведен пример взаимодействия между СПП и существующими сетями КТСОП/ЦСИС. На стороне СПП применяется моделирование, в то время как при взаимодействии со стороной существующих сетей используется эмуляция. Особенности предоставления услуг в данном случае можно охарактеризовать следующим образом:

- необходимо взаимодействие между услугами СПП и КТСОП/ЦСИС;
- наличие только услуг, подобных КТСОП/ЦСИС;
- опыт конечного пользователя существующих сетей не может быть применен для сквозного соединения.

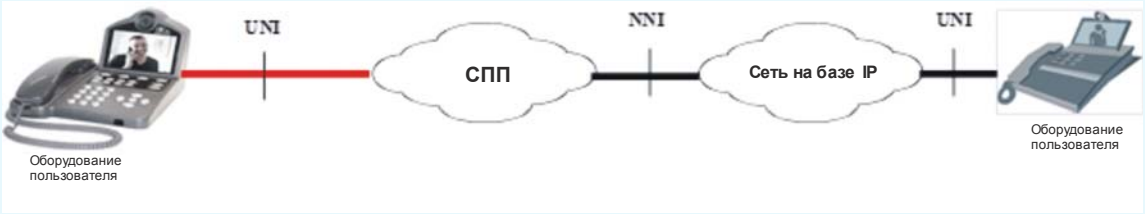
Рисунок 1-16: Схема взаимодействия 1между эмуляцией и моделированием СПП



Ниже, на Рисунке 1-17 показан еще один пример взаимодействия между СПП и существующей сетью на базе IP с поддержкой услуг по передаче голоса (например, VoIP). На стороне СПП применяется моделирование, в то время как при взаимодействии со стороной существующих сетей используется эмуляция. Особенности предоставления услуг в данном случае можно охарактеризовать следующим образом:

- необходимо взаимодействие между услугами СПП и сетью на базе IP;
- опыт пользователей как СПП, так и сетей на базе IP может не соответствовать варианту сквозных соединений.

Рисунок 1-17: Схема взаимодействия 2 между эмуляцией и моделированием СПП



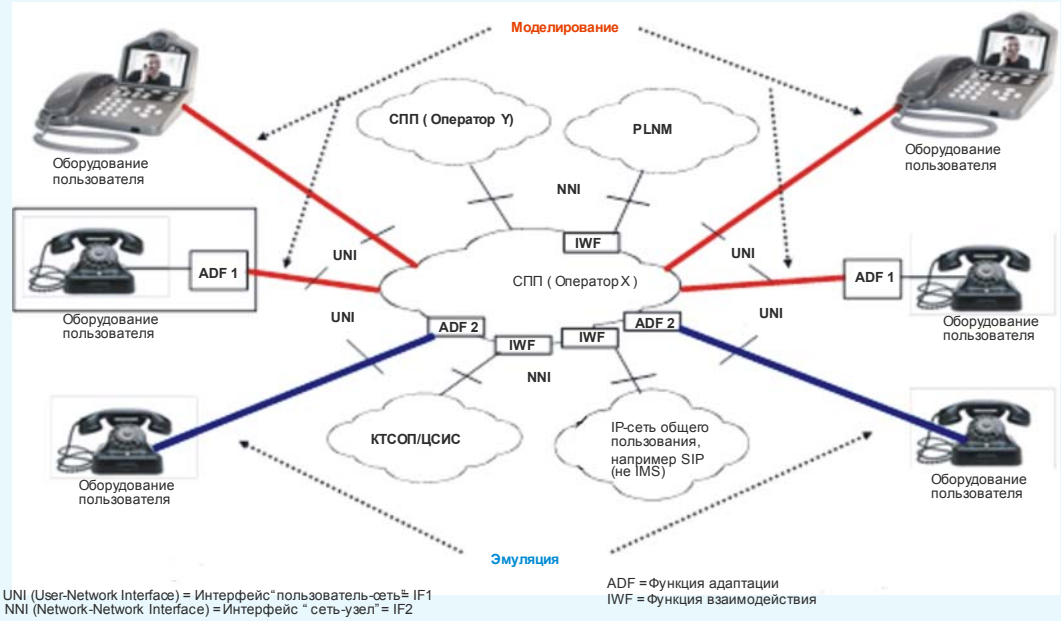
1.3.4.4 Общая конфигурация использования имитации и моделирования

Ключевым требованием технологии эмуляции и моделирования является поддержка услуг по передаче голоса. КТСОП/ЦСИС в настоящее время является основной сетевой инфраструктурой для

поддержки услуг по передаче голоса, включая различные дополнительные услуги, особенно в случае ЦСИС. Кроме того, наблюдается непрерывный рост количества конечных пользователей услуг по передаче голоса в существующей IP-среде.

Поэтому для того чтобы охватывать сети КТСОП/ЦСИС и сети на базе IP, СПП должны поддерживать свои возможности по передаче голоса, такие как эмуляция и моделирование. Таким образом, сочетание этих возможностей с соответствующими сценариями взаимодействия поможет поддержать потребности конечных пользователей в услугах по передаче голоса, если их устройства подключены к сетям фиксированной подвижной и существующей сети на базе IP, для того чтобы предоставлять услуги по передаче голоса независимо от местонахождения конечного пользователя. Ниже, на Рисунке 1-18 приведена модель общей конфигурации использования эмуляции и моделирования с указанием комбинированной ситуации взаимодействия.

Рисунок 1-18: Общий вид использования эмуляции и моделирования СПП



1.3.4.5 Сервер вызова, поддерживающий переход к СПП

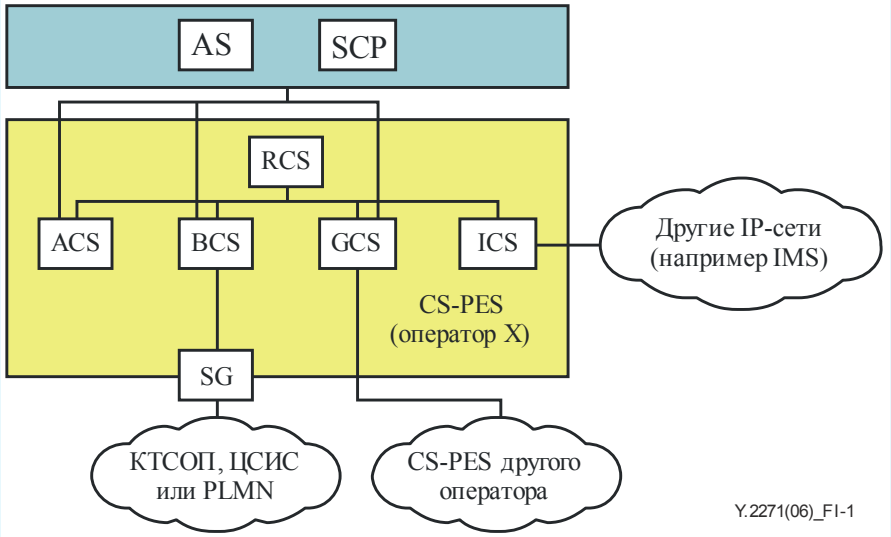
Сервер вызова является ключевым элементом в процессе эмуляции КТСОП/ЦСИС, который отвечает за управление вызовами, управление шлюзами, управление медиаресурсами, маршрутизацию, профиль пользователей, а также аутентификацию, авторизацию абонентов и учет. Сервер вызова может предоставлять базовые и дополнительные услуги КТСОП/ЦСИС, а также дополнительные услуги через взаимодействие услуг с внешним узлом управления услугами (SCP) и/или сервером приложений на уровне услуг/приложений.

Сервер вызова может работать в одном или в нескольких из следующих режимов, как определено в Рекомендации МСЭ-Т Y.2271. На Рисунке 1-19 приведен пример развертывания сервера:

- сервер вызова доступа (ACS) – для осуществления функций управления шлюзами доступа и управления медиаресурсами, обеспечивая тем самым предоставление базовых и дополнительных услуг КТСОП/ЦСИС;

- коммутационный сервер вызова (BCS) – для реализации функций взаимодействия, чтобы обеспечить подключение к сетям КТСОП/ЦСИС;
- сервер вызова IMS (ICS) – для обеспечения функциональной совместимости между компонентами эмуляции КТСОП/ЦСИС и мультимедийными компонентами на базе IP в пределах одного домена СПП;
- сервер вызова шлюза (GCS), – для обеспечения функциональной совместимости между разными доменами СПП от различных поставщиков услуг;
- сервер вызова, выполняющий маршрутизацию (RCS) – для обеспечения функций маршрутизации между серверами вызова.

Рисунок 1-19: Пример развертывания сервера вызова

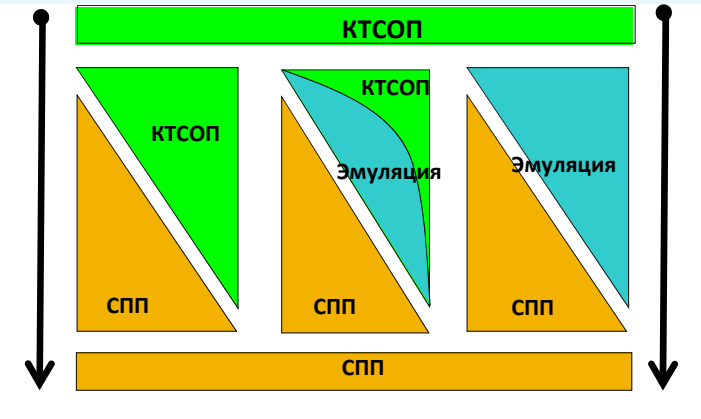


Примечание: AS – сервер приложения; SCP – узел управления услугами; SG – шлюз сигнализации, PES – компонент эмуляции услуг КТСОП.

1.4 Сценарии перехода

При использовании эмуляции и/или моделирования СПП имеются различные пути перехода от существующих сетей к СПП. Этот вопрос следует решать в зависимости от ситуации в каждой стране или от положения поставщика услуг. В настоящем отчете в качестве основы для рассмотрения представлены три различных типа сценариев перехода, однако не следует исключать и другие возможности. Ниже, на Рисунке 1-20 приведено графическое представление трех указанных типов перехода от КТСОП/ЦСИС к СПП.

Рисунок 1-20: Общие сценарии перехода



Существуют следующие три сценария:

- Сценарий с наложением (Рисунок 1-20, левая сторона). Сети СПП будут развертываться и функционировать совместно с КТСОП/ЦСИС. СПП будут занимать все более возрастающую долю, в то время как доля КТСОП/ЦСИС будет постоянно сокращаться, пока наконец не произойдет полный переход к СПП.
- Сценарий с заменой (Рисунок 1-20, правая сторона). Эмуляция СПП будет широко использоваться для поддержки услуг по передаче голоса, однако существующие оконечные устройства, такие как "черный телефон", будут продолжать эксплуатироваться. Таким образом, конечный пользователь не заметит замену технологии, на основе которой работает его аппарат.
- Смешанный сценарий (Рисунок 1-20, средняя часть). В этом сценарии используются как наложения, так и эмуляция, поэтому вначале некоторые из подключений пользователей к КТСОП будут заменяться эмуляцией СПП, в то время как другие пользователи КТСОП сохранят свои подключения к КТСОП. А по мере дальнейшего развертывания сетей СПП пользователи эмуляции и КТСОП будут заменяться пользователями СПП.

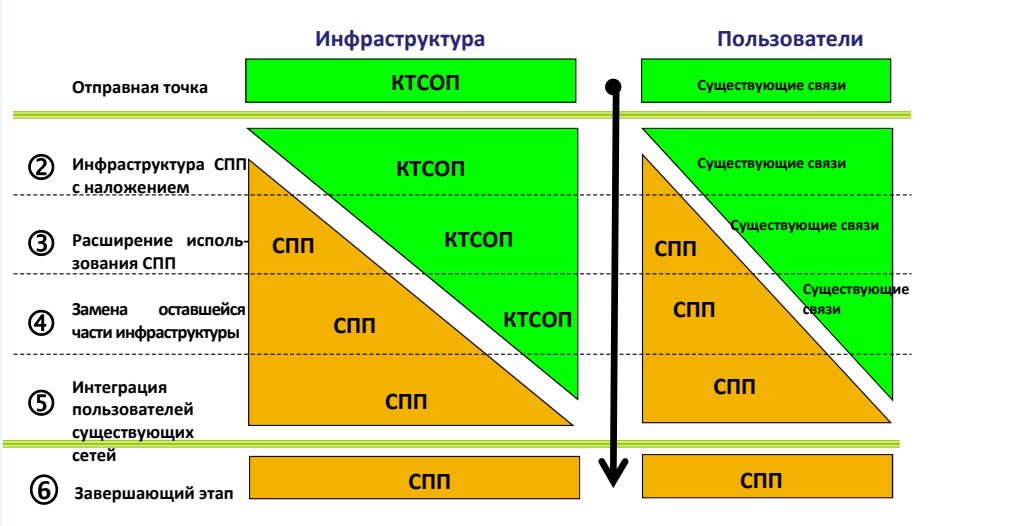
1.4.1 Сценарий с наложением

Сценарий с наложением целесообразно использовать для страны или оператора, которые уже имеют стабильную или новую инфраструктуру КТСОП/ЦСИС. В данном случае трудно обосновать замену всего оборудования КТСОП/ЦСИС на СПП, поскольку эта существующая инфраструктура еще не окупила вложенные в нее средства. А сама инфраструктура находится в довольно хорошем состоянии и сможет использоваться в течение нескольких последующих лет без каких-либо серьезных затрат на эксплуатацию, управление и техническое обслуживание, включая устранение сбоев.

Согласно этому сценарию оператор сможет постепенно подготовить в достаточном объеме ресурсы для последующего инвестирования, продолжая в то же время предоставлять услуги своим клиентам. Кроме того, оператор также сможет удовлетворять потребности пользователей, которые используют расширенные возможности за счет вновь развернутых СПП. Далее по мере увеличения числа клиентов, желающих использовать улучшенные возможности, оператор будет расширять зону покрытия СПП, тем самым сокращая число пользователей существующих сетей. В конечном счете сети СПП будут развернуты полностью и охватят всех пользователей. В этом случае пользователи СПП будут соединяться с пользователями КТСОП/ЦСИС при помощи своего

моделирования, однако через взаимодействие между сетями СПП и КТСОП/ЦСИС. Ниже, на Рисунке 1-21 показаны этапы этого сценария.

Рисунок 1-21: Сценарий перехода с наложением

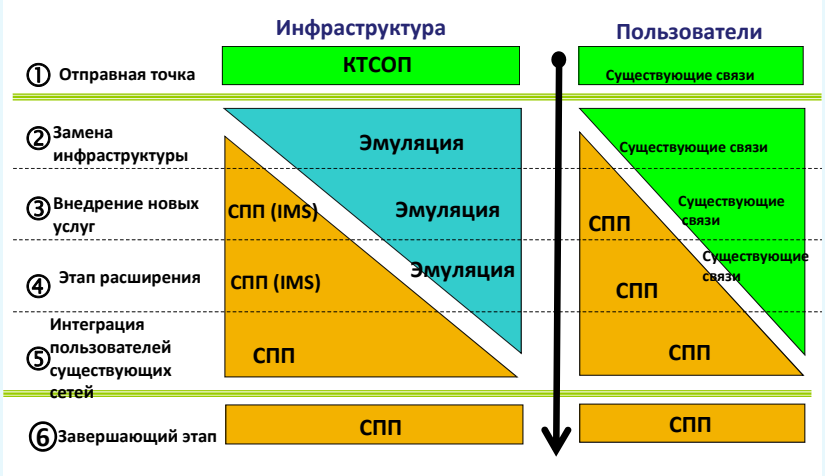


1.4.2 Сценарий с заменой инфраструктуры

Данный сценарий будет полезен для страны или оператора, которые не имеют достаточно развитой инфраструктуры КТСОП/ЦСИС и которые испытывают нехватку возможностей подключения для поддержки услуг по передаче голоса. В таком случае продолжать развертывание оборудования КТСОП/ЦСИС затруднительно, поскольку для этого потребуются новые инвестиции наряду с необходимостью инвестиций для СПП. Однако в этом случае существующие абоненты даже при использовании КТСОП/ЦСИС будут получать постоянную поддержу без замены своих оконечных устройств, если это возможно.

Согласно данному сценарию оператор прекратит процесс развертывания сетей КТСОП/ЦСИС, а вместо этого инвестирует средства в СПП. Затем оператор предоставляет существующим пользователям КТСОП/ЦСИС функцию адаптации (ADF) для обеспечения непрерывного использования услуг по передаче голоса, что означает расширение возможностей эмуляции СПП, как показано на Рисунке 1-22. Далее по мере увеличения числа клиентов, желающих использовать улучшенные возможности, оператор будет расширять зону покрытия СПП, тем самым сокращая число пользователей услуг эмуляции. В конечном счете все пользователи будут полностью охвачены услугами СПП. Ниже, на Рисунке 1-22 показаны этапы этого сценария.

Рисунок 1-22: Сценарий перехода с заменой инфраструктуры

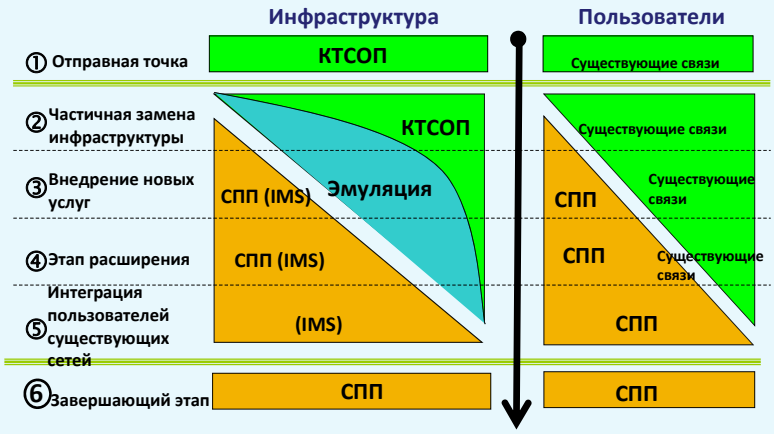


1.4.3 Смешанный сценарий

Дани сценарий будет полезен для страны или оператора, которые находятся на промежуточном этапе, т. е. некоторая часть сетей КТСОП/ЦСИС требует замены, а другая часть находится в хорошем и стабильном состоянии, используя новую инфраструктуру КТСОП/ЦСИС. В этом случае следует учитывать положения сценариев как с наложением, так и с заменой. Иными словами, оператор должен сохранять сети КТСОП/ЦСИС с соответствующими клиентами до тех пор, пока не окупятся его инвестиции или пока состояние сетей КТСОП/ЦСИС не потребует серьезных затрат на эксплуатацию, управление и техническое обслуживание, включая устранение сбоев, при этом для замены потребуется время. В другом случае оператор приступит к развертыванию инфраструктуры СПП, заменяя ту часть сетей КТСОП/ЦСИС, которая нуждается в замене. На Рисунке 1-23 показаны этапы этого сценария.

Согласно данному сценарию оператор постепенно подготовит достаточный объем ресурсов для следующего нового инвестирования и в то же время сохранит своих клиентов в сетях КТСОП/ЦСИС. Кроме того, оператор также сможет удовлетворять потребности пользователей, которые используют улучшенные возможности за счет вновь развертываемых СПП. Далее по мере увеличения числа клиентов, желающих использовать улучшенные возможности, оператор будет расширять зону покрытия СПП, тем самым сокращая число пользователей существующих сетей. Окончательным решением станет полномасштабное развертывание СПП для охвата всех пользователей.

Рисунок 1-23: Mixed migration scenario



2 Развитие технологий, способствующих переходу к СПП

За последние 10 или более лет наблюдается все более ускоряющийся процесс интеграции в области информации и связи как по оборудованию, так и по сетям. Операторы традиционных сетей общего пользования отметили снижение телефонного трафика в своих коммутируемых сетях электросвязи общего пользования, отчасти из-за роста популярности мобильных телефонов и перехода от услуг телефонных сетей к услугам доступа в интернет общего пользования.

В течение последних нескольких лет разработана концепция новой интегрированной широкополосной сети, получившая название "сети последующих поколений" – СПП.

Основные характеристики СПП могут быть определены на основе проблем, стоящих перед операторами сетей: необходимость предоставления услуг по широкополосным каналам (для увеличения доходов); необходимость объединения разнообразных сетевых услуг – передача данных (веб-навигация), аудиоуслуга, телефония, мультимедийные и новейшие "популярные" интернет-услуги, такие как мгновенный обмен сообщениями и услуги присутствия, широковещательные услуги, а также желание клиентов иметь возможность доступа к своим услугам из любой точки мира (встроенная мобильность). Вместо того чтобы пытаться решить конкретные проблемы с помощью той или иной сети (например, КТСОП), для следующего поколения необходимо было сформировать систему сетей, поддерживающих гибкую платформу для предоставления услуг.

2.1 Аспекты обслуживания

Понимание потребностей в услугах должно стать первым шагом для всех разработок в области электросвязи, и в связи с этим определение характеристик среды должно производиться на начальном этапе идентификации услуг. Развитие процессоров, наращивание их вычислительной способности и тот факт, что полупроводниковая технология создает устройства, достаточно малые, чтобы монтировать их на платах, приводит к требованиям использовать мультимедийные услуги различными способами, для которых необходимо широкополосное соединение в сетях фиксированной или подвижной связи.

В таблице 2-1 приведены высокоуровневые показатели требований, предъявляемых к среде передачи с точки зрения ширины полосы пропускания и качества обслуживания (QoS). Для многих услуг, за исключением обычных услуг по передаче голоса, необходима полоса пропускания не менее 2 Мбит/с режимом высокого приоритета для удовлетворения требованиям QoS. Для поддержания этой тенденции по оказанию услуг настоятельно требуется, чтобы сети имели

достаточные возможности для работы с таким трафиком (например, сеансы связи, потоки и т. д.), предоставляли бы широкополосное соединение с запасом и хорошим управлением. СПП являются одним из способов удовлетворения этих требований на уровне класса оператора, но управляемым способом.

Таблица 2-1: Требования к мультимедийным услугам

Услуга	Полоса пропускания (нисходящий канал)	Требования к качеству обслуживания (QoS)
Широковещательное телевидение (MPEG-2)	от 2 до 6 Мбит/с	Параметризована
ТВЧ (MPEG-4)	от 6 до 12 Мбит/с	Параметризована
PPV или NVoD	от 2 до 6 Мбит/с	Имеет приоритет
VoD	от 2 до 6 Мбит/с	Имеет приоритет
Картинка в картинке (MPEG2)	вплоть до 12 Мбит/с	Параметризована
PVR	от 2 до 6 Мбит/с	Имеет приоритет
Интерактивное телевидение	вплоть до 3 Мбит/с	Лучший из возможного
Высокоскоростной доступ к интернету	от 3 до 10 Мбит/с	Лучший из возможного
Видеоконференция	от 300 до 750 кбит/с	Имеет приоритет
Голосовая/видеотелефония	от 64 до 750 кбит/с	Имеет приоритет

2.2 Технология доступа к транспортной среде

Как объяснялось выше, для поддержки различных видов мультимедийных услуг требуется, чтобы сети обладали достаточной пропускной способностью и возможностями для управления трафиком. Обеспечение требуемой ширины полосы пропускания является отправной точкой соответствия этим требованиям к услугам (и среде). Существуют две концепции обеспечения полосы пропускания – по сетям фиксированной связи и по сетям подвижной связи.

Сети подвижной связи все еще находятся в процессе развития. Предоставляя выигрыш в мобильности, подвижная связь является ключевым средством доступа для путешествующих пользователей, таких как бизнесмены, студенты и т. д., которые могут пользоваться возможностью соединения в любом месте, где бы они не находились

В последние годы значительно увеличился интерес к приложениям беспроводной связи в диапазонах частот между 57 и 134 ГГц благодаря возможности использования широкополосной связи, что соответствует растущим требованиям к приложениям с высокой скоростью передачи данных в диапазоне сотен мегабитов в секунду, включая возможности соединений "последней мили". В этих диапазонах можно ожидать появления различных конфигураций линий связи на короткие расстояния, в том числе систем высокой плотности.

В настоящее время доступны беспроводные решения в диапазонах 60/70/80/95 ГГц, однако по стоимости эти системы еще не могут конкурировать с более низкочастотными технологиями. В этих диапазонах частот все еще существуют проблемы, связанные с разработкой. Для того чтобы системы, работающие в диапазонах 60/70/80/95/120 ГГц, могли конкурировать с более низкочастотными системами, количество введенных в эксплуатацию систем подобного рода должно быть очень велико.

Высокие рабочие частоты в диапазонах 60/70/80/95/120 ГГц позволяют конструировать антенны небольшого размера с высоким коэффициентом усиления и направленным излучением. Следовательно, для устройств связи, находящихся в непосредственной близости, действующие

антенны могут быть предназначены для формирования радиосетей из мелких ячеек с минимальными помехами.

Примеры наружного/внутреннего применения, в которых могут использоваться преимущества диапазонов 60/70/80/95/120 ГГц:

- беспроводные локальные сети (WLAN) и беспроводные персональные сети (WPAN);
- микросотовая архитектура и архитектура с повторным использованием частот, например фиксированные линии для подвижной связи;
- мультимедийные услуги с высоким разрешением для кочевых пользователей;
- беспроводные системы распределения видеосигналов;
- линии беспроводной связи, обслуживающие подземные туннели и большие конференц-залы;
- линии беспроводной связи со скоростью передачи данных до 10 Гбит/с и выше.

Использование диапазонов 60/70/80/95/120 ГГц имеет, в числе прочих, следующие преимущества:

- повторное использование частот в областях с высокой плотностью застройки со сниженным потенциалом возникновения нежелательных помех;
- использование антенны меньшего размера (коэффициент усиления антенны пропорционален размеру антенны и длине волны);
- радиооборудование малых размеров для применения кочевыми пользователями;
- антенны с узким лучом (ширина луча антенны обратно пропорциональна рабочей частоте), что позволяет уменьшить помехи и применить повторное использование частот;
- потенциальная возможность совместного использования частот с другими службами радиосвязи;
- поддержка передач с высокой пропускной способностью благодаря использованию более широкой полосы пропускания (закон Шеннона).

К недостаткам данных полос частот относятся:

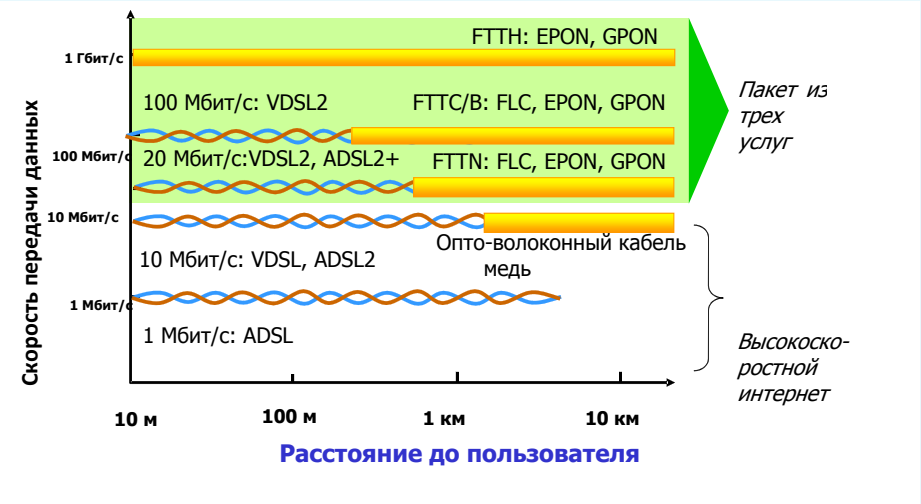
- помеха для сигнала, создаваемая объектом или человеком;
- поглощение в кислороде в диапазоне 60 ГГц;
- восприимчивость к отказам в регионах с сильными дождями и снегопадами;
- непригодность для передач на дальние расстояния.

В сетях фиксированной связи услуги предоставляются по технологии xDSL, которая является весьма популярной технологией широкополосного доступа в мире (действительно наилучшей технологией сегодня для создания широкополосных сетей), широкополосные оптоволоконные сети в настоящее время развертываются в различных странах в виде FTTC (оптоволокно до распределительного шкафа) и FTTH (оптоволокно до дома). С развитием сетей PON (пассивных оптических сетей), скорость 100 Мбит/с теперь экономически эффективна и доступна для всех. Таким образом, во многих развитых странах для пользователей-бизнесменов, а также некоторым домашним пользователям услуги предоставляются по волоконно-оптическим сетям.

Как показано на Рисунке 2-1, технология на основе волоконной оптики обеспечивает доступ на более протяженные расстояния, чем существующие сети, имеющие достаточную полосу пропускания. Эта возможность в значительной степени расширяет географию предоставления широкополосных соединений в том числе в сельских районах. В особенности сочетание волоконных линий с линиями xDSL позволяет обеспечить экономически эффективное предоставление конечным пользователям широкополосных услуг на все более дальних

расстояниях, сохраняя при этом широкополосные функциональные возможности, например, FTTC с VDSL, что обеспечивает скорость 30 Мбит/с для отдельного домохозяйства.

Рисунок 2-1: Развитие технологии передачи данных

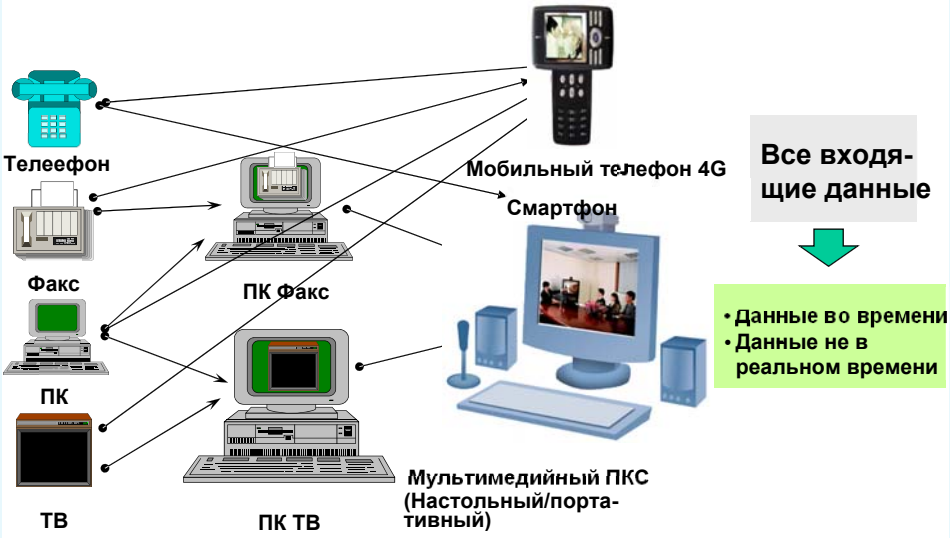


2.3 Совершенствование оконечных устройств

Благодаря развитию технологий обработки оконечные устройства претерпели значительные изменения и продолжают совершенствоваться. За последние 10 лет оконечные устройства, особенно портативные компьютеры и мобильные телефоны, включая смартфоны (например, КПК), сохраняют ведущую роль среди большинства достижений в развитии услуг электросвязи. Главными ключевыми направлениями этого развития являются портативность и интеллектуальность.

Как показано на Рисунке 2-2, функции существующих терминалов для графических, текстовых и видеоприложений интегрируются в одном физическом устройстве, например на базе ПК или мобильного телефона. Функция голосовой связи также хорошо разработана и интегрируется в небольшое устройство, называемое мобильным телефоном, и эти функции также включаются в интегрированное оконечное мультимедийное устройство на базе ПК. При такой интеграции все виды трафика, в том числе голосовая связь, превращаются в данные, поэтому выходным сигналом оконечного устройства должны быть "данные, но с различиями при передаче в реальном времени или не в реальном времени". Подобная интеграция различных функций в портативном ПК дает возможность вести кочевой образ жизни, например, в подвижном персональном офисе и т. д.

Рисунок 2-2: Совершенствование оконечных устройств

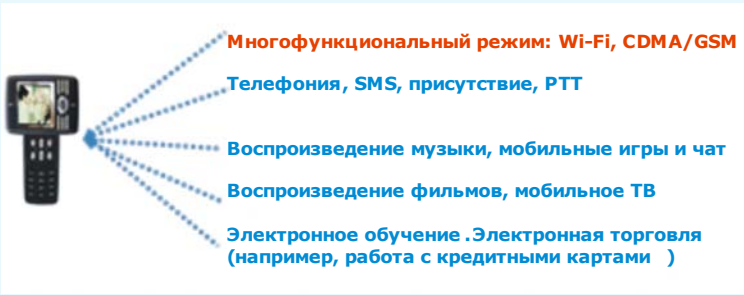


По окончании этого развития мобильные оконечные устройства должны стать одним из замечательных средств улучшения жизни людей с учетом использования ИКТ. Мобильный телефон уже не является просто телефоном, а превращается в интеллектуальное портативное устройство, позволяющее людям общаться в любом месте и в любое время, включая также личные развлечения (Рисунок 2-3).

Рисунок 2-3: Совершенствование мобильного оконечного устройства

В результате такого совершенствования оконечные пользовательские устройства, даже если говорить только о мобильных смартфонах, сегодня способны поддерживать большинство мультимедийных услуг, как показано на Рисунке 2-4.

Рисунок 2-4: Различные услуги с помощью многофункциональных оконечных устройств



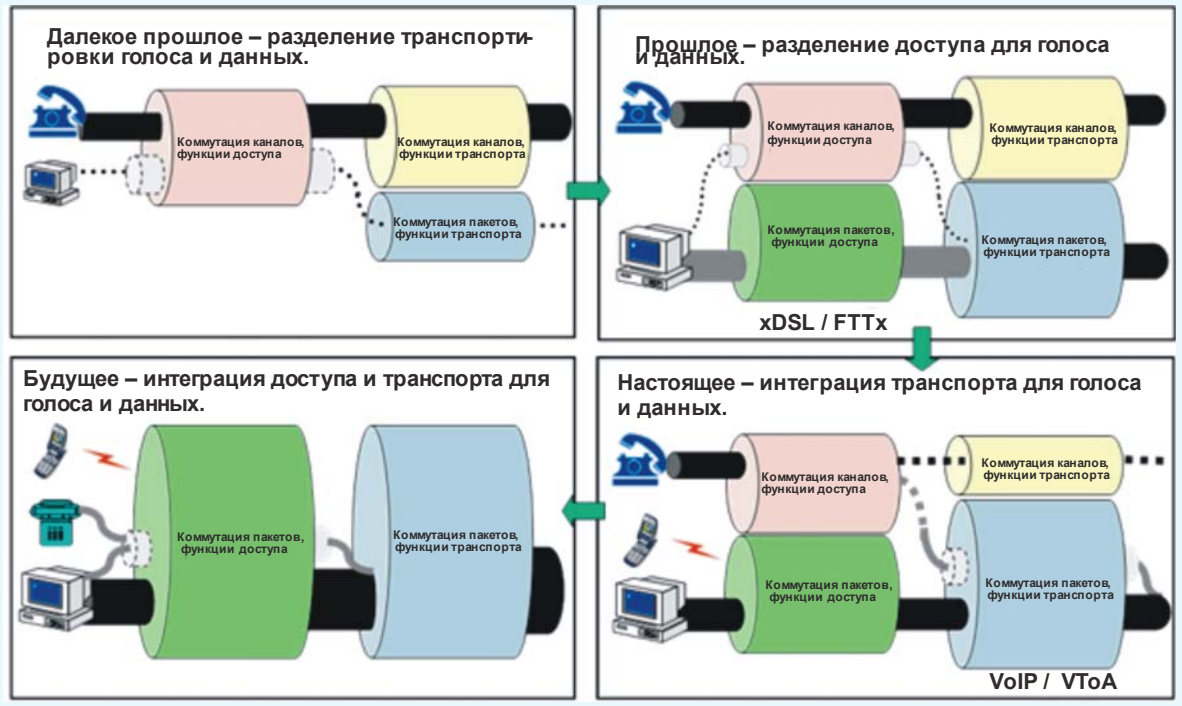
2.4 Развитие сетей электросвязи

Многие технологии разрабатываются и используются в сетях не только подвижной, но и фиксированной связи. В этом коротком отчете довольно трудно провести подробный анализ таких разработок. Поэтому в данном отчете делается попытка проанализировать основные направления развития сетей электросвязи в настоящее время и в будущем.

Одним из важных изменений или направлений развития сетей электросвязи должен стать переход от "коммутации каналов" к "коммутации пакетов". До конца 1980-х годов самой популярной темой развития сетей электросвязи было изменение технологий от аналоговых к цифровым, например появление сетей ЦСИС и т. д. Однако с появлением в середине 1990-х годов технологии IP переход от сетей на основе коммутации каналов к сетям на основе коммутации пакетов является наиболее важным моментом развития. На Рисунке 2-5 показан общий обзор результатов, которых удалось добиться в области технологических разработок, и будущие направления деятельности.

- Далекое прошлое. Сети электросвязи были достаточно четко разделены в зависимости от услуг, например голосовая связь и передача данных. Поэтому технология КТСОП была разработана для голосовых услуг, в том числе для передачи данных в голосовой полосе частот, например для факсимильной связи, а технология PSDN была разработана для передачи данных. При этом в обеих технологиях для доступа к сетям использовалась коммутация каналов.
- Прошлое. Осуществлялось масштабное развертывание пакетных технологий в большинстве сетей не только в базовых, как раньше, но и в сетях доступа. В основном этого удалось достичь при помощи IP-технологии с поддержкой xDSL, и таким образом был сделан значительный вклад в формирование соединенного мира. В некоторых услугах передачи данных по-прежнему использовались схемы доступа с коммутацией каналов, например с применением модемов.
- Настоящее. Пакетная передача данных является основной возможностью, которую предоставляют сети электросвязи как для передачи голоса, так и для передачи данных, включая подвижную связь. Используя преимущества широкополосного доступа, инфраструктура на основе коммутации пакетов охватывает многие виды мультимедийных услуг, включая голосовую связь. Однако сети с коммутацией каналов до сих пор сохраняют позиции в качестве основной сети для голосовой связи, хотя некоторые из сетей голосовой связи начинают переходить на транспортную сеть с коммутацией пакетов.
- Будущее. Ожидается, что возможности пакетной передачи данных позволят охватить весь диапазон сетей, т. е. базовые сети и сети доступа. И будут поддерживаться не только мультимедийные услуги, но и услуги голосовой связи как в фиксированных, так и в подвижных сетях с возможностями организации широкополосных передач.

Рисунок 2-5: Тенденции развития сетей электросвязи



Примечание: V: Голос, D: Данные.

2.5 Аспекты нумерации и маршрутизации

2.5.1 Нумерация и наименование

Отдельные пользователи идентифицируются по именам или номерам, а система распознавания имен и номеров переводит то или иное имя/номер в маршрутизируемый адрес сети. Поскольку СПП и существующие сети в течение некоторого времени будут работать параллельно, СПП должны поддерживать существующие планы наименования, нумерации и адресации для сетей фиксированной и подвижной связи. План международной нумерации для телефонной связи определен в Рекомендации МСЭ-Т E.164, а в Рекомендации МСЭ Y.2001 Общий обзор СПП рассматривается тема нумерации, наименования и адресации в СПП. Адрес представляет собой идентификатор для конкретного пункта завершения связи и используется для маршрутизации в этот пункт завершения. Маршрутизация является процессом распределения и сбора информации, связанной с топологией, расчета маршрутов, установления и обслуживания таблицы маршрутизации в сети (Y.2612). В традиционных аналоговых сетях для адресации элементов сети использовались номера. В цифровых коммутаторах адресация отделена от нумерации. Однако схемы нумерации имели довольно длительный срок службы, поскольку клиенты знают и используют номера, а оборудование в помещении клиента (CPE) интегрирует их.

Однако если речь идет о СПП, то можно рассматривать другой URI, т. е. SIP URI. При вызовах VoIP идентификаторы TEL URI или SIP URI преобразуются в адреса IP через доменную систему именования (DNS). Идентификаторы SIP URI могут быть включены в домен поставщика услуг или в собственный домен. Ниже приводятся некоторые примеры SIP URI:

SIP: 911125368781@<dummy> > только формат E.164

SIP: 911125368781@opr1.in > E.164 + домен поставщика услуг

SIP: abc@opr2.in > Имя + домен поставщика услуг

Таким образом, существующая схема нумерации может также использоваться в СПП. Для сети и конечного пользователя схема нумерации не имеет никакого значения. За маршрутизацию вызовов на базе номера E.164 будет отвечать программный коммутатор и SIP-сервер. Всем абонентам SIP присваивается номер согласно E.164. Функции, выполняемые сервером SIP программного коммутатора, обеспечат создание базы данных для всех таких абонентов SIP, в которой будут храниться IP-адреса, выделенные для соответствующих номеров E.164. Маршрутизация вызова от КТСОП к абоненту SIP будет осуществляться на основе таблицы согласно этой базе данных. Самое большое преимущество данного подхода состоит в том, что сохраняется такая же схема нумерации, что и существующая в настоящее время. В результате у конечных пользователей не будет путаницы при внедрении новых технологий, используемых для передачи голоса по сети.

Распознавание номеров/имен традиционно осуществляется при помощи таблиц маршрутизации в отдельных цифровых АТС. В интернете для распознавания номеров/имен используется система доменных имен (DNS). Поскольку СПП являются сетями с коммутацией пакетов и используют протокол IP, система DNS, вероятно, будет логичным выбором в качестве механизма распознавания номеров/имен в рамках СПП.

Нумерация E.164 (ENUM) связана с преобразованием телефонных номеров в универсальные идентификаторы ресурсов (URI) с использованием системы имен доменов (DNS). ENUM позволяет осуществлять конвергенцию между КТСОП и IP и использует DNS, тем самым позволяя экономить на капитальных затратах.

Каждому поставщику услуг необходима внутренняя система DNS ENUM, поддерживающая нумерацию и маршрутизацию и являющаяся частью магистральной линии связи этого оператора. При применении концепции этого типа оператор может использовать имеющуюся у него схему нумерации наряду с существующим идентификационным кодом оператора, который имеет следующий вид:

(Код зоны от 2 до 4 цифр) + (идентификационный код оператора 1 цифра) + (номер абонента от 5 до 7 цифр).

Все коммутаторы КТСОП и IP должны оканчиваться в одной и той же магистральной линии IP-оператора, через которого соединена система DNS. Система DNS выводит маршрутизируемый адрес назначения и завершает вызов. Кроме того, при использовании глобальной системы DNS маршрутизация и коммутация возможны при сценарии сетей со многими операторами и многими услугами.

Для вызовов от IP в направлении КТСОП телефонный номер места назначения может быть представлен как SIP URI. Для таких вызовов шлюз извлекает телефонный номер и задействует его для инициирования вызова с использованием сигнализации ISUP.

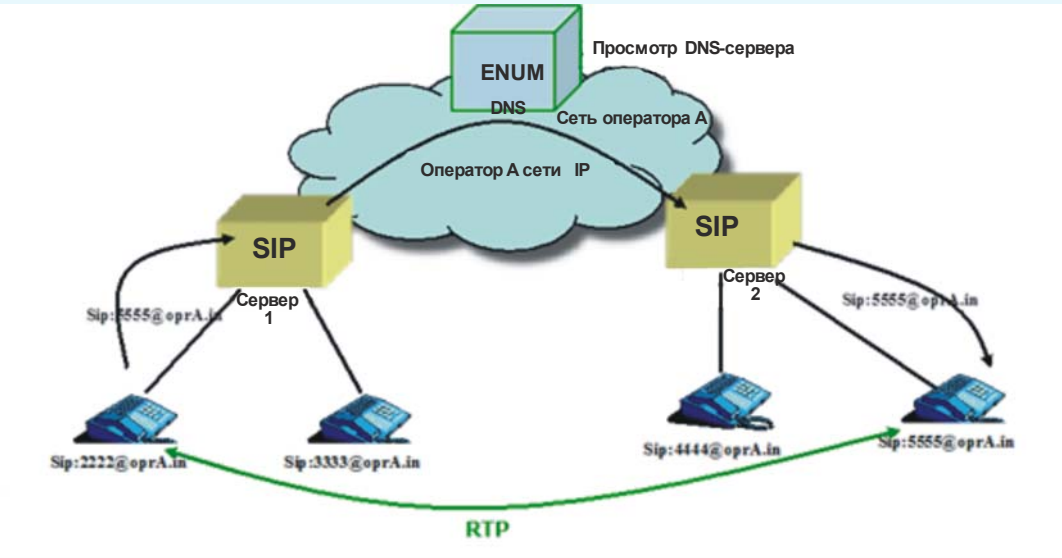
Это позволяет представить номер E.164 как URI, который может быть превращен в IP-адрес при помощи DNS. Основные тактические дискуссии разворачиваются вокруг древовидной схемы, которая будет использоваться для телефонных номеров. Намечена договоренность о создании единой всемирной древовидной схемы (так называемое "золотое дерево"), однако на данный момент единственным вариантом древовидной схемы, реализуемой в настоящее время, является e164.arpa. В контексте обсуждения "золотого дерева" осуществляется поиск бизнес-модели для ENUM. Оригинальной концепцией для ENUM стала бы глобальная, общедоступная каталогизированная база данных с возможностью подписки на услуги для абонентов и делегированием на уровне страны кода в домене e164.arpa. Этот вариант также называется *пользовательской ENUM*. Однако до сих пор не существует жизнеспособного экономического обоснования концепции пользовательская ENUM.

Техническая концепция ENUM является вполне жизнеспособной и сегодня главным образом реализуется в виде *операторской ENUM.* Группы операторов и поставщиков услуг связи заключают соглашения об обмене абонентской информацией через ENUM в частных пиринговых

взаимоотношениях, в то время как сами операторы управляют информацией абонентов. Операторская ENUM также называется *инфраструктурной ENUM*.

Нумерация ENUM, кроме того, используется для преобразования номеров в адреса в спецификациях систем IMS и в спецификациях IPX ассоциации GSM. Таким образом, реализация IMS требует внедрения операторской ENUM.

Рисунок 2-6: Функциональная совместимость и ENUM



2.5.2 Маршрутизация

Маршрутизация является процессом распределения и сбора информации, связанной с топологией, расчета маршрутов, установления и обслуживания таблицы маршрутизации в сети (Y.2612). Маршрутизация в IP-сетях определяется информацией в отдельных маршрутизаторах. Информация о маршрутизации между сетями распространяется при помощи пограничного шлюзового протокола (BGP). В традиционных сетях маршрутизация выполняется в пределах сети. Если определено, что конкретный адрес не находится в пределах сети, то соединение перенаправляется в соответствующую точку присоединения. Маршрутизация может также включать механизмы переполнения или управления трафиком, которые должны предотвращать отключения или перегрузку в сети.

Базовая архитектура использует хорошо известные IP-протоколы, такие как OSPF, BGP и т. д. для обновления маршрутизации, и MPLS для управления трафиком. Конфигурация и процедуры маршрутизации для передачи IP-трафика от одного оператора к другому будут зависеть от того, каким образом эти операторы связаны между собой. Кроме IP-соединений и протоколов маршрутизации между двумя операторами, в СПП потребуются специальные меры для обеспечения плавной передачи голосовых и видеосигналов из одной сети в другую. Возникнут вопросы, связанные с обходом брандмауэров, безопасностью, соглашениями об уровне обслуживания, передачей протоколов в двух сетях (функциональная совместимость) и законным перехватом вызовов. Для успешного решения этих вопросов на границах между двумя операторами СПП необходима установка таких устройств, как пограничные контроллеры сеансов (SBC). Сетевые устройства наподобие маршрутизаторов и коммутаторов в базовых и пограничных сетях должны поддерживать протоколы IPv4 и IPv6 для упрощения перехода на IPv6 в будущем.

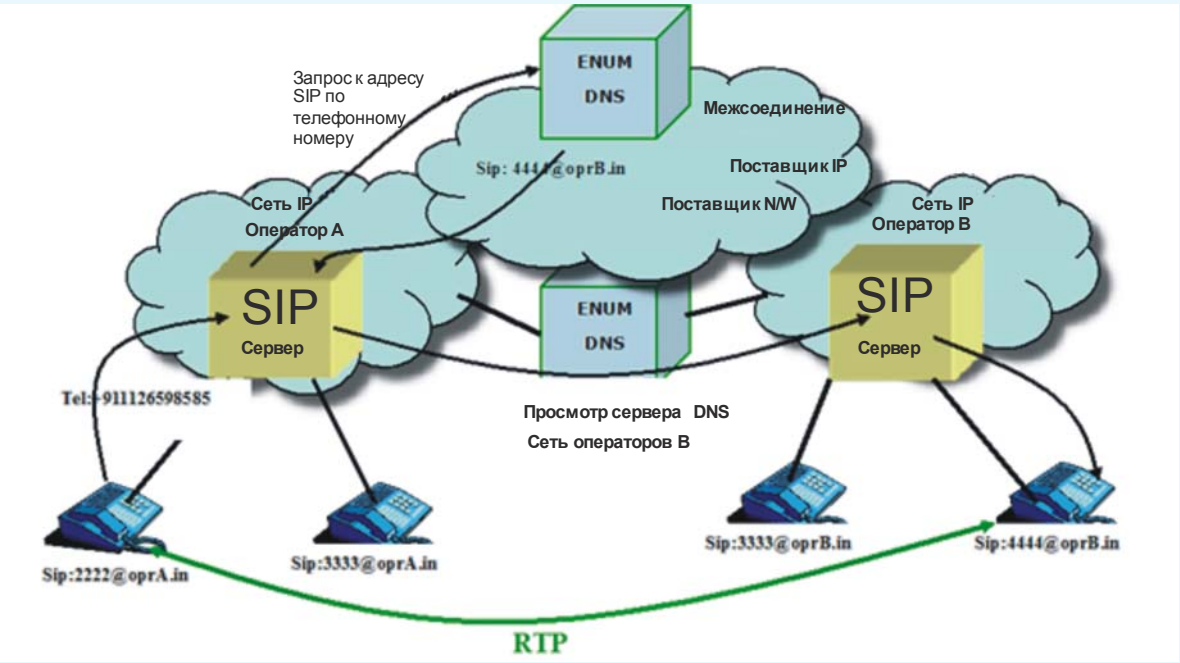
В сетях подвижной связи реализована концепция роуминга. Это означает, что абоненты могут совершать и принимать звонки в гостевых сетях и получать счета от операторов своей домашней

сети. Согласно спецификациям GSM вызовы абоненту роуминга направляются через домашнюю сеть, которая определяет плату за роуминг. Активные вызовы, совершаемые абонентом роуминга, направляются непосредственно к месту назначения без прохождения через домашнюю сеть. Оператор гостевой сети регистрирует детальную информацию о вызове и отправляет их оператору домашней сети при помощи так называемой процедуры перевода счетов (TAP), которая определена ассоциацией GSMA. При использовании абонентами роуминга мобильного интернета соответствующая информация во всех случаях направляется в домашнюю сеть, которая осуществляет управление доступом к интернету.

Маршрутизация и роуминг в сетях последующих поколений используют механизмы IP-протоколов. Следует ожидать, что операторы будут поддерживать свое влияние на трафик в роуминге и участвовать в цепочке прохождения вызова абонентов роуминга. С технической точки зрения это не потребуется при условии, что HLR-информация может быть доступна также через другие сети. Решение вопросов маршрутизации и обмена информацией включено в спецификации IMS.

В сетях на основе протокола IP соединения в сеансе SIP устанавливаются при помощи GLOBAL ENUM DNS следующим образом.

Рисунок 2-7: Установление соединения в сеансе SIP при помощи GLOBAL ENUM DNS



3 Проблемы регулирования, возникающие в процессе перехода к СПП

Проблемы регулирования, возникающие при переходе к СПП, в той или иной форме могут быть связаны с процессом конвергенции на уровнях предоставления услуг и доступа к сети. В этом разделе обсуждается ряд проблем в области регулирования, относящихся к СПП, с точки зрения перспективы. В число этих проблем входят открытый доступ, определение рынка, качество обслуживания (QoS) и межсетевые соединения.

При рассмотрении этих проблем важно помнить, что СПП унаследуют некоторые из регуляторных обязательств, возложенных на КТСОП, такие как правомерный перехват и доступ к службам экстренного вызова. Необходимость обеспечения доступа к службам экстренного вызова

учитывалась как в 3GPP, так и в TISPAN. Однако в рамках архитектуры IMS 3GPP первое внедрение служб экстренного вызова планируется только для версии 7 и последующих версий, тогда как в двух предыдущих версиях IMS (R5 и R6) доступ к службам экстренного вызова обеспечивался только через домен с коммутацией каналов, существующую базовую инфраструктуру GSM, используемую для голосовых вызовов.

GPRS уже дает возможность законного перехвата для услуг на основе коммутации пакетов, оказываемых в сетях подвижной связи 2G. Система GPRS может направлять дубликаты всех пакетов, которыми пользователь обменивался через PDP-контекст, а также адрес объекта, определенный через этот контекст. Перехват на законных основаниях был внедрен уже исходя из первой спецификации R5 IMS 3GPP.

3.1 Соображения по регуляторным проблемам высокого уровня

Хотя СПП и обеспечиваемые ими услуги, по-видимому, обладают многочисленными преимуществами, необходимо обладать более ясным представлением обо всех имеющихся вариантах, а также о всех преимуществах и недостатках, связанных с СПП. Ниже приведены вопросы, полезные для идентификации этих соображений.

- Какие сети для каких услуг предназначены?
- Какие действия могут быть предусмотрены регуляторными органами для содействия переходу к СПП в интересах потребителя?
- Каким образом переход к СПП отражается на регуляторной деятельности крупнейших операторов?
- Каким образом внедрение сетей СПП влияет на межсетевые соединения, установление тарифов на оказание услуг, нумерацию, управление спектром частот и т. д.?

С целью подготовки перехода существующей инфраструктуры электросвязи к СПП следует внимательно рассмотреть возможные проблемы, которые могут возникнуть в СПП, такие как межсетевые соединения, защита прав потребителей, переопределение универсального доступа, технологическая нейтральность, качество обслуживания, нумерация и лицензирование. Очень важно провести исследования (технические, экономические, а также в области регулирования), касающиеся мер по переходу к сетям СПП с целью определения правильного периода времени для перехода. Важно отметить, что регулирующий орган должен гарантировать, что рынок, появившийся в результате перехода, будет честным, открытым и конкурентным и, с другой стороны, разъяснить регулятору все технические, экономические и регуляторные вопросы, возникающие вследствие перехода к сетям СПП, с тем чтобы он определил на возможно более раннем этапе сферы интересов, связанных с его деятельностью.

Для этих целей были рассмотрены следующие вопросы для изучения:

- обзор законодательного и регуляторного режима электросвязи и определение тех элементов, для которых может потребоваться адаптация в целях обеспечения конвергенции;
- сбор данных, касающихся ожиданий операторов и поставщиков услуг в отношении сетей СПП;
- изучение стратегии перехода основных операторов фиксированной и подвижной телефонной связи в отношении сегментов базовой сети и сети доступа;
- определение элементов, затрудняющих или ускоряющих переход к СПП (на технологическом, экономическом и регуляторном уровнях);
- выявление новых экономических моделей, которые будут связаны с СПП, их приемлемость и долговечность;
- разработка стратегии перехода сетей фиксированной и подвижной телефонной связи к СПП;

- подготовка амбициозной дорожной карты для этого перехода, которая может быть адаптирована к развитию новых технологий наряду с бюджетом, реальными сроками выполнения и показателями/механизмами контроля за ее осуществлением.

Данное исследование должно проводиться в соответствии с предлагаемой ниже последовательностью этапов:

1 сбор и анализ информации по законодательной и регуляторной структуре электросвязи;

2 организация семинара/практикума по проблемам СПП, открытого для всех участников рынка электросвязи и сектора ИКТ;

3 сбор данных от операторов фиксированной и подвижной телефонной связи и поставщиков услуг доступа к интернету;

4 анализ и использование информации о ситуации в каждой стране и сравнение с опытом других стран;

5 подготовка дорожной карты, выпуск заключительного отчета об исследованиях и программного документа по переходу к СПП.

Одним из способов формирования регуляторной точки зрения мог бы стать акцент на необходимости рассмотрения вопросов регулирования СПП в рамках методологического подхода. В этом плане вопрос о том, являются ли СПП общественным благом или нет, является хорошим поводом для изучения многих аспектов, таких как неисключаемость поставок, отсутствие конкуренции в потреблении и внешние последствия в экономической деятельности. Исследование этих аспектов может внести ценный вклад в установление регуляторного режима для СПП на очень высоком уровне, при этом возможно принятие нового подхода к регулированию, который создаст иную нормативно-правовую базу, нежели в традиционной электросвязи.

Ниже приведено краткое изложение основных пунктов, касающихся вышеупомянутых аспектов.

- Неисключаемость поставок. Этот фактор означает, что поставки соответствующего продукта должны охватывать всех без исключения. Продукт, предлагаемый на рынке в стране или обществе, доступен для всех проживающих там людей. Участники рынка не могут осуществлять поставку на уровне рыночных операций. Один из основных моментов заключается в том, что поставляемый продукт не поставляется по запросу. Продукт, который предоставляется одному человеку, одновременно предоставляется каждому члену общества. Поставки соответствующего продукта носят однородный характер. Сама поставка должна представлять однородный продукт.

- Отсутствие конкуренции в потреблении. Этот фактор означает, что потребление человеком какого-либо продукта не создает помех для потребления его другим человеком. Потребительские предпочтения отдельных лиц являются неоднородными. С другой стороны, неоднородный характер предпочтений в отношении потребления не создает конкуренции или соперничества в потреблении.

- Внешние последствия экономической деятельности. Это означает соотношение между доходами и затратами для других объектов, связанных с продуктом. Продукт, который предоставляется в качестве общественного блага, не является столь эффективным в плане соотношения доходов и затрат, в отличие от функциональности свободного рынка. Общественные блага создают отрицательный внешний эффект, поэтому не могут рассматриваться как эффективный экономический механизм с точки зрения открытого рынка.

МСЭ-D разработал ряд документов и провел ряд семинаров, связанных с регулированием, определением затрат и политическими подходами, с тем чтобы помочь странам в развитии их услуг электросвязи. Значительное внимание в последние годы уделялось сетям последующих поколений, в первую очередь тому, каковы проблемы и преимущества новых технологий электросвязи/ИКТ. Для содействия Членам МСЭ в этом вопросе был подготовлен отчет "Стратегии развертывания СПП

в широкополосной среде – Регуляторные и экономические аспекты"[1]. В нем рассматриваются стратегические проблемы высшего уровня, а также экономические и фундаментальные аспекты, связанные с переходом к СПП. Цель отчета – обеспечить надлежащую информацию для содействия в разработке национальных стратегий и регуляторных подходов к широкополосной связи, которые принесли бы пользу отрасли электросвязи, потребителям и всем предприятиям, пользующимся услугами электросвязи.

3.2 Сети доступа последующих поколений

Как было сказано выше в разделе 3.1, сети последующих поколений начали изменять основные элементы сектора электросвязи, такие как услуги, сетевая структура и действующая модель сетевой структуры. Таким образом, необходим обновленный регуляторный подход, отличающийся от обычного, который использовался в сетях электросвязи предыдущего поколения. Одна из основных причин этого вытекает из последствий конкретных технических изменений в структуре СПП. Следовательно, национальные регуляторные органы должны рассмотреть вопрос о том, каким образом действующие нормативно-правовые положения могут быть адаптированы к этой новой среде в соответствии с существующей структурой рынка.

Для начала следует обратить особое внимание на то, являются ли сети NGA (сети доступа последующих поколений) необходимыми структурами. В существующих сетях была только одна сетевая инфраструктура доступа, поэтому на ней лежала обязанность по обеспечению доступа абонентских линий. Тем не менее в сфере применения СПП, которая не зависит от наличия специальных сетей доступа, даже доступ по волоконно-оптическим линиям не является необходимой функцией для услуг СПП. Для того чтобы волоконно-оптические линии были необходимым элементом, должны отсутствовать какие-либо иные сети доступа. В процессе перехода к сетям на базе IP существующие телефонные базовые сети могут рассматриваться в качестве альтернативы сетям NGA. Следовательно, СПП можно рассматривать как технические устройства, способные предоставить больше новых услуг на основе IP (видеовызовы, широкополосную связь, IP-телевидение, интеллектуальные услуги и т. д.) по сравнению с существующей структурой на основе телефонных сетей. Более того, так как сети СПП представляют собой новый подход в секторе электросвязи, структура рынка и предпочтения спроса еще не сформировались. Поскольку сети СПП и NGA отличаются от существующих сетевых структур электросвязи с точки зрения возможностей и функциональности, соответствующая структура рынка с учетом этих сетей еще не определена.

Таким образом, как отмечалось выше, в процессе перехода к СПП, необходим новый нормативно-регуляторный подход. Одним из ключевых моментов для развития конкуренции, при одновременном стимулировании инвестиций в сети доступа СПП, является вопрос о развязывании абонентских линий (LLU) в волоконно-оптической среде. В настоящее время регулирование развязывания абонентских линий сосредоточено на последней миле. Однако переход к технологиям FTTH, FTTB и FTTC означает смещение акцента в сторону последней четверти мили или менее. Учитывая затраты и другие задействованные ресурсы, модель LLU, пригодную для существующих медных сетей, возможно, придется адаптировать для волоконной оптики или различных идентифицированных средств. Там, где регулирующие органы предоставляют мандат LLU, одним из вариантов может быть предложение по потоку битов на уровне центрального офиса, где сама сеть доступа является полностью прозрачной. Другие варианты могут включать требуемое совместное расположение на уровне уличного шкафа и обратную линию от шкафа до узла оператора. Кроме того, процесс перехода к СПП предполагает новый подход к LLU, который

[1] С отчетом можно бесплатно ознакомиться на веб-сайте: http://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Studies.aspx.

отличается от обычного взгляда на LLU в существующих сетях. В качестве нового метода в процессе перехода к СПП можно рассматривать отсутствие регулирования LLU в сетях NGA. Это связано с тем, что регулирование LLU в процессе перехода будет тормозить формирование эффективности распределения и честной конкуренции. Компании, развертывающие сети NGA, не должны подвергаться воздействию LLU до тех пор, пока не будут погашены невозвратные издержки, а на рынке услуг не будет сформирована конкурентная среда. Продолжительность возврата инвестиций зависит от бизнес-модели компании, структуры рынка и благосостояния общества, но в целом понятно, что это займет по крайней мере 4 или 5 лет. Обязательство по LLU в сетях NGA может привести к возникновению на рынке проблемы безбилетника. Вопрос безбилетника не должен учитываться только при возврате инвестиций, а также в контексте честности и различий в услугах различных поставщиков, участвующих в переходе к СПП.

После того как будет сформирована конкурентная рыночная структура и будет завершен этап перехода, появятся другие устройства, не имеющие отношения к LLU и позволяющие воспользоваться преимуществами использования волоконно-оптического кабеля, такие как доступ через битовый поток, коммутаторы и виртуальное развязывание. Помимо этого необходимо также решить, какой рынок предпочтительнее в качестве конкурентного – розничный рынок услуг или оптовый рынок доступа. Однако обеспечение собственной транзитной передачи для конкурентоспособных операторов может представлять трудности до тех пор, пока не будет доступно совместное использование кабельных туннелей.

Существует также целый ряд трудностей, связанных с развертыванием новых волоконных линий. Значительные средства потребуются на долгосрочные инженерно-строительные работы, включающие обновление пассивной сетевой инфраструктуры в местах общественного пользования, такие как рытье траншей и прокладка туннелей, а также подключение абонентских кабелей в частной сфере, например прокладка кабелей в жилых зданиях и помещениях. К этому добавляются значительные трудности, связанные с ведением переговоров, что оказывается не под силу индивидуальным поставщикам услуг. По указанным причинам регуляторные органы в качестве одного из решений проводят изучение совместного использования пассивной инфраструктуры.

Еще одна проблема, возникшая в связи с FTTx, касается ликвидации действующим оператором главных коммутационных щитов (кроссов) – в этом случае "старая" схема LLU для медных линий оказывается устаревшей, по крайней мере при их полном развязывании и при возможности совместного использования линий, поскольку в рамках традиционных сценариев LLU развязывание происходит на уровне кросса MDF. Там, где точки межсетевых соединений будут ликвидированы, конкурирующим операторам будет важно и то, чтобы они не несли дополнительных расходов при переходе к СПП и чтобы были в состоянии продолжить предоставление своих услуг, не столкнувшись с проблемой "неподъемных" инвестиций. Так, например, действующий нидерландский оператор KPN объявил[2], что при переходе к СПП он ликвидирует все свои кроссы MDF, чтобы свести свою сеть к меньшему количеству узлов коммутации и использовать DSLAM только в уличных распределительных шкафах. KPN рассчитывает, что продав здания, в которых находились ее кроссы MDF, компания выручит 1 млрд. евро, которые затем можно будет использовать для финансирования развития своей технологии FTTx. В настоящее время KPN и нидерландский национальный регуляторный орган OPTA ведут обсуждение планов KPN по ликвидации кроссов MDF, причем в эти планы могут быть включены условия поэтапного свертывания доступа к MDF, а также предложение KPN предоставить "развязывание абонентских вспомогательных линий связи" (SLU) для уличных распределительных шкафов и "оптовый широкополосный доступ" (WBA) на местном, региональном или национальном уровнях коммутации. Возможно, по мере того как операторы продолжат развертывать свои сети доступа

[2] См. http://erg.eu.int/doc/whatsnew/kpn_van_den_beukel_erg_17_apr_07.pdf.

СПП, регуляторные органы в других странах пожелают последовать тем процессам в сфере регулирования, которые имеют место в Европе и в других регионах мира

На самом деле важным этапом для экономики должно стать не формирование конкуренции на рынке инфраструктуры в процессе перехода к СПП, а создание конкуренции на рынке услуг. При такой конкуренции на рынке должно происходить более эффективное внедрение инноваций в экономику. Таким образом, хотя и желательно, чтобы рыночная конкуренция была построена на основе услуг СПП, нельзя полностью исключить фактор распространения волоконно-оптических сетей в рамках NGA. Распространение волоконных сетей существенно повлияет на конкуренцию в сфере услуг на основе СПП.

3.3 Определение рынков

Выявление и определение соответствующих рынков представляют собой основу для анализа положения дел в сфере конкуренции, необходимого для организации прогнозируемого регулирования во многих странах, в частности в ЕС. После перехода к СПП данная задача значительно усложнится из-за размывания границ между технологиями и услугами. Это усложнение может стать источником разногласий между регуляторными органами и участниками рынка.

Пример развертывания СПП компанией Deutsche Telekom и ее разногласия с регуляторным органом по поводу обязательства предоставить конкурентам доступ к своей сети – наглядный пример тех новых проблем в области регулирования, которые влечет за собой переход к СПП. Создавая благоприятную среду для СПП, следует обратить внимание на ее технические аспекты. В основе разногласий между Deutsche Telekom и регуляторным органом лежит разное толкование качественных различий между доступом по волоконно-оптическим кабелям и доступом по DSL. По мнению Deutsche Telekom, дополнительная полоса пропускания, предоставляемая волоконно-оптическим кабелем, качественно изменяет обслуживание, позволяя, например, оказывать услуги телевидения высокой четкости, и этим обусловлены отличия этого рынка от рынка DSL, на который компания имеет сегодня значительное влияние. Однако с точки зрения регуляторного органа данный проект в основном является модернизацией предоставляемых компанией Deutsche Telekom услуг DSL в стремлении удержать своих нынешних абонентов DSL.

Последствия подобных разногласий могут быть весьма серьезными, если операторы, занимающие существенное положение на рынке, пригрозят заморозить свои инвестиции. Однако с учетом потенциального возврата капиталовложений, европейские регуляторные органы, по-видимому, уверены, что операторы будут и далее вкладывать средства в подобные проекты.

3.4 Качество обслуживания

Унифицированное транспортирование услуг СПП ставит вопросы, связанные с тем, что IP-транспорт работает без установления соединения, особенно для интерактивных голосовых или мультимедийных потоков в режиме реального времени, которые чувствительны к потере пакетов, задержке или дрожанию. Однако уже существует множество технологий, обеспечивающих качество обслуживания (QoS) в IP-сети. Эти технологии можно ориентировочно разделить на технические подходы, основанные либо на избыточности, которая связана с относительными приоритетами, либо на прямом сквозном резервировании ресурсов.

Следует отметить, что в основном в интернете используется модель "наилучшего возможного качества", не дающая гарантий QoS. Многие приложения в интернете используют протокол управления передачей (TCP), ограничивающий трафик пользователей в случае перегруженности. Однако TCP не подходит для приложений, работающих в режиме реального времени, например потокового видео, голосовой или мультимедийной связи, когда невозможно ограничить скорость передачи пакетов в случае перегруженности. В последнее время появляется все больше приложений, таких как голосовая телефония или потоковое видео, работающих в режиме

реального времени в сетях не только фиксированной, но и подвижной связи, занимающей значительную часть базового интернет-трафика. Сегодня для базовой сети с избыточным предоставлением услуг, как и в случае множества интернет-магистралей, управление таким трафиком является сложной задачей, включая проблемы, касающиеся добросовестного использования сетевых ресурсов и взрывного роста объема данных.

Сети последующих поколений, однако, отличаются от интернета, даже если они используют одни и те же технологии IP-транспорта. СПП основаны на четких гарантиях, предоставляемых сетью конечным пользователям для приложений, нуждающихся в хорошем качестве, таких как IP-телевидение и гарантированные услуги VoIP. Такие приложения, как ожидается, составят бóльшую часть трафика СПП.

Однако сети последующих поколений являются управляемыми и закрытыми. Таким образом, многие из методов обеспечения функции QoS, связанные с дифференцированными приоритетами и резервированием ресурсов, которые не получили широкого применения в интернете из-за масштабируемости и связанных с этим расходов, могут найти применение в сетях последующих поколений. Кроме того, в архитектуре СПП домен транспортировки управляется доменом обслуживания, который обеспечивает надлежащее распределение ресурсов транспортным доменом на весь период оказания данной услуги сетью. В интернете ничего подобного не существует, поскольку "управление" в нем является сквозным и не ограничено рамками сети.

Важнейшей и пока не решенной проблемой остается необходимость координации различных сетей последующих поколений, чтобы таким образом обеспечить сквозное качество обслуживания QoS. Широко распространенным заблуждением является утверждение, будто в КТСОП сквозная функция QoS обеспечивается за счет резервирования канала TDM со скоростью 64 кбит/с во всех сетях на пути прохождения сигнала. Хотя это и верно, но сквозная функция QoS в КТСОП определяется также надлежащей сквозной передачей сигналов по системе сигнализации МСЭ № 7 (SS7). Этот же принцип сквозной сигнализации может быть применим и к любым другим носителям при транспортировке пакетов, возможность чего была продемонстрирована в принятой МСЭ спецификации протокола управления вызовом, независимого от носителя (BICC), представляющего собой адаптацию SS7.

По определению и в соответствии с проектом архитектура IMS использует для сигнализации о вызове (сеанса связи) протокол SIP. SIP представляет собой, в сущности, сквозной протокол Интернет, однако группы 3GPP и TISPAN ETSI расширили его таким образом, чтобы его можно было применять для функций управления сетью при вызовах речевой и мультимедийной связи в СПП. Это происходит аналогично осуществлению функций управления вызовами и услугами в традиционной архитектуре интеллектуальных сетей на базе SS7. МСЭ разрабатывает протоколы сигнализации СПП для резервирования ресурсов на основе каждого вызова отдельно, которые будут применяться в сетях, и в первую очередь в точках межсетевых соединений. Эта работа ведется в тесном сотрудничестве с группами 3GPP и TISPAN ETSI. МСЭ уже подготовил ряд рекомендаций о протоколах сигнализации СПП для резервирования ресурсов, а дальнейшей разработкой занимается ИК11 МСЭ-Т.

Конечно, регуляторные органы не обязаны вникать в технические детали обеспечения QoS в СПП. Однако в целях поддержки основных услуг, таких как интерактивная голосовая связь, регуляторные органы могли бы внести свой вклад в определение основных требований, предъявляемых к точкам межсетевых соединений, так же как сегодня это происходит при соединениях телефонных сетей.

3.5 Межсетевые соединения

Потребность в соединениях между сетями электросвязи определяется в основном насущной необходимостью завершения услуги. В этом отношении СПП не являются исключением; в действительности они предполагают даже бóльшие требования к межсетевым соединениям,

нежели существующие телефонные сети, и причиной этого является повсеместный доступ к предоставляемым по СПП услугам.

Помимо традиционных требований к межсетевым соединениям для завершения услуги между различными сетями последующих поколений, а также между сетями последующих поколений и другими сетями голосовой связи необходимо обеспечить абоненту возможность:

- подключаться из любой другой сети и получать из своей домашней сети перечень оказываемых ею услуг, чтобы получить соответствующее обслуживание, что аналогично концепции роуминга в сетях подвижной связи, однако применительно ко всем видам широкополосного пакетного доступа;
- получать доступ к услугам, оказываемым его сетью, вместо услуг, предлагаемых в гостевой сети, как это уже происходит в сетях подвижной связи благодаря интерфейсу интеллектуальной сети (IN) Специализированного приложения для усовершенствованной логики сетей подвижной связи (CAMEL), который позволяет находящимся в роуминге абонентам получать, например, информационные сообщения в сети, а также доступ к дополнительным услугам на своем родном языке; а также
- получать доступ к дополнительным услугам, оказываемым поставщиками услуг третьей стороны, – принцип, который в настоящее время применяется к некоторым услугам контента в сетях поколений 2.5G и 3G, например, в виде доступа к альтернативным порталам протокола беспроводных приложений (WAP) или услугам I-mode.

Для формулирования требований к межсетевым соединениям в рамках СПП необходимо дать общее определение понятию "мультимедийный вызов". Такое определение может сыграть решающую роль при выборе либо режима "платит вызывающая сторона" (CPP), либо принципа bill & keep (взаимное бесплатное предоставление услуг). Что касается межсетевых соединений в среде СПП на основе протокола IP, важно внести ясность в то ошибочное суждение, которое связывает режим CPP с транспортировкой на основе коммутации каналов. Режим CPP в большей степени касается соглашения о завершении услуги применительно к тому или иному конкретному вызову между двумя доменами сети, нежели реального резервирования ресурсов для этого конкретного вызова. Тот факт, что при традиционной голосовой телефонии при этом предполагается резервирование выделенного канала, является всего лишь технической деталью, которая будет претерпевать изменения по мере перехода сетей на пакетную транспортировку. В условиях СПП подобная гарантия завершения услуги будет иметь смысл применительно к индивидуальным мультимедийным вызовам только в том случае, если существует или считается необходимым взаимодействие в сфере сигнализации между соответствующими объектами управления на границах сетевых доменов. Чтобы такая сигнализация существовала, необходимо наличие общего определения требований к подобным мультимедийным вызовам аналогичного тому, что уже существует в отношении голосовых вызовов.

Весьма вероятно, что в условиях СПП проблема роуминга окажется еще более сложной. В настоящее время в отрасли подвижной связи действуют соглашения о взаимном роуминге, не требующие вмешательства со стороны регуляторных органов. Эти органы участвовали только в решении вопросов тарификации роуминга. В отношении СПП регуляторным органам необходимо будет продумать вопрос о том, есть ли необходимость санкционировать предоставление роуминга? Например, должен ли оператор подвижного доступа в СПП в обязательном порядке предоставлять клиентам какого-либо оператора волоконной сети доступа в СПП возможность роуминга в своей сети доступа, и наоборот?

Остро стоит и проблема доступа к услугам третьей стороны. В прошлом операторы подвижной связи пытались закрепить своих абонентов за собственной платформой предоставления услуг. К счастью, от этой практики уже отказались, даже фактически третьи стороны оказывают большинство услуг через операторские порталы. Аналогичным образом регуляторным органам необходимо будет тщательно отслеживать доступ третьих сторон к услугам в среде СПП. Хотя на

бумаге архитектура IMS и СПП путем использования СПП-OSE и СПП-SIDE закрепляет доступ третьей стороны к платформам поставщиков услуг, на практике выполнить это требование будет достаточно сложно и, возможно, это создаст предпосылки для неконкурентного поведения, завуалированного техническими аргументами.

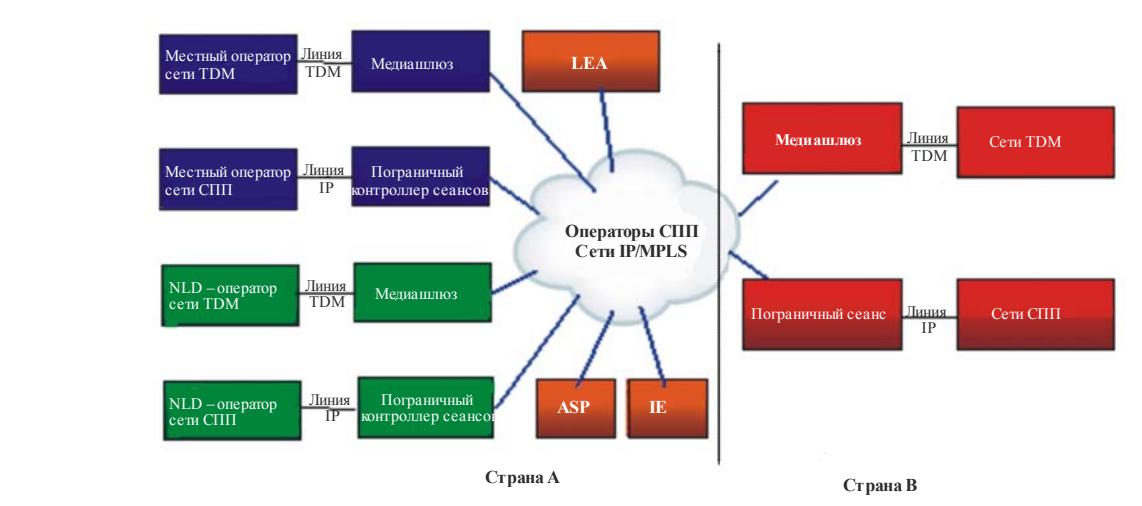
3.5.1 Архитектура межсетевых соединений

Многие из созданных за последние годы сетей содержат большую часть элементов СПП. Вначале имел место медленный процесс в плане применения передовых подходов к организации межсетевых соединений, даже если технология была разработана или ее разработка была близка к завершению. Благодаря эффективности и гибкости IP-технологии большинство создаваемых новых сетей базируются на IP.

Межоператорские сценарии в среде СПП показаны на Рисунке 3-1.

Межсетевое соединение на равной основе традиционных КТСОП и сетей подвижной связи на базе протокола пользователя ЦСИС (ISUP) может осуществляться через медиашлюз для преобразования IP в TDM или TDM в IP и через шлюз сигнализации для транспортировки SS7 поверх IP.

Рисунок 3-1: Архитектура межсетевых соединений межоператорской среды в сценарии СПП



Примечание: LEA – Правоохранительный орган
ASP – Поставщики услуг приложений
IE – Коммунальная станция для межсоединений

Как показано на Рисунке 3-1, сети СПП соединены между собой пограничными контроллерами сеансов (SBC), которые расположены на административной границе сети для реализации соответствующей политики во время мультимедийных сеансов. Политика сеанса может быть определена в области обеспечения безопасности, соглашений об уровне обслуживания, ресурсов сетевых устройств, пропускной способности сети, межсетевого взаимодействия и функциональной совместимости протоколов между сетями.

Контроллеры SBC могут выполнять целый ряд функций, таких как:

- сетевая безопасность;
- DOS-атаки (типа "отказ в обслуживании"), а также контроль перегрузки;
- трансляция сетевых адресов и обход брандмауэра;
- законный перехват;

- управление качеством обслуживания (QoS);
- передача протоколов;
- учет вызовов.

Медиашлюз (MGW), показанный на Рисунке 3-1, управляется программным коммутатором, устанавливаемым в сетях СПП операторами сетей КТСОП и подвижной связи. Шлюз сигнализации (SGW) может быть интегрирован в медиашлюз, либо представлять отдельное устройство.

3.5.2 Интерфейсы

3.5.2.1 Физические интерфейсы

Пограничный контроллер сеансов (SBC) предоставляет интерфейс(ы) IP для других сетей СПП. Физические интерфейсы состоят из:

- интерфейсов Gigabit Ethernet;
- интерфейса(интерфейсов) 10/100 Base-T Fast Ethernet.

Контроллер SBC обеспечивает резервными подсистемами сигнализации и управления медиаданными, каждая из которых включает резервные сетевые интерфейсы. Подсистемы SBC осуществляют связь друг с другом через любой из доступных IP-интерфейсов.

3.5.2.2 Интерфейсы сигнализации

Предполагается, что сетевой моделью, для которой определены интерфейсы сигнализации, являются сети последующих поколений (СПП) полностью на базе IP, где в качестве контрольной точки сети может выступать:

- программный коммутатор; или
- центральная сеть IMS (мультимедийные услуги на базе IP).

Вопросы стандартизации систем сигнализации в основном находятся в ведении сектора МСЭ-Т и, следовательно, не попадают в сферу действия настоящего Вопроса. Однако регуляторные аспекты, связанные с принятием определенных типов интерфейсов, имеют большое значение. В то время как МСЭ-Т занимается стандартизацией протоколов и сигнализации, в этом Вопросе следует выяснить, должны ли регуляторные органы предписывать какой-либо установленный стандарт для обеспечения функциональной совместимости или оставить такое решение за операторами, что может привести к недостатку функциональной совместимости.

13-я Исследовательская комиссия МСЭ-Т уже направила две Рекомендации в ответ на заявление о взаимодействии по этому Вопросу. В Рекомендациях МСЭ-Т Y.2701 и Y.2201 приведены требования по безопасности для интерфейсов и требования высокого уровня для услуг и пропускной способности сетей последующих поколений. Помимо этих рекомендаций существует серия рекомендаций, посвященных СПП.

Кроме того, МСЭ-Т утвердил Рекомендацию Q.3401 по вопросам сигнализации – Набор параметров сигнализации в СПП, которой, возможно, захотят пользоваться регуляторные органы.

3.5.3 Точки межсетевых соединений

Во время переходного этапа на основного оператора может быть возложено обязательство сохранять традиционные возможности межсетевых соединений КТСОП. При допущении, что конкуренты могут связаться с конечными пользователями на базе СПП основного оператора посредством традиционных межсоединений, необходимость в регуляторном обязательстве обеспечивать новые возможности межсоединений на базе СПП может не возникнуть. Основной оператор предоставит межсетевое соединение на базе IP в какой-то момент переходного этапа.

Когда переходный этап приближается к завершению, оператор может аннулировать традиционное межсетевое соединение. В той степени, в которой такой оператор сохраняет власть над рынком, на него почти со всей определенностью должно быть возложено регуляторное обязательство по обеспечению межсоединений с СПП по ценам, основывающимся на затратах. В мире интернета подавляющее большинство межсоединений осуществляется в виде или одноранговой связи, или транзита. В случае СПП участники рынка могут выбрать одноранговую связь, транзит или какую-либо иную форму межсетевых соединений. Фактически одноранговая связь обеспечивает обмен трафиком только между основными клиентами и клиентами аналогичного ранга, но не предусматривает доступ к третьим сторонам. Напротив, в типовом случае транзитной связи транзитный клиент может использовать сеть транзитного поставщика для доступа к пунктам назначения в любой точке интернета. Маловероятно, что основной поставщик услуг будет заинтересован предлагать одноранговые структуры конкурирующим с ним мелким операторам. Он может предложить одноранговые структуры лишь нескольким местным крупнейшим конкурентам. На этом этапе небольшие местные конкуренты имеют ограниченный выбор вариантов – или платить за межсоединения КТСОП, или приобрести услугу транзита у одного из основных операторов. Множество проблем стоит на пути реализации надежной инфраструктуры межсоединений для СПП на базе IP и организации эффективной работы этой инфраструктуры. Немалых усилий требует заключение и поддержание договоренностей по межсоединениям с другой компанией. В зависимости от обстоятельств иногда могут потребоваться технические мероприятия. Что часто упускается из виду – это расходы на административную и договорную деятельность по созданию механизмов межсоединений на базе IP. Может быть изучен один из вариантов, который предусматривает создание коммутационной станции для межсоединений на основе IP, через которую по умолчанию может осуществлять транзит IP-трафика всех операторов, при отсутствии между операторами договоренности по одноранговой связи.

3.5.3.1 Коммутационная станция для межсоединений (IE)

Основной принцип работы коммутационной станции для межсоединений состоит в том, чтобы дать возможность различным операторам присоединяться к общей точке, чтобы эффективно обмениваться взаимным трафиком. Коммутационные станции интернета могут являться одним из вариантов, который, возможно, пожелают рассмотреть регуляторные органы в качестве модели, подходящей для межсоединений с СПП.

Роль коммутационных станций для межсоединений

- Выставление счетов между операторами

В настоящее время выставление счетов между операторами является основным спорным вопросом между различными поставщиками услуг, и, видимо, он будет усугубляться, если не будут введены корректирующие меры. Обеспечить решение этой важной задачи может использование коммутационной станции для межсоединений также в качестве расчетного центра по выставлению счетов между операторами. Начисление платы между операторами может зависеть от: a) категории обслуживания; b) контента; и c) сетевых элементов, используемых при передаче трафика на коммутационную станцию для межсоединений.

- Услуги интеллектуальной сети

Услуги интеллектуальной сети в сценарии с участием многих операторов и многих услуг могли бы предоставляться с помощью объединения коммутационной станции для межсоединений/ расчетного центра по выставлению счетов между операторами.

- Переносимость номеров

Кроме того, для сценария с участием многих операторов и многих услуг можно было бы рассмотреть вопрос о переносимости номеров с помощью централизованной базы данных коммутационной станции для межсоединений/центра клиринговых расчетов по выставлению счетов между операторами.

- Упрощение

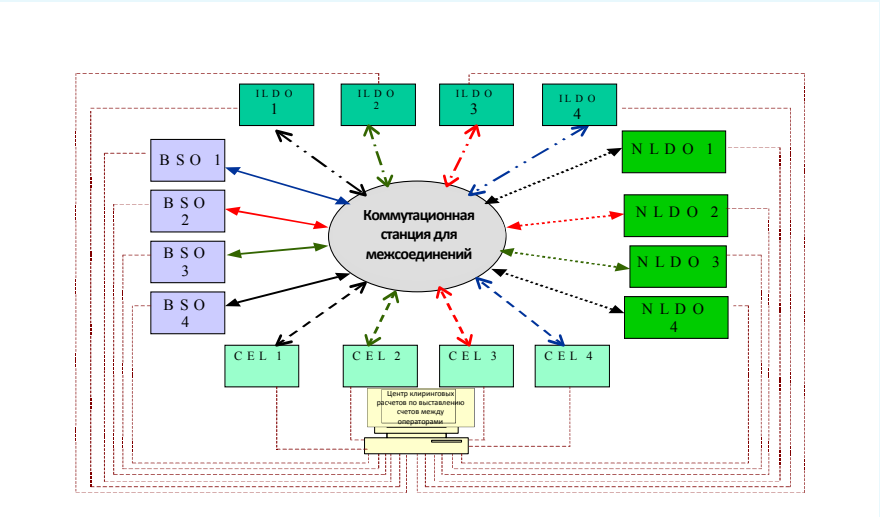
Использование коммутационной станции для межсоединений/центра клиринговых расчетов по выставлению счетов между операторами могло бы также привести к упрощению сетевой архитектуры, уменьшению количества точек присоединения (POI), упрощению расчетов по плате за использование межсоединений, а также к сокращению периодов ожидания пропускной способности для обеспечения межсоединений.

Проблемы, связанные с действующими режимами межсоединений

Действующие в настоящее время соглашения по присоединению в среде с участием многих операторов и многих услуг могут привести к следующему:

- высокой стоимости межсоединений и высокой плате за порты;
- соглашениям об асимметричном присоединении и судебным процессами ввиду неопределенности и неравных условий деятельности;
- задержке в обеспечении межсоединений ввиду ограничений, связанных с пропускной способностью;
- неоптимальному использованию ресурсов;
- неэффективному распределению вызовов;
- высоким эксплуатационным затратам по управлению расчетами между операторами;
- выставлению счетов между операторами;
- сложности расчетов по плате за использование межсоединений;
- совместному использованию интеллектуальной сетевой платформы;
- реализации переносимости номеров;
- росту капиталовложений (CAPEX) и эксплуатационных расходов (OPEX), что делает работу нецелесообразной.

Рисунок 3-2: Коммутационная станция для межсоединений



Примечание: BSO – поставщики базовых услуг/поставщики услуг фиксированных линий; CEL – сеть подвижной связи.

3.5.3.2 Местоположение точек присоединения

В настоящее время операторы взаимодействуют между собой на одноранговой основе во взаимосогласованных точках присоединения (POI). В тех районах, где операторы не могут взаимодействовать между собой на одноранговой основе, для транзита используется сеть других операторов.

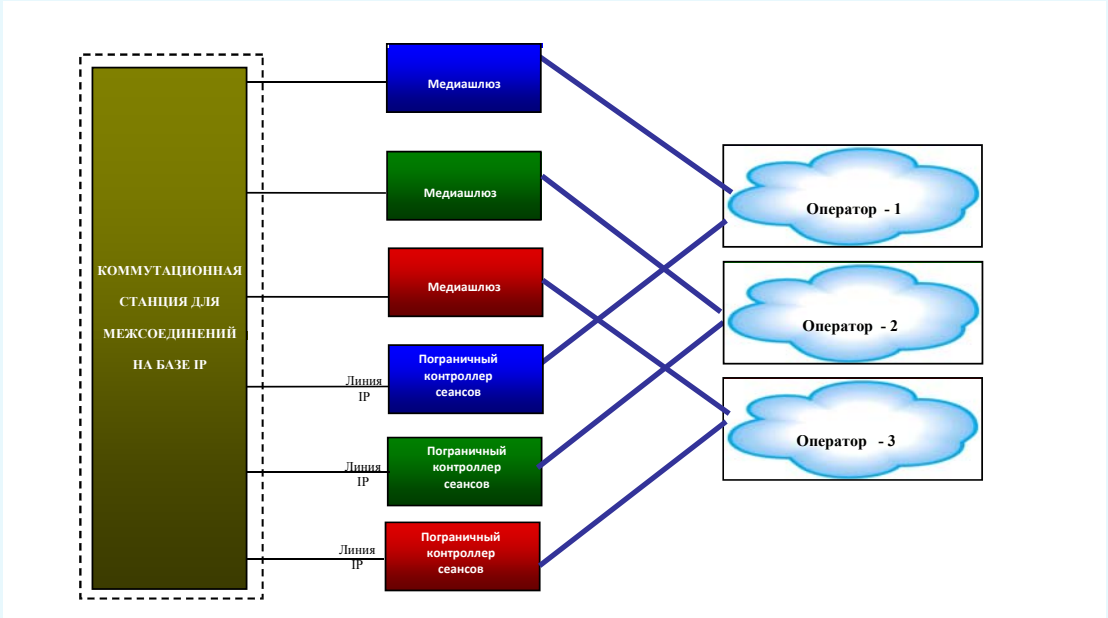
Сейчас оба взаимодействующих на равной основе партнера должны иметь коммутаторы на базе TDM в местоположениях POI. С внедрением сетей MPLS концепция стоимости передачи с учетом расстояния утрачивает свою значимость. Это ограничение исключается в СПП с их разделением функций управления и среды передачи данных и распределенной архитектурой. Для среды СПП предлагается следующая методика.

i) Операторам может быть разрешено выбирать либо централизованную контрольную точку в своей сети, контролирующую распределенные медиашлюзы, либо контроллеры SBC в зоне обслуживания.

ii) Оператору должно быть разрешено размещать медиашлюзы и/или контроллеры SBC в любом месте страны, где желательно наличие POI.

iii) Коммутационная станция для межсоединений предназначена для межсетевого соединения между различными операторами в среде СПП, как показано на Рисунке 3-3.

Рисунок 3-3: Модель коммутационной станции для межсоединений



На уровне зоны обслуживания можно создать одну или несколько коммутационных станций для межсоединений в зависимости от требований к трафику в местоположениях, где присутствует большинство операторов.

Преимущество этой модели состоит в том, что она делает сетевое планирование более эффективным. Каждый оператор знает физическое местоположение, в котором необходимо будет на более плановой основе развернуть сеть передачи, позволяющей создать точки POI.

Архитектура для межсоединений в СПП должна быть сравнимой или более прочной, чем существующая структура услуг по сетям КТСОП/ЦСИС/сетям подвижной связи, поскольку, как ожидается, СПП со временем заменят эти сети. Следовательно, одна из основных задач такой архитектуры должна состоять в восстановлении услуги при минимальном времени простоя в случае отказа в межсоединении. Это означает, что необходимо использовать отказоустойчивую многоузловую архитектуру с протоколами IP и технологиями организации сетей, специально сконфигурированных для удовлетворения этому строгому требованию.

Межсоединение в среде СПП должно действовать на двух логических уровнях: уровень сигнализации и уровень среды передачи. Чтобы свести к минимуму затраты и степень сложности при межсоединении, возможность установления соединений на уровне 2 (L2) можно предпочесть межсоединениям на уровне 3 (L3) с логическими виртуальными локальными вычислительными сетями/виртуальными частными сетями (VLAN/VPN).

Межсоединение в среде СПП обычно обеспечивает надежную среду с небольшим временем ожидания, в которой качество оптовых межсоединений гарантируется всеми операторами.

3.5.4 Плата за межсоединение

Действующая в настоящее время концепция платы за межсоединение в среде КТСОП/сети подвижной связи основана на расстоянии и времени/продолжительности вызова. В среде СПП на базе IP поставщик сети в большинстве случаев остается поставщиком услуг, но он необязательно будет единственным поставщиком услуг. Vonage, Skype и SIPgate являются примерами конкурирующих фирм, которые предоставляют услуги, не имея в эксплуатации собственной сети. В обозримом будущем скорее всего поставщики интегрированных и независимых услуг будут

сосуществовать и конкурировать в целях привлечения тех же конечных пользователей-клиентов. Это разделение функций имеет глубинные последствия как для поставщика сети, так и для поставщика услуг. Теоретически в мире, базирующемся на IP, поставщику сети безразличен характер передаваемого по ней трафика приложения; в этом контексте голосовая связь является лишь еще одним приложением.

В условиях СПП плата за межсоединение могла бы рассчитываться на основе различных моделей, включая модель "Bill & Keep" (взаимная договоренность об отсутствии платы), или в тех случаях, когда используется плата, ее размер мог бы определяться используемыми шириной полосы и приложениями, качеством предоставляемого обслуживания, количеством используемых сетевых элементов, объемом данных, которыми обмениваются во время сеанса связи, временем суток и т. д.

В сетях последующих поколений может потребоваться намного больше элементов для начисления платы, как показано ниже:

- начисление платы на основе продолжительности вызова, пропускной способности канала-носителя, времени суток, дня недели и т. д.;
- начисление платы на основе QoS, ширины полосы, приложения и т. д.;
- определение стороны, которой начисляется плата (осуществляющая вызов, вызываемая или третья сторона);
- начисление платы за дополнительные услуги и услуги с добавленной стоимостью.

Должна быть обеспечена возможность для выполнения функций по ведению записей данных о вызовах (CDR), выставлению счетов абонентам, выставлению счетов за междугородную связь, а также автоматическому дублированию и преобразованию формата.

Для направления соответствующей информации в центры, занимающиеся выставлением счетов, потребуются стандартные интерфейсы и протоколы.

В среде СПП важно разработать такой режим платы за межсоединение, который обеспечивает определенность в расчетах между операторами и способствует заключению соглашений о межсоединении. Например, в Индии в настоящее время принята основанная на затратах плата за использование межсоединений (IUC), которая включает плату за начало, передачу и завершение сеанса связи. Однако существует не менее четырех возможных моделей платы за межсоединение в сетях на базе СПП. К ним относятся следующие: 1) платит сеть вызывающей стороны; 2) взаимная договоренность об отсутствии платы; 3) плата на основе качества обслуживания; и 4) плата на оптовой основе. Работа, связанная с определением платы за межсоединение, могла бы включать оценку различных элементов затрат, относящихся к различным сетевым элементам, которые участвуют в обеспечении вызова в среде СПП, либо осуществляться на бартерной основе, либо на основе измерения передаваемого трафика (объема, уровня обеспеченного QoS и т. д.). Даже при использовании модели "Bill & Keep" некоторые страны могут продолжать применять взимание с операторов платы, которая выплачивается оператором происхождения вызова поставщику доступа. В тех случаях, когда плата за межсоединение определяется на основе сетевых элементов, необходимо прилагать все усилия к тому, чтобы точно оценить стоимость соответствующих сетевых элементов на основе вкладов, предоставляемых различными операторами. Важно выявить те сетевые элементы, которые участвуют в завершении междугородного вызова от его начала до пункта назначения в среде с участием нескольких операторов.

Переход к СПП окажет значительное влияние на затраты в сети и на взаимосвязь между затратами по передаче трафика и расстоянием, на которое данный трафик передается. Из-за сходства СПП и интернета возник вопрос о том, не приведет ли переход к СПП к "кончине фактора расстояния", учитываемого в плате за межсоединение. Если плата за интернет, как правило, не зависит от расстояния, на которое передаются данные, то в случае СПП затраты в сети, связанные с расстоянием, могут стать намного ниже. Поэтому плата за межсоединение, определяемая на

основе затрат, поможет обеспечить правильную нормативно-правовую базу, способствуя более быстрому развертыванию СПП на рынке.

Четыре основных элемента платы за межсоединение в режиме СПП

В интернете о некоторых вещах известно на уровне приложения или услуги, а на уровне сети известно о совсем иных вещах. В режиме VoIP сервер, осуществляющий протокол наподобие SIP, знает время начала сеанса и может знать время его окончания, но практически ничего не знает о задействованных между этими двумя моментами сетевых ресурсах. Будет известно топологическое местоположение (логическое местоположение в сети) оконечных точек начала и завершения вызова, но географическое расположение может оставаться неизвестным. Наряду с этим сеть на базе IP будет иметь дело со значительно более широким кругом приложений, чем только традиционная передача голоса. Идея, согласно которой следует считать, что затраты создаются инициатором вызова, в целом неверна. В общем случае очевидный "верный ответ" на вопрос о том, как распределить затраты среди конечных пользователей, отсутствует. Базовой сети известны совсем другие вещи. В среде на базе IP каждая IP-дейтаграмма адресуется по отдельности и, в принципе, может иметь отдельный маршрут (хотя на практике маршрутизация является значительно стабильнее, чем можно предположить на основе вышесказанного). Относительно простые приложения могут генерировать очень большое число IP-дейтаграмм. Для целей учета эти данные необходимо обобщать, в противном случае системы учета захлебнутся в неуправляемых объемах информации. По аналогичным причинам обычной практикой является измерение трафика по определенной линии передачи данных "точка–точка", а создание матрицы совокупного трафика на основании пунктов назначения сквозного трафика было бы дорогостоящим и обременительным мероприятием.

3.5.4.1 Платит сеть вызывающей стороны (CPNP)

Принцип CPNP, при котором за вызов платит сеть, инициирующая этот вызов, основывается, как правило, на продолжительности вызова; обычно сторона, которая принимает (завершает) вызов, ничего не платит. В сетях на базе IP начисление платы может осуществляться на основе количества переданных пакетов данных, а не на основе продолжительности вызова. Эта система может принимать форму начисления платы на основе элементов (EBC) или начисления платы на основе пропускной способности (CBC). Обе эти системы образуют системы, основывающиеся на затратах.

Ограничения

- При начислении платы на основе элементов (EBC) скорость межсоединения зависит от количества сетевых элементов. Реализация системы EBC (или CBC) в IP-сетях повлечет за собой транзакционные издержки (например, для определения точек межсоединения IP).
- Монополия на завершение вызова.

3.5.4.2 Взаимная договоренность об отсутствии платы (Bill & Keep)

При этом режиме плата за завершение вызова отсутствует. В основном система "Bill & Keep" представляет собой своего рода бартерный обмен, при котором оператор *A* в своей сети завершает трафик, поступающий из сети оператора *B*, и наоборот. Поскольку потоки трафика могут уравновешиваться в обоих направлениях, то платежи не осуществляются, а цена для оператора *A* за завершение своего трафика в сети *B*, включает элемент *предоставления пропускной способности сети* для завершения трафика, поступающего от оператора *B*. В этом смысле услуги по межсоединению не являются бесплатными.

В режиме "Bill & Keep" транзакционные издержки можно сократить, и отсутствует проблема монополии на завершение вызовов. Отсутствие платежей за услуги по завершению вызовов позволяет избежать проблемы арбитража.

Ограничения

- В случае системы "Bill & Keep" поставщики услуг заинтересованы в том, чтобы как можно скорее передать свой трафик в другую сеть для завершения вызова, что создает эффект "горячей картофелины". Для преодоления этой проблемы может быть целесообразным устанавливать требования в отношении минимального количества и размещения точек присоединения, с тем чтобы такая система могла применяться к какому-либо конкретному сетевому оператору.

3.5.4.3 Плата на основе качества обслуживания

Если два поставщика услуг пожелают компенсировать друг другу издержки по передаче трафика, чувствительного к задержке с предпочитаемым качеством обслуживания, то каждый из них захочет проверить, как другая сторона выполняет взятые на себя обязательства

При использовании системы на основе QoS это, по-видимому, повлечет за собой проведение измерений: 1) объема трафика каждого класса обслуживания, которым обмениваются в каждом направлении поставщики услуг; и 2) показателей качества фактически предоставленного обслуживания. Измерение QoS намного сложнее как в техническом, так и в коммерческом плане.

Ограничения

- Обязательства, которые берут на себя поставщики услуг, касаются прежде всего показателей средней задержки и отклонений от нее. Во-первых, важно помнить, что измерение этих показателей подразумевает определенную степень сотрудничества между сетевыми операторами, которые непосредственно конкурируют между собой за привлечение одних и тех же клиентов – конечных пользователей. Ни один из операторов не будет с готовностью раскрывать конкуренту внутренние эксплуатационные характеристики своей сети. И ни один из них не захочет, чтобы другая сторона раскрывала перед возможными клиентами какие-либо недостатки его сети.
- Во-вторых, могут возникнуть опасения в связи с тем, что измерительные серверы, эксплуатируемые в своей собственной сети в интересах конкурента, могли бы стать настоящим "оперативным кошмаром" или, возможно, поставить под угрозу систему безопасности в рамках собственной сети.

3.5.4.4 Плата на оптовой основе (можно также называть "отель для межсоединений")

Традиционный режим платы за межсоединения, а именно на поминутной основе, несомненно, усложняет бесперебойное урегулирование требований об оплате. Причина состоит в том, что продукты СПП основаны на таких показателях, как пропускная способность, качество обслуживания и класс обслуживания. Поскольку объединение трафика осуществляется в общем узле, необходимо санкционировать начисление платы за межсоединения для СПП на оптовой, а не на поминутной основе, как это делается в большинстве случаев в настоящее время. В условиях СПП общие затраты в сети и затраты по передаче трафика становятся намного ниже по отношению к объемам трафика и, соответственно, снижается средний уровень затрат в сети, связанный с каждой единицей трафика. Начисление платы за межсоединения на оптовой основе устанавливало бы четкие и равные условия для операторов и содействовало бы экономии судебных издержек и времени, затрачиваемого на урегулирование нежелательных тяжб и споров.

В связи с этим необходимо также определить, какие вопросы следует урегулировать и какие вопросы можно оставить для решения путем взаимных переговоров.

3.5.5 Экономические последствия договоренностей по вопросам межсоединений

СПП обещают более простые сетевые архитектуры, более высокие значения ширины полосы, меньшее количество элементов сети, снижение затрат и более широкие функциональные возможности. Кроме того, разграничения транспортировки и услуг сделают возможным

независимое развитие бизнес-моделей, сетевых элементов сети и приложений. Следовательно, переход к сетям последующих поколений подразумевает технологические изменения, изменения предлагаемых на рынке продуктов и услуг и, в конечном счете, структуры рынка в связи с внедрением сетей (доступа) последующих поколений. Кроме того, сети СПП и NGA также влияют на способ расчета затрат из-за появления новых источников затрат и соотношений стоимость/объем (CVR). Расчет затрат на нормативно-правовой основе и режим начисления платы должны отражать эти изменения. Очевидно, при подходе к затратам, ориентированном на голосовую связь в сетях электросвязи, созданных в прошлом, необходимо учитывать растущую роль передачи данных и тот факт, что голосовая связь становится "еще одним видом передачи данных". Это предполагает существенные изменения во взглядах и анализе затрат в среде СПП.

Если посмотреть на развитие тарифных структур для новых розничных услуг на рынке (в частности в связи с увеличением групп тарифов и тарифов единой ставки) и на новые формы использования, то рост мобильного широкополосного доступа и IP-телевидения больше всего влияет на изменение архитектуры сети в нужную сторону и оказывает воздействие на уровень затрат и структуры затрат операторов. С увеличением трафика передачи данных в сетях, полностью основанных на IP, которые совместно используют несколько услуг, фиксированные расходы в меньшей степени распространяются на голосовые услуги. Это означает, что эффект масштаба, стимулируемый ростом трафика данных, позволяет снизить затраты на голосовые услуги.

Введение в эксплуатацию сетей СПП и сетей на основе IP предполагает, что сети станут более централизованными, чем в настоящее время. Это, вероятно, должно стимулировать внедрение меньшего количества POI. Важно, чтобы нормативно-правовая база, например в отношении структур и уровней тарифов, учитывала такое развитие событий.

Еще одним экономическим результатом, связанным с переходом к СПП, является разделение уровней сети и уровней услуг в IP-сетях, что подразумевает новые соотношения "стоимость–объем" (CVR), по мере снижения затрат на передачу (благодаря сетям, полностью основанным на IP, извлекая выгоду из экономии за счет масштаба производства и диверсификации услуг), тогда как расходы на уровень управления и платформы услуг возрастают (за счет дополнительных инвестиций в программные коммутаторы и платформы IMS). Поскольку уровень управления и уровень обслуживания имеют общие нагрузку на сеть, число активных конечных пользователей, количество установленных соединений (вызовов) и сигнализации в качестве источника затрат, то такое разделение может мотивировать введение в действие новых режимов начисления оплаты.

Переход к IP-межсоединениям, по всей вероятности, можно было бы ускорить путем отказа от принципа технологической нейтральности и убеждения операторов использовать межсоединения на основе IP. Это может быть реализовано как часть режима соискатель/поставщик, введя требование о том, что когда соискатель запрашивает IP-межсоединение, другой оператор обязан его предоставить. Преимуществом такой структуры является то, что IP-межсоединения будут определяться требованиями самых продвинутых операторов. В противном случае не произойдет крупномасштабного перехода на IP-межсоединения, пока не проявят интерес крупные операторы. Однако в связи с введением IP-межсоединений возникает ряд вопросов, включая вопрос о том, как сформулировать стандартное предложение и как регулировать плату за использование межсоединения и плату за линии межсоединения.

В связи с тем что в настоящее время существует большое количество POI, некоторые операторы хотели бы подумать над тем, как уменьшить количество POI в СПП, потому что это положительно повлияет на существующую расстановку сил среди операторов и будущее управление качеством обслуживания, но по ряду причин это не должно быть сделано путем быстрых изменений количества POI и архитектуры POI.

В настоящее время большинство поставщиков услуг переходят к сетям на основе IP. В то время как голосовой трафик внутри сети передается по IP, межсетевые соединения по-прежнему базируются на технологиях TDM и CS#7. Тем самым демонстрируются элементы неэффективности, так как это приводит к множеству преобразований между сетями с коммутацией пакетов и сетями с

коммутацией каналов при обработке трафика двумя или более сетями. Пока действует существующая структура межсоединений с несколькими уровнями точек присоединений, маршрутизация вызова является неэффективной. Еще одним негативным результатом являются препятствия для использования всех преимуществ СПП, в том числе создания новых услуг и формирования новых бизнес-моделей.

В целях повышения эффективности в будущем вместо технологии TDM должны быть реализованы межсоединения на основе IP. На сегодняшний день существующие поставщики услуг внедрили метод межсоединений на основе TDM. Если эти сети будут переводиться на IP-межсоединения, то потребуются дополнительные инвестиции. Таким образом, должен быть достигнут баланс между одноразовыми инвестициями при переходе от TDM к IP-межсоединениям, с одной стороны, и потенциальным увеличением статической и динамической эффективности, которая достигается в результате этого перехода. Поскольку расходы в основном ложатся на поставщиков традиционных услуг, то стимулы для перехода на IP-межсоединения ограничены.

3.6 Законодательная база для СПП

Для развертывания СПП необходимы высокие авансовые расходы. Прежде чем вкладывать столь значительные средства, инвестор потребует наличия стабильной нормативно-правовой и законодательной среды. Проблемы и препятствия нормативно-правового характера, связанные с переходом к СПП, появление новой категории поставщиков услуг, изменение бизнес-моделей, риски, связанные с сетевой безопасностью, конкуренция и создание равных условий для участников и т. д. должны решаться на приоритетной основе. До тех пор пока не будут должным образом пересмотрены условия лицензирования и регуляторные положения, трудно будет стимулировать плавный переход к СПП. Принимая во внимание все вышеуказанные вопросы и с учетом того, что сети и инфраструктуры в различных странах находятся на этапе быстрого развития, самое время рассмотреть вопросы регулирования и лицензирования, связанные с СПП. Это позволит не только более внимательно познакомиться с лицензированием и нормативно-правовой базой, но и способствовать снижению инвестиционных рисков для операторов. Первоначально нормативно-правовая база в различных странах регулировала деятельность поставщиков услуг доступа (т. е. операторов основных услуг и операторов услуг сотовой подвижной электросвязи), поставщиков услуг междугородной связи и услуг доступа в интернет (ISP). Виды услуг по каждой лицензии были жестко определены, и вероятность попадания любой отдельной услуги в сферу действия других лицензий электросвязи была очень невелика. Затем появилась единая лицензия на оказание услуг доступа, в соответствии с которой получатель лицензии мог предоставлять различные услуги доступа, т. е. услуги фиксированной связи и доступа в интернет. Столь эффективно развивающаяся структура лицензирования позволила привлечь серьезные инвестиции в индустрию электросвязи, результатом чего стал масштабный рост сектора, улучшение качества обслуживания, конкуренция, возможность выбора для клиента и прежде всего широкий охват услугами электросвязи географических территорий и населения. Быстрый рост электросвязи в рамках сектора одновременно свидетельствовал о высокой скорости технического прогресса. Передовая архитектура и иерархия сети способствовали предоставлению новых услуг и приложений без каких-либо затруднений, что невозможно было представить ранее, когда услуги были жестко привязаны к типу установленных коммутаторов (станций). Новые разработки способствуют появлению большого количества услуг и приложений за дополнительную плату, которые могут быть предоставлены с использованием различных платформ, размывая границы между различными лицензиями. Например, поставщикам услуг интернета разрешено предоставление услуг широкополосной связи, но та же платформа поддерживает также и интернет-телефонию. IP-телевидение и многие другие услуги класса triple play (пакета из трех услуг), предоставляемые обычно по лицензии поставщика услуг доступа, технически могут предоставляться поставщиками услуг интернета (ISP) поверх услуг широкополосной связи. Главная задача, стоящая перед регуляторными органами, – это как сохранить баланс между существующей нормативно-правовой базой и быстрым техническим прогрессом, происходящим в секторе электросвязи. Привязанность к существующей нормативно-

правовой базе может ограничить для массового потребителя пользование плодами технического прогресса, в то же время разрешение применения новых технологий и приложений и стимулирование использования IP-сетей противоречит положениям существующего законодательства и может повлиять на сохранение равных условий для участников. Пока сторонники одной концепции поддерживают поощрение перехода к СПП, поскольку эти сети являются удобными для пользователей и позволяют клиентам получить доступ к новым дополнительным услугам и приложениям по более низкой цене, другие полагают, что СПП являются ничем иным, как техническим достижением, и, следовательно, как считают они, юридических оснований для перехода нет. Решение о том, переходить к СПП или нет, имеет коммерческую подоплеку, и поэтому, по их мнению, оно может быть предоставлено поставщикам услуг. По их словам, не следует вмешиваться в существующую, проверенную временем структуру лицензирования.

Переход к СПП подразумевает, что границы между различными бизнес-моделями, услугами и рынками будут постепенно исчезать. Для того чтобы справиться с этой ситуацией, режим лицензирования должен содержать универсальные лицензии для сетевых операторов, позволяя последним предлагать любые услуги и приложения на базе IP в единой сети, полностью основанной на IP.

Одним из основных вопросов, который необходимо рассмотреть при внесении поправок в лицензирование, является вопрос об утвержденных IP-межсоединениях. Кроме того, существуют некоторые незначительные вопросы, касающиеся лицензирования, которые могут иметь негативные последствия для поставщиков услуг, но не представляющие серьезных препятствий для перехода к СПП.

Изменения режима лицензирования, полностью нейтрального в технологическом плане, важны для перехода к СПП, и они также технологически нейтральны, так что нет необходимости ждать дальнейшего технологического или рыночного прогресса.

Интересным вопросом является обсуждение роли нормативно-правовой базы для стимулирования и укрепления СПП. Сети СПП представляют собой значительные изменения на рынке, вызванные техническими и экономическими процессами. В условиях конкуренции СПП нуждаются в определенной структуре, однако возникает вопрос, может и должна ли такая структура быть заранее определенной или же должны преобладать рыночные механизмы, а регулирование должно активизироваться лишь в случае затруднений в развитии конкуренции.

Роль регулирования состоит в том, чтобы поэтапно двигаться вперед в случае сбоев механизмов рынка, например при злоупотреблениях господством на рынке или лишении права выхода на рынок. Это казалось "естественным" развитием во времена становления открытого рынка, когда существовала опасность того, что законные монополии станут фактическими монополиями, несмотря на официальную открытость рынка. Сегодня ситуация другая. Регулирование должно быть оправдано сбоями рынка. Переход к СПП не связан с рыночными сбоями, нарушениями конкуренции или лишением права выхода на рынок. Такие результаты вероятны в зависимости от ситуации на местах, но никакой очевидной связи между переходом к СПП и, например, господством на рынке не существует. Таким образом, любая попытка "планировать" переход к СПП с точки зрения регулирования должна предприниматься с большой осторожностью. В качестве альтернативы можно сначала позволить работать рыночным механизмам, а вмешиваться затем только в том случае, если рынок не выполняет своих функций. Это также будет означать, что переход на СПП следует дорожной карте, определяемой технологиями и рынком, а не регуляторными положениями.

4 Анализ развертывания СПП

4.1 Цели развертывания СПП

Сценарии и план перехода должны приниматься в зависимости от ситуации в каждой стране или от конкретного оператора. В общем существуют две точки зрения высокого уровня, которые следует учитывать при необходимости перехода.

Согласно первой точке зрения, переход к СПП рассматривается как способ усовершенствования инфраструктуры. В этом случае план перехода должен быть направлен на замену существующих сетей электросвязи так называемыми "сетями, полностью основанными на IP", включая интенсивное развертывание "широкополосного доступа".

С другой точки зрения, переход к СПП рассматривается в качестве фактора, способствующего развитию общества, в частности стимулирования создания "электронного общества". В этом случае план перехода должен быть направлен на поддержку конвергенции, в частности конвергенции сетей фиксированной и подвижной связи, а также поддержку различных приложений (например, электронное здравоохранение, USN и т. д.).

Рекомендуется комбинировать данные этих подходов с соблюдением баланса в зависимости от ситуации в каждой стране и конкретного оператора.

4.2 Изучение накопленного опыта

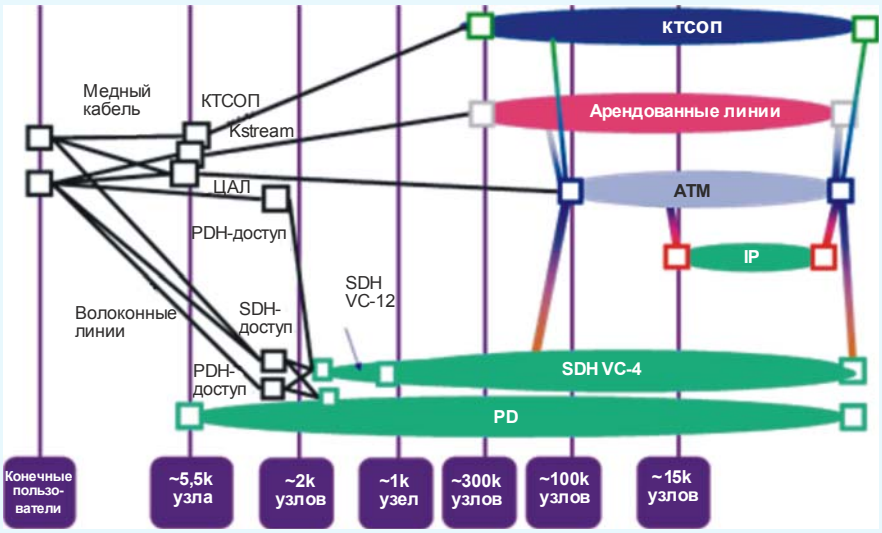
4.2.1 Совершенствование инфраструктуры

Одним из примеров передового опыта перехода к СПП, объявленного компанией BT, является проект под названием "Сеть XXI века", в котором ключевую роль играют сети BT, предназначенные для работы в XXI веке. Один из интересных моментов, связанных с планами развития сети XXI века компании BT, – это структура существующих сетей и сети XXI века. Это дает нам очень важную информацию о преимуществах внедрения СПП, особенно для сетевых операторов.

Далее на Рисунке 4-1 показаны структуры действующих сетей компании BT, включающие различные сети передачи и разнообразные узлы, выполняющие разные функции в соответствии с услугами, за которые они отвечают, и географическим расположением. Для базовой сети также существуют разные сети, поддерживающие различные виды маршрутизации в соответствии с особенностями конкретных услуг.

Подобная структура и конфигурация сети, ориентированные на оказание услуг, являются причиной дублирования элементов инфраструктуры, в частности передающих узлов или узлов маршрутизации. Кроме того, она требует усложненной схемы функционирования служб и сетей, поскольку в предоставлении конкретных услуг участвуют различные системы. Эти аспекты требуют более значительных инвестиций, что может привести к дублированию предоставления услуг и потребовать дополнительных ресурсов для целей эксплуатации и обслуживания, что в свою очередь вызовет больший расход людских и финансовых ресурсов.

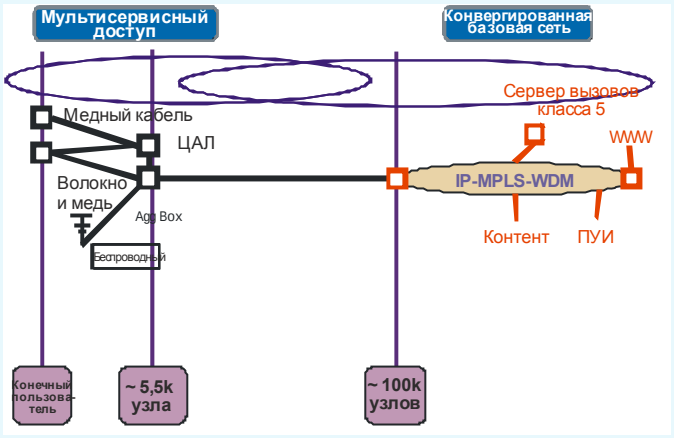
Рисунок 4-1: Существующие сервисные структуры компании BT с рядом узлов



В отличие от действующей сетевой конфигурации компании BT сеть XXI века имеет довольно простую структуру, но более широкие функциональные возможности не только в отношении голосовых услуг, но и для услуг широкополосного доступа. На Рисунке 4-2 приведена простая модель конфигурации сети XXI века. На Рисунке 4-1 показана простота структуры и особенно заметное уменьшение количества узлов при сохранении масштабного охвата клиентов. Эта структура использует преимущества характеристик сети, полностью основанной на IP, что позволяет построить простую конфигурацию базовых сетей, и поэтому все услуги должны маршрутизироваться базовыми IP-сетями с различными потоками, которые обрабатываются отдельно от управления трафиком и аспектов предоставления услуг, но используют одни и те же системы.

Еще одним преимуществом этой структуры является сокращение и расширение контактных точек клиентов, что позволяет осуществлять более полный охват клиентов. Именно по этой причине данная структура сохраняет большую часть узлов на стороне клиента при одновременном удалении других узлов из предыдущей структуры.

Рисунок 4-2: Сетевые структуры компании BT с рядом узлов (сети XXI века)



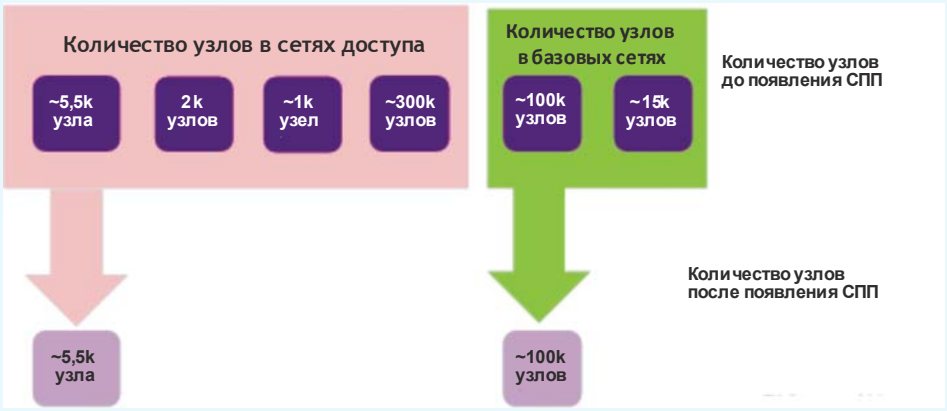
Внедрение СПП в сети компании BT под названием "Сеть XXI века" показывает, как инфраструктура может быть усовершенствована в целях удовлетворения будущим тенденциям развития предпринимательской деятельности и требованиям пользователей и операторов. Необходимо внимательно рассмотреть путь реализации СПП компанией BT и извлечь уроки из аспектов усовершенствования инфраструктуры.

В одном из отчетов говорится о том, что эта новая структура позволит на 30–40% уменьшить выбросы парниковых газов, которые в настоящее время становятся серьезной проблемой для всего мира. Простые расчеты подтверждают выводы, содержащиеся, в докладе:

- уменьшение количества узлов доступа с 8,8 тыс. узлов до 5,5 тыс. узлов (снижение на 37,5%);
- уменьшение количества базовых узлов со 115 до 100 узлов (снижение на 14%).

В настоящем отчете мы не пытаемся оценить этот результат с точки зрения затрат, однако это, как правило, предполагает огромную экономию средств, включая затраты на эксплуатацию каждого узла.

Рисунок 4-3: Выгоды компании BT от внедрения сетей XXI века



4.2.2 Стимулирование развития общества

Другим видом перехода к СПП является обеспечение инфраструктуры для построения нового общества, в частности электронного общества. Такой подход был заявлен Республикой Корея в проекте под названием "BcN: широкополосные конвергированные сети", который в настоящее время реализуется в Республике Корея.

Одной из отличительных особенностей корейского варианта является то, что запускают этот проект практически на завершающем этапе развертывания сетей широкополосной связи. Поэтому их видение BcN совершенно другое, чем у компании BT. Основными пунктами являются следующие:

- построить новейшую информационную инфраструктуру в мире;
- создать среду для использования мультимедийных услуг высокого качества;
- подготовить базовый план в соответствии с ростом рынка отрасли ИТ.

Как показывают эти концептуальные заявления, Корея сосредоточивает свои усилия скорее на создании новой социальной инфраструктуры, тогда как деятельность компании BT основное внимание уделяет совершенствованию своей инфраструктуры. Таким образом, Корея использует модель, основанную на распределении ролей, где у каждого сектора имеется своя роль. В соответствии с этой моделью правительство выполняет функцию стимулирования разработки новых услуг и приложений, которые будут использоваться для построения электронного общества,

таких как электронное обучение, электронное здравоохранение, USN и т. д. Операторы сети уделяют большое внимание модернизации своей инфраструктуры для поддержания услуг конвергенции, в частности услуг FMC и IPTV, в то же время продолжая расширять возможности сетей доступа, чтобы обеспечить бóльшую ширину полосы для клиентов.

5 Ситуационные исследования

5.1 Ситуационные исследования по инвестициям в LLU и волоконно-оптические сети

ICTA, национальный регуляторный орган (NRA) Турции, принял решение об инвестициях в развитие волоконной оптики. Согласно опубликованному 3 октября 2011 года решению ICTA операторы, вкладывающие средства в развитие волоконно-оптических сетей, освобождаются от каких-либо обязательств на период в 5 лет, или до тех пор, пока число абонентов розничных услуг не достигнет уровня 25% от общего числа абонентов широкополосного доступа. Это означает, что в течение этого периода услуги волоконных сетей не будут оцениваться в каких-либо определениях рынка. Турция все еще находится в процессе перехода от существующих сетей к СПП. В начале процесса перехода, по заявлению Turk Telekom – действующего оператора услуг фиксированной связи, в ICTA проведен весьма глубокий анализ ситуации. В течение периода оценки в ICTA также обсуждался вопрос о том, как можно наилучшим образом активизировать развертывание оптоволоконной инфраструктуры и ее распространение в кратчайшие сроки посредством содействия операторам в инвестировании средств.

В течение пятилетнего периода компания Turk Telekom также будет предоставлять оптовые услуги через оптоволоконную инфраструктуру путем перепродажи для клиентов доступа к битовым потокам на равных условиях и без дискриминации. С другой стороны, регуляторные положения в области развертывания волоконных сетей не должны противоречить приоритетным приложениям. Законодательные акты, принятые в качестве приоритетных, должны поддерживать льготы для волоконной оптики.

Решение турецкого регуляторного органа о предоставлении льгот для волоконных сетей может рассматриваться в качестве альтернативного метода стимулирования операторов для инвестиций в волоконную оптику и возврата инвестиций в максимально короткий и разумный период времени. Тем не менее выводы и результаты этого решения о предоставлении льгот должны, безусловно, контролироваться. Мы должны иметь в виду, что все подходы, необходимые в новой ситуации, включают некоторые риски и могут привести к отрицательным последствиям. Тем не менее, мы считаем, что вышеуказанное решение турецкого национального регуляторного органа о льготах может быть принято в качестве ролевой модели для ряда стран, имеющих структуру рынка, аналогичную турецкой.

Это регуляторное положение направлено на защиту инвестиций, чтобы не препятствовать распространению волоконной оптики. В заключение в процессе внедрения волоконной оптики страны должны провести анализ своей структуры и инфраструктуры рынка. Национальные регуляторные органы в странах должны найти способ защиты инвестиций, соответствующий их собственной структуре рынка, особенностям инфраструктуры и благосостоянию страны.

5.2 Ситуационные исследования по развертыванию СПП

МСЭ недавно запустил проект для развивающихся стран в Азиатско-Тихоокеанском регионе с целью получения оценки технических и регуляторных аспектов перехода к СПП на основе опыта конкретных стран. Задачей проекта является также содействие наращиванию потенциала в переходе к среде СПП с помощью семинаров и профессиональной подготовке по соответствующим вопросам, связанным с СПП в Азиатско-Тихоокеанском регионе, а также распространение

ситуационных исследований на тему СПП путем содействия механизму сотрудничества. Отчет о передовом опыте реализации СПП в Азиатско-Тихоокеанском регионе – ситуационные исследования по Индии, Филиппинам, Шри-Ланке и Бангладеш – можно найти в онлайновом режиме по адресу: http://www.itu.int/ITU-D/tech/NGN/CaseStudies/CaseStudies.html.

6 Метод перспективных технологий и состояние развития СПП

6.1 Метод определения наиболее перспективных технологий построения СПП

Эта методика основана на принципе моделирования построения или реорганизации инфокоммуникационной сети для оценки стоимости и продолжительности перехода к использованию определенного набора технологий, которые отвечают всем требованиям владельца сети.

На Рисунке 6-1 показан обобщенный алгоритм метода. Этот алгоритм включает четыре параллельные (независимые) подготовительные процедуры, результаты которых затем используются при определении наиболее перспективных с точки зрения стоимости и срока строительства (реорганизации) вариантов построения инфокоммуникационной сети.

Первая из четырех процедур (обозначена цифрой 1 на Рисунке 6-1) состоит из двух основных этапов: ввод информации о структуре существующей или проектируемой сети и выделение независимых сегментов сети, которые должны быть построены. Первый из этих этапов включает постепенное введение информации о каждом элементе сети (оборудовании или канале связи) для тех уровней, о модернизации или построении которых идет речь. Кроме типа и технических характеристик каждого элемента на этом этапе должна быть введена информация о взаимном соединении элементов друг с другом через специальные интерфейсы (как в пределах того же уровня, так и с оборудованием других уровней).

Вторая процедура (обозначена номером 2 на Рисунке 6-1) предназначена для выделения из совокупности наборов технологий, которые сегодня можно рассматривать в качестве перспективных для модернизации или построения инфокоммуникационной сети, только тех наборов, которые отвечают требованиям владельца сети. Данная процедура состоит из трех основных этапов: формирование требований к сети на всех уровнях, экспертная оценка существующих наборов технологий построения инфокоммуникационных сетей и оценка соответствия перспективных технологий требованиям к проектируемой сети. В результате выполнения этой процедуры должен быть получен список тех наборов технологий (для каждого из уровней сети), которые полностью отвечают требованиям, установленным для этой сети ее владельцем. Переход к этим наборам технологий на последующих этапах методики будет аналогичным с точки зрения стоимости и продолжительности реорганизации для каждого из них.

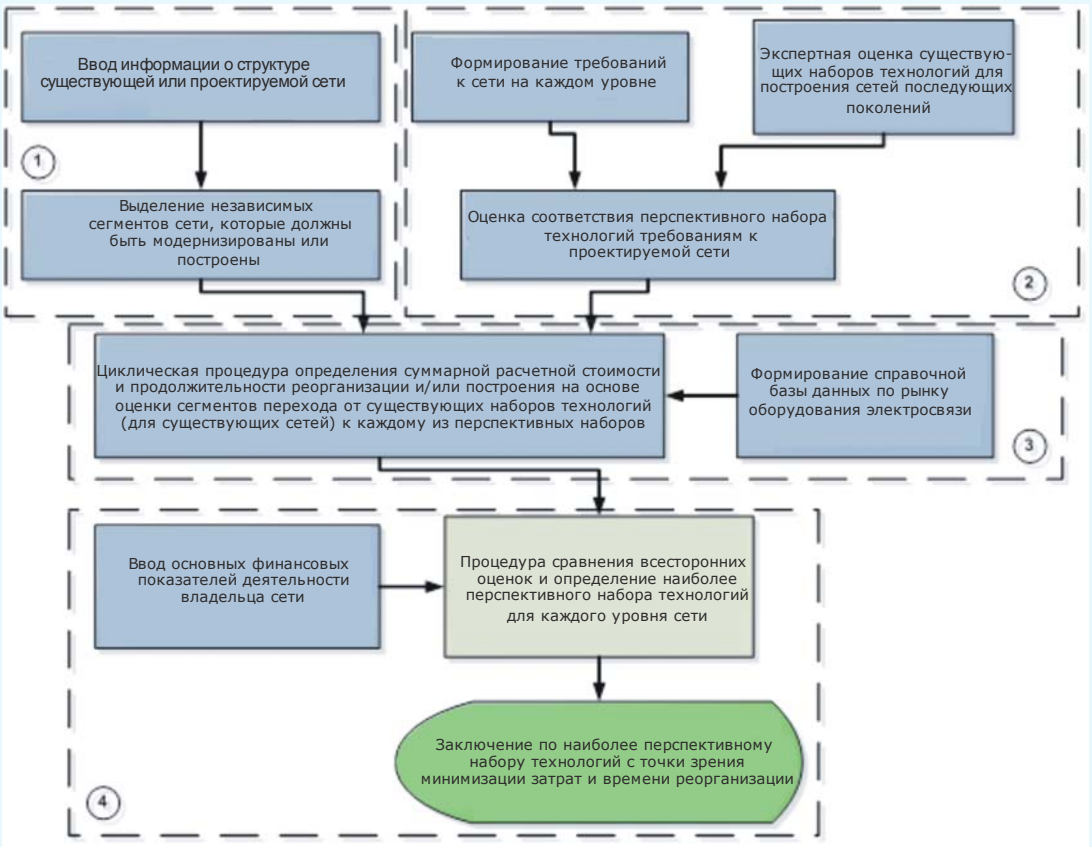
Третья процедура (обозначена цифрой 3 на Рисунке 6-1) является наиболее сложной с точки зрения количества операций. Эта процедура включает циклический перебор всех выбранных независимых сегментов (которые подлежат модернизации или построению) для последовательной оценки их перевода на новые перспективные наборы технологий (или построения сети с использованием этих наборов технологий). Различие между модернизацией существующей сети и построением новой заключается, в первую очередь, в том, что при обновлении действующей сети учитываются дополнительное время и затраты на демонтаж существующего оборудования и/или существующих каналов связи. Основой для этой процедуры является специально созданная информационная база данных о рынке оборудования электросвязи, которая включает информацию о возможной взаимозаменяемости моделей друг с другом. Результатом этой процедуры является вектор стоимости и продолжительности модернизации (или построения) сети (по ее уровням) с использованием набора перспективных технологий.

Последняя процедура алгоритма (обозначена цифрой 4 на Рисунке 6-1) включает определение наиболее перспективного набора технологий на каждом уровне сети на основе сравнения затрат и продолжительности модернизации (или построения) с учетом основных финансовых показателей

деятельности владельца сети по основному направлению (например, путем определения сроков окупаемости оператора сети электросвязи).

Следует также отметить, что алгоритм, приведенный на Рисунке 6-1, показывает только общий принцип определения набора перспективных технологий, а его спецификация для конкретных условий (создание новой сети или реорганизация существующих, построение сетей на различных уровнях и т. д.) предполагает использование подробных алгоритмов.

Рисунок 6-1: Обобщенный алгоритм метода



6.2 Текущее состояние развития СПП

Базы данных МСЭ, в особенности базы данных по тарифной политике, демонстрируют различную полезную статистику. Целью этой базы данных является отслеживание и демонстрация тенденций применения тарифной политики в отношении ценообразования, моделей стоимости/тарифных планов, аналитического учета, платы за межсоединения, управления универсальными услугами и контроля за ценами в разных странах. Данные предоставляются ежегодно регуляторными органами по электросвязи и операторами сетей. Это позволяет отражать положение дел в регионах на дату заполнения вопросника. Далее на Рисунках от 6-2 до 6-4 приводятся статистические данные, особенно в отношении сетей последующих поколений, поступающие из Всемирной базы данных МСЭ по тарифной политике[3].

[3] См. Дополнительную информацию в разделе "Око ИКТ": http://www.itu.int/icteye

Рисунок 6-2: Стадии внедрения системы СПП операторами

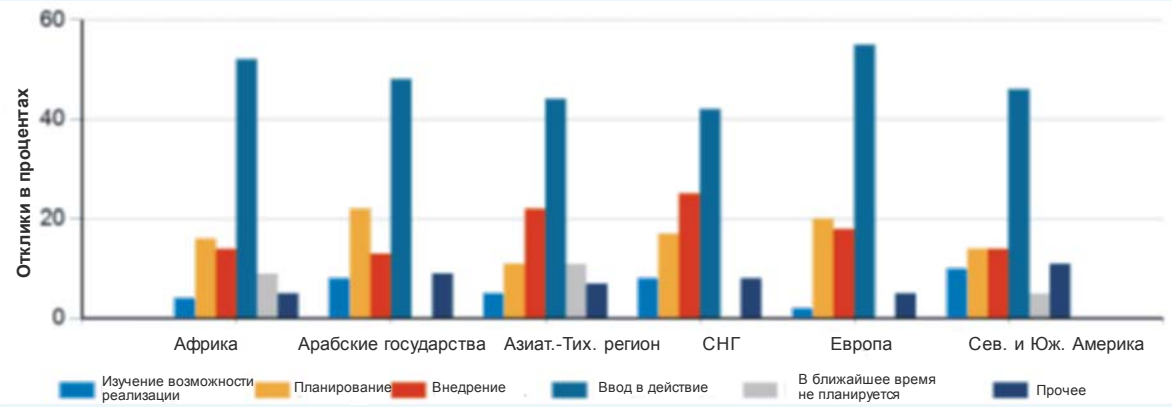


Рисунок 6-3: СПП: регулирование использования сетей IP для услуг голосовой связи, 2012 год

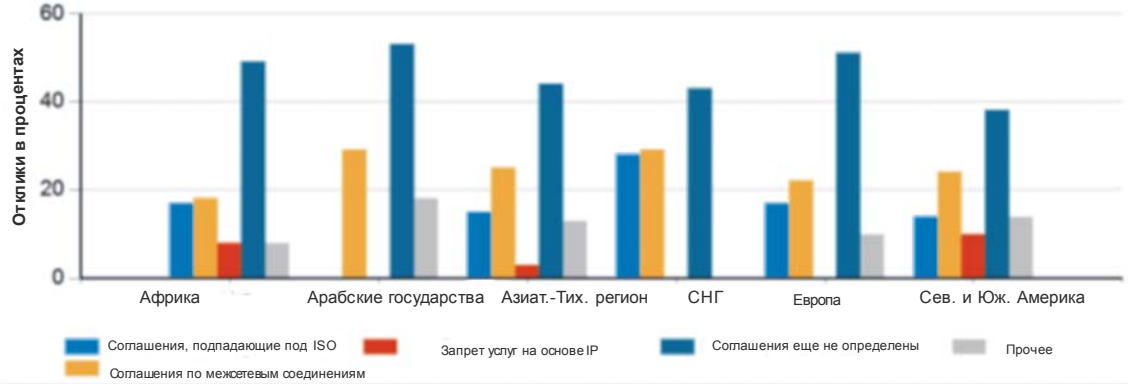
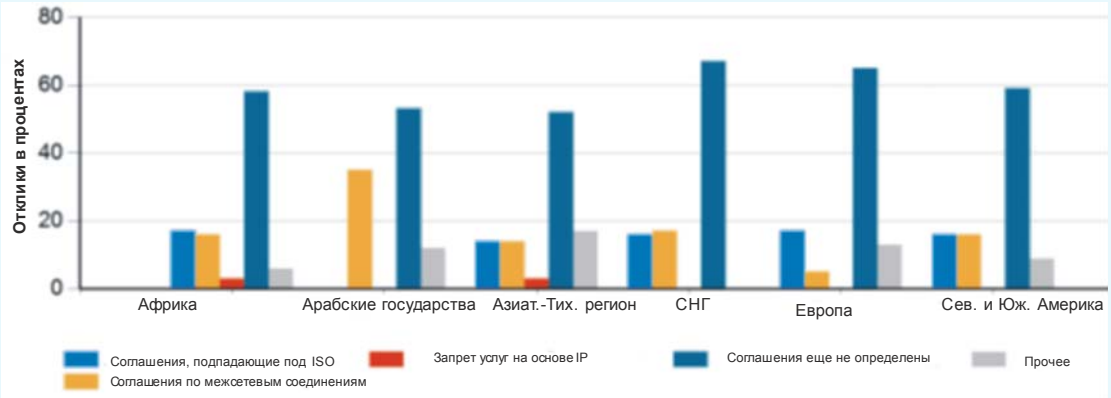


Рисунок 6-4: СПП: регулирование использования сетей IP для услуг передачи данных, 2012 год



Annexes

Annex 1: Trends in Telecommunications

Annex 2: Tariff Considerations for Data Services including NGN

Annex 3: NGN Functional Architecture/Security

Annex 4: Quality of Service in NGN

Annex 5: NGN Management

Annex 6: NGN Testing

Annex 7: Examples of Migration Scenarios

Annex 8: NGN Issues

Annex 9: ITU NGN Standards

Annex 1: Trends in Telecommunications

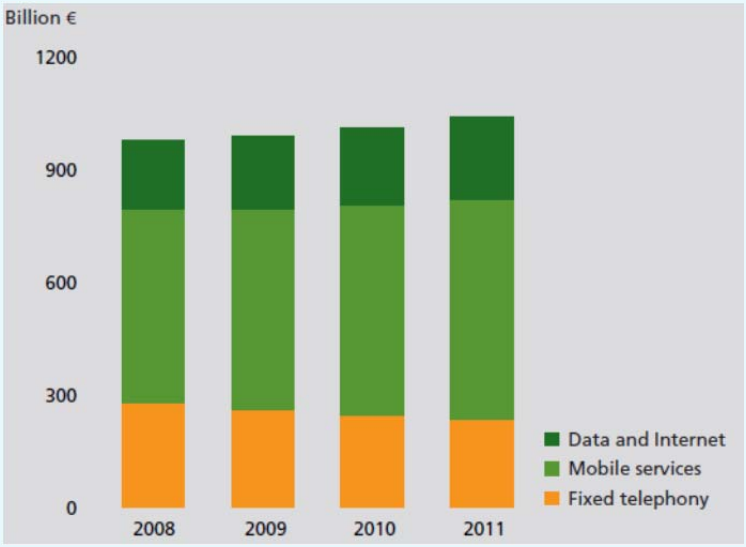
1 Market Trends

1.1 Overall Telecom Market Trends

General analysis of telecom market trend is rather positive in many of countries. Many of reports informed their last year analysis results. This report makes references to various reports: the analysis from Ofcom, United Kingdom published as "The International Communications Market 2012", ITU reports on "Measuring the information society: 2012" and "ICT Facts and Figures: 2011 and 2013" . These reports do not cover all areas on the world but give certain information to look at overall trend of telecom businesses.

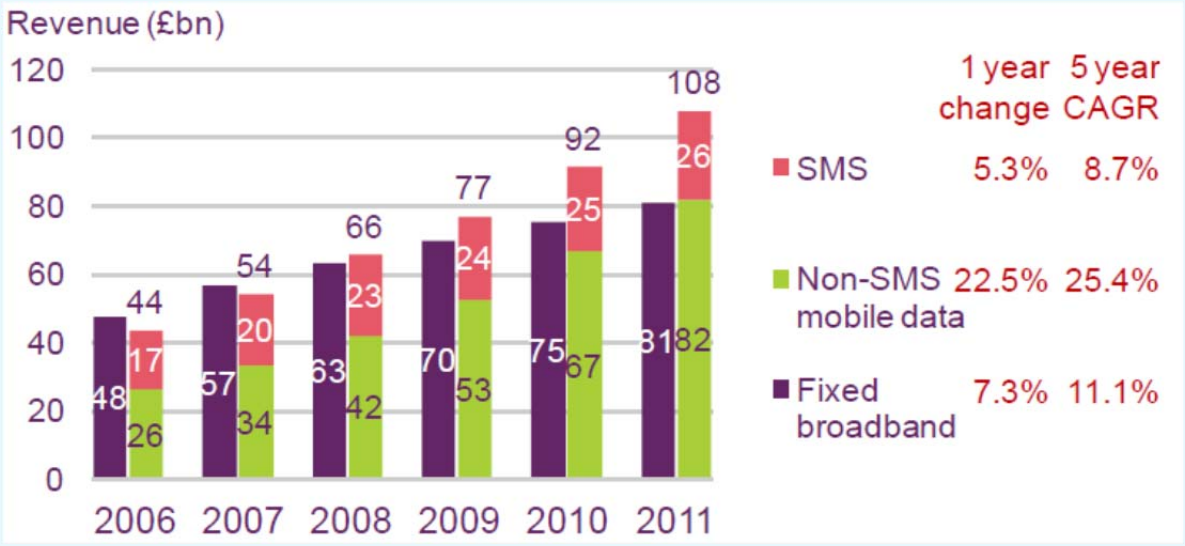
Figures from the ITU show that by the end of 2011 2.3 billion people (around a third of the world's population) accessed the internet globally, almost double the 1.2 billion figures recorded in 2006. Over this period growth in internet use was fastest among developing countries, and by 2011 62% of internet users were located in developing countries, an increase from 44% in 2006. This trend is lead by expansion in mobile and broadband services for data and internet as the key telecommunication market while fixed voice oriented services are continuously diminishing as shown in Figure 1-1.

Figure 1-1: Global telecom services market growth by segment (IDATE)



The report by Ofcom, United Kingdom indicated that there was rapid growth in the take-up of fixed broadband services across the 17 countries in the five years to 2011, during which time fixed broadband take-up almost doubled to reach 42 connections per 100 homes. Increasing take-up of fixed broadband and mobile voice and data services have contributed to an accelerating decline in the use of traditional fixed telephony services in most of the countries. Despite significant growth in fixed broadband take-up, revenues from mobile data services exceeded those from fixed broadband connections for the first time among surveyed 17 countries in 2011 as shown in Figure 1-2.

Figure 1-2: Fixed broadband and mobile data revenues (2006 ~ 2011) (IDATE)



As a total in the survey of Ofcom, mobile data has seen the fastest growth rate (CAGR) of 25.4% between 2006 and 2011 meaning that, for the first time in 2011, mobile data revenues (£82bn) exceeded fixed broadband revenues (£81bn, CAGR of 11.1%). The report analyzed that this growth in mobile data revenue has been driven by a rapid increase in the adoption of smartphones, from which it is much easier and quicker to access the internet. SMS revenues increased at a slower CAGR of 8.7% between 2006 and 2011. Although SMS volumes are still growing but revenues have failed to keep pace as operators have started to offer large bundles of SMS messages as part of subscription packages; this has stimulated use but caused revenue pressure for SMS in many markets. However, much of the revenue growth in fixed broadband in developed countries was realised towards the start of the five-year period when take-up was growing rapidly. Fixed broadband may now be approaching market saturation in many European countries, as the majority of households subscribe to fixed broadband services – limiting revenue growth for the year 2011.The Ofcome report identified three of the key developments which are transforming the global telecoms market, both in terms of industry structures and consumer behaviour:

- The mobile data explosion: the growth in mobile data, with key volume, subscriber and revenue statistics, and sheds some light on the transition from large-screen PCs to small screen smartphone mobile data use.
- Continued growth in superfast broadband networks: the deployment of superfast technologies across countries, and the extent to which consumers are migrating to these services.
- Increased use of text messaging: the contrasting levels of use and expenditure related to texting, and examine attitudes towards texting.

1.2 Trends in the Voice Service Market

The Ofcom report indicated that the fixed voice call volumes continuously fell in most of countries for which figures were available in 2011 except France, where they increased by 0.6% to 113 billion minutes during the year (Figure 1-3). The resilience of the fixed voice market in France is largely as result of high take-up of managed VoIP services, often provided as part of a triple-play bundle of fixed broadband and IPTV services over naked DSL. Naked-DSL-based broadband services do not require a standard fixed line, so VoIP over naked-DSL provides a low-cost alternative to voice calls made over traditional fixed networks, as no line rental is paid. It is this which is the primary driver of the 13.1% fall in fixed voice revenues in France in 2011, despite call volumes increasing during the year. In the UK, fixed voice call volumes fell by 10.0% to 116 billion minutes in 2011, this rate of decline being the fourth highest among 15 countries.

It is noted that the major drivers behind declining fixed call volumes are the low cost of mobile voice and text services and high smartphone take-up, which has contributed to the increasing use of alternative forms of communication such as email and instant messaging. France and the Netherlands (where VoIP use is widespread) were the only countries compared where fixed call volumes increased in the five years to 2011 (up by 1.8% and 0.4% a year on average, respectively). Conversely, the highest average annual rate of decline over the period (13.0%) was in Australia, where fixed call volumes halved over the period, largely due to the increasing use of mobile voice services. As a consequence, fixed voice revenues continuously fell in 2011, the fastest rates of decline, with revenues falling by 17.8% in China and 15.3% in India during the year.

Figure 1-3: Fixed line call volumes and revenue, 2006 and 2011

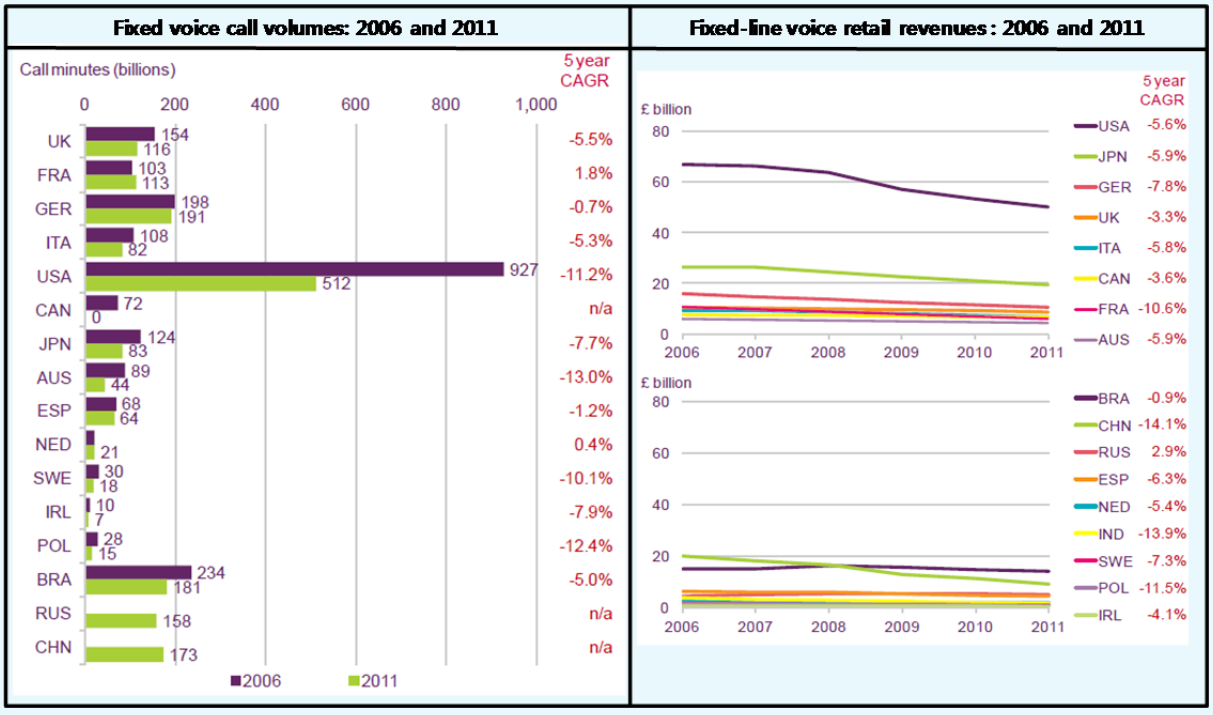
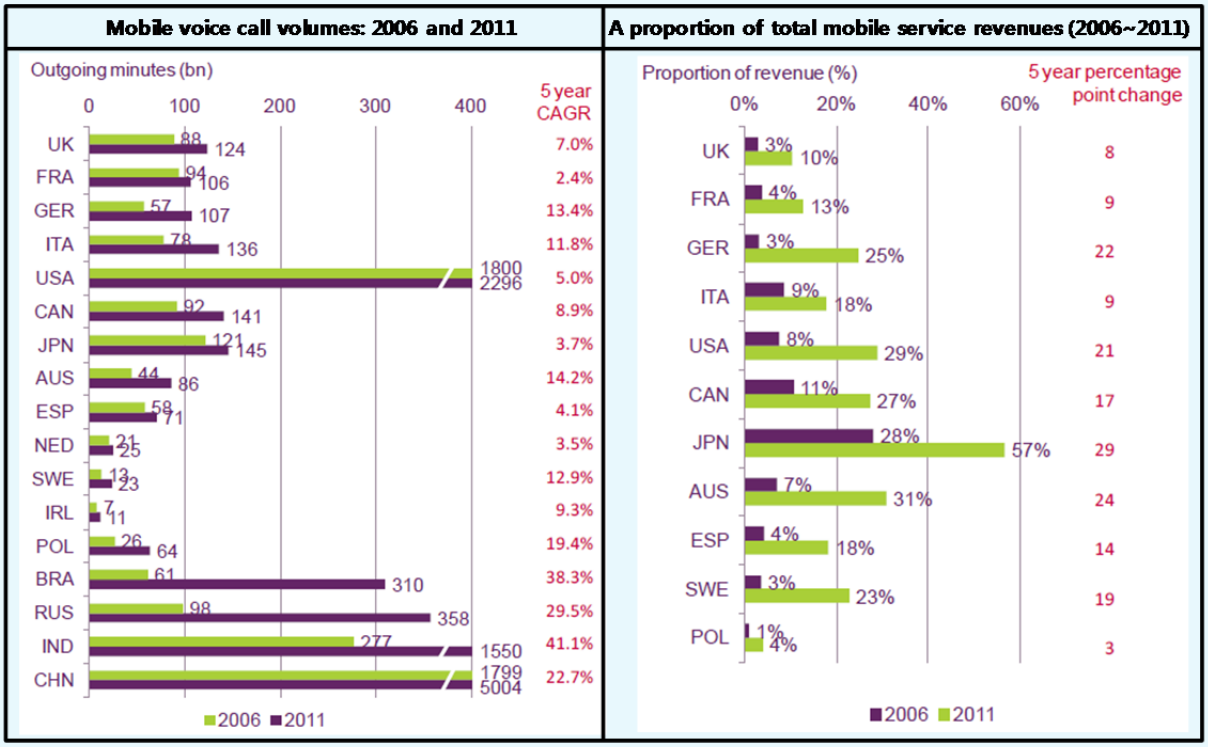


Figure 1-4 shows the status of mobile voice call minutes and revenues by Ofcom report. The countries where the highest proportion of calls originated on mobiles in 2011 were China (97%), the United States (82%) and Poland (81%). In China and Poland this is partly due to the limited availability of fixed telephony networks, while the proportion of calls that are mobile-originated will be overstated in China, the US and Canada as the mobile call volumes used in the calculation include incoming call minutes. Germany and France were the only comparator countries where less than half of voice call minutes originated on mobile networks in 2011 (36% of voice call minutes were mobile-originated in Germany in 2011, while the figure was 49% in France).

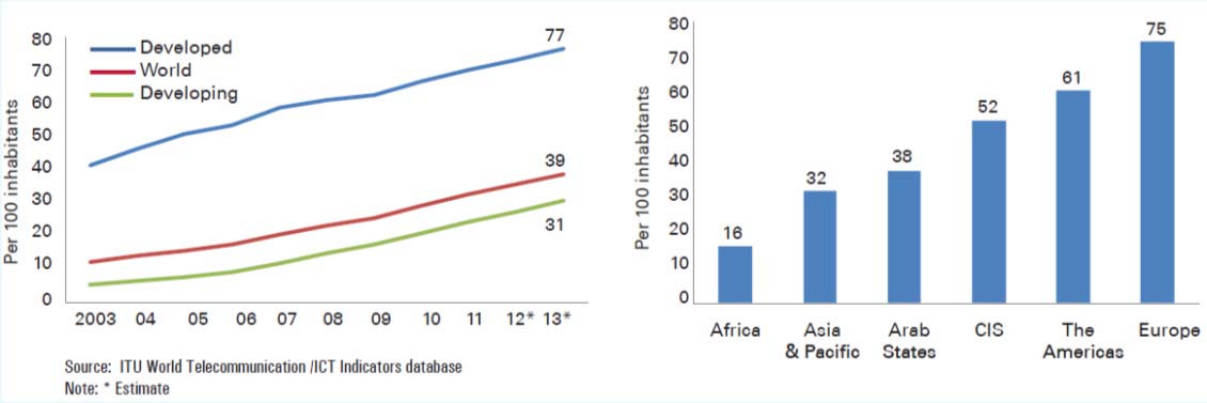
Figure 1-4: Mobile call volumes and revenue, 2006 and 2011



1.3 Broadband Market Trends

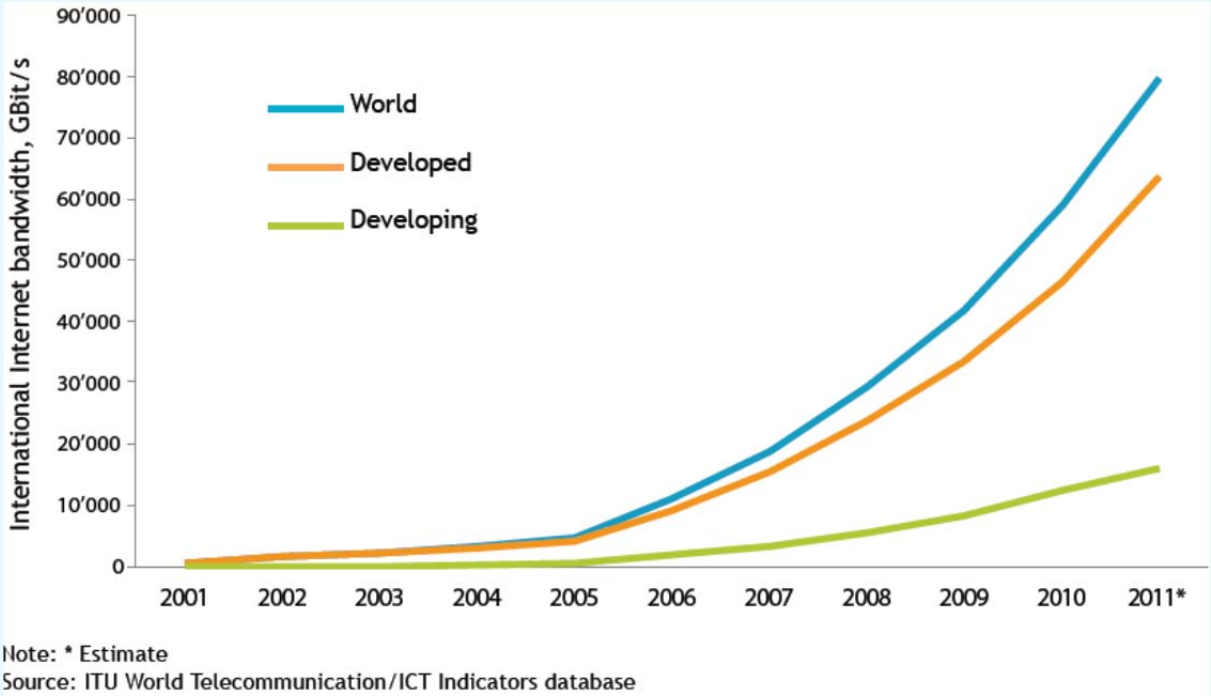
Benefitting fixed broadband and mobile, especially smartphones, internet users (use of more data including information) is increasing as shown in Figure 1-5 (by ITU, ICT facts and figures 2013).

Figure 1-5: Internet users by development level and region



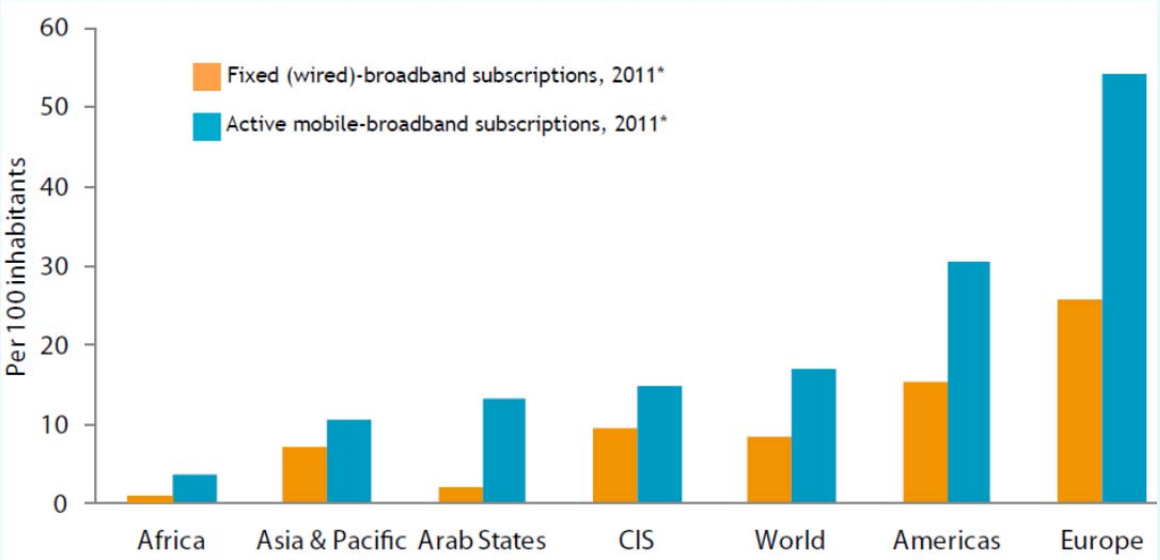
As a consequence, bandwidth consumption of the world continuously increased as shown in the Figure 1-6 below (by ITU, ICT facts and figures 2011).

Figure 1-6: Growth of bandwidth



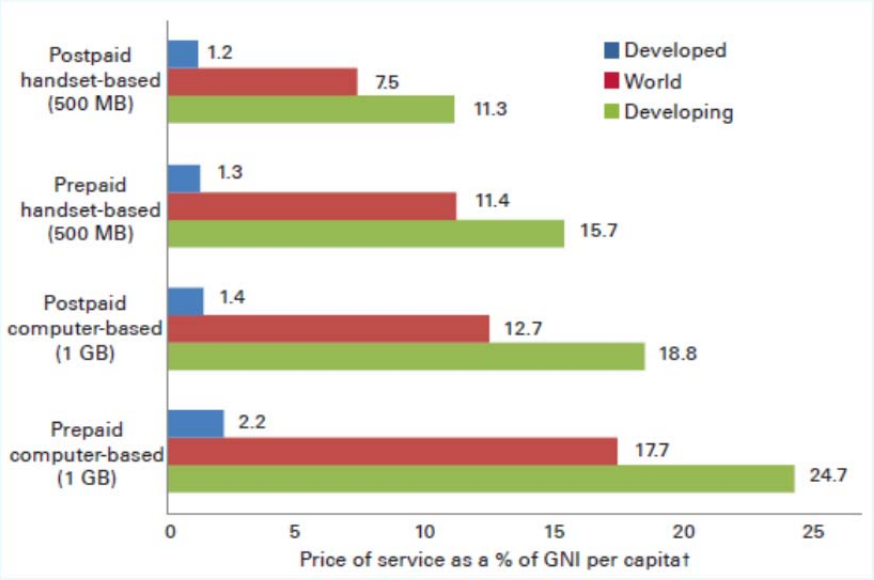
One interesting phenomena is that mobile broadband users are exceed fixed broadband users as shown in Figure 1-7 (ITU, ICT facts and figures 2013). This phenomena is apparent in all of the regions, in both developed or developing countries, which in turn means users enjoyed connectivity over mobile environments.

Figure 1-7: Status of broadband in 2011



Following the analysis by ITU as shown in Figure 1-8, it is noted that mobile broadband is more expensive in developing countries but considerably cheaper than fixed broadband services. By early 2013, the price of an entry-level mobile-broadband plan represents between 1.2-2.2% of monthly GNI p.c. in developed countries and between 11.3-24.7% in developing countries, depending on the type of service. However, in developing countries, mobile broadband services costs are considerably lower than fixed-broadband services costs: 18.8% of monthly GNI p.c. for a 1 GB postpaid computer-based mobile-broadband plan compared to 30.1% of monthly GNI p.c. for a postpaid fixed-broadband plan with 1 GB of data volume. Among the four typical mobile-broadband plans offered in the market, postpaid handset-based services are the cheapest and prepaid computer-based services are the most expensive, across all regions.

Figure 1-8: Price of mobile-broadband services, early 2013



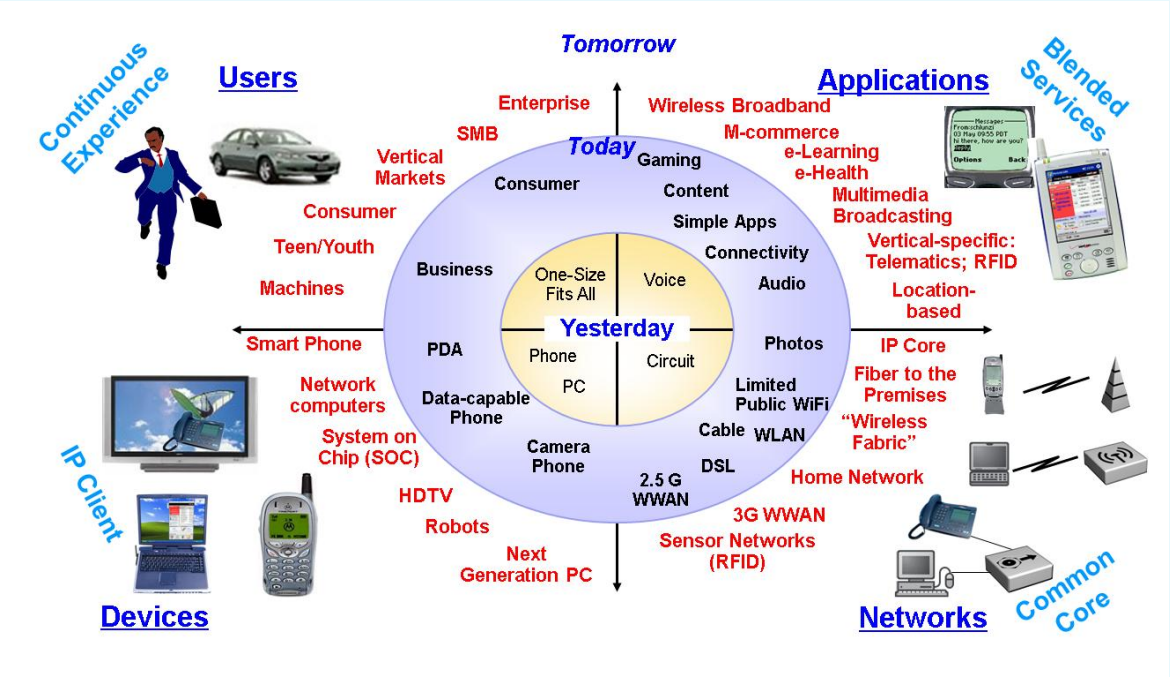
2 Overall Trends in Telecommunications

2.1 Overall Development Trends

There are various angles to look at trends of development in telecommunication such as users' aspects, services/applications' aspects, devices' aspects and networks' aspects etc. Because of the recent developments in telecommunication (should be included with the concept of ICT), this is not an easy task with short sentences like in this report. Therefore this report broadly looks at the development trend from these four different aspects.

In this regard, following Figure 2-1 provided an overview of technology development, taking into account the evolving trends related to users and services/applications.

Figure 2-1: Abstraction of development trends



- **User perspective:** Previous users were quite well-fitted with fixed types of services e.g. a black phone for voice service and a facsimile terminal for graphic service. So it featured as one size service fits all kinds of users. However, users today request more dynamic types of services depending on their lifestyle, and whether they are using the service as a consumer or for their business, etc. This is likely to continue developing in the future and as a result their usage of telecommunication services and applications with require services at anytime, anywhere and on any device.
- **Service/Application perspective:** Voice services have been the key service for telecommunication providers during more than 100 years. This has is now expanding to cover more other services than just voice, including multimedia services with broadband connectivity which are available today. It is further anticipated to expand to cover various services/applications mixed together, which sometimes is called convergence and other the provision of blending services.
- **Network perspective:** Previous circuit oriented networks have evolved to the packet networks of today (mainly using internet protocol (IP)), including continuously increasing bandwidth using xDSL and fibre optics and wireless technologies such as WiFi and WiMAX. This will be leveraged by common core networks in the near future, which will be IP-based but enhanced by other elements such as Quality of Service (QoS) and security.
- **Device perspective:** The area which has seen the most remarkable development is the device area. The key themes in the development of devices include the need for them to be portable, multi-functional and smart. Moreover, as the use and growth of IP is expected also for the near future, devices should be IP-enabled.

2.2 Convergences

During the past several years, the ICT domain has continuously developed to support various types of convergences with a vision of "Any Time, Any Where, Any Services and Any Devices." This trend has been led by the development of the associated technology and the notion of "any information/service over any transport infrastructure." One traditional example of this is VoDSL (Voice over DSL). DSL was developed to provide broadband connectivity but today this is used for voice services such as VoIP. Another example is TVoMobile (TV service over Mobile). Mobile was developed to provide voice services while users move around, but today mobile is also used for watching TV.

Especially with development of NGN, fixed mobile convergence (FMC) is now becoming the first instance of converged fixed and mobile services, and IPTV is also following with the convergence between telecom and broadcasting. Moreover, convergences using ICT are rapidly expanding to cover many of the industrial areas.

Figure 2-2: High level view of the converged environment

Convergence can be classified into two main groups:

- **Internal Convergence** (within the same industry): This means the convergence between different services and/or networks but within the same industries, such as FMC and IPTV. FMC is the convergence between fixed and mobile, but both two belong to the same industry, the telecom industry. IPTV is the convergence between telecom and broadcasting but they also belong to telecom industry in their wider interpretation.
- **External Convergence** (between different industries): This means the convergence between/amongst different industries, e.g., Telematics/ITS, USN, e-Health, Networked Robotics and others. This type of convergence requires more complicated processing not only from the technical aspect but also from regulatory and political aspects.

Whether internal or external convergences, the high level view of how services are used in a converged environment can be show as in Figure 2-2 above. Networks will then look like a cloud which allows for the provision of connectivity to the devices anywhere, anytime and where any service can be delivered to any device. Consequently, end users can make use of the services they wish to use in close relation to their real life using handy smart terminal devices and sensors (e.g. USN), even while driving a vehicle.

2.3 Trend of User Willingness

As technology develops further (or maybe even the other way round), end user willingness to pay for specific telecommunication services are also continuously changing. Actually it is better to say "expanding" or "increasing."

Figure 2-3 shows some interesting results of users' willingness to pay for services. All types of services shown in the figure (such as online shopping, accessing news online, etc.) have been identified as important activities for end users, which they are not willing to pay for, especially when they are using their mobile phones. However, there is a certain amount of willingness to use the services, even using the mobile phone, when advertisements cover the associated costs. Both these two cases show that there are potential customers who are willing to use such services if they are made available in an economically beneficial way, such as using flat-rates for the fixed-mobile convergence access.

Figure 2-3: Customers' willingness to pay for services

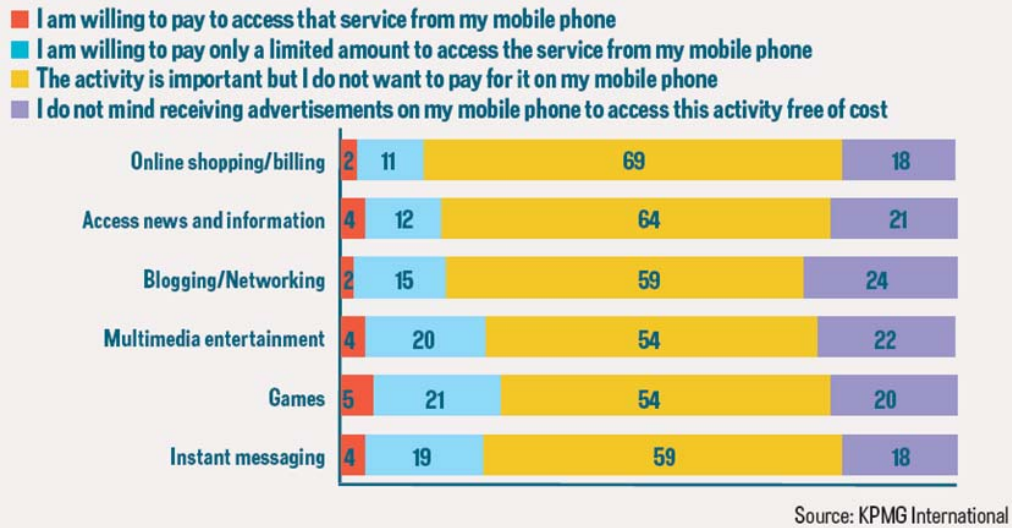
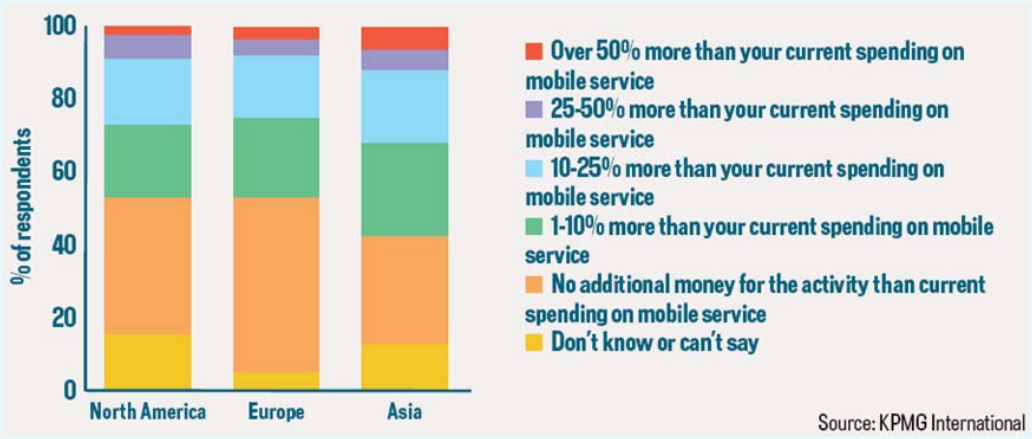


Figure 2-4 shows the results of research done on end user willingness to pay for convergence services. One can see that people in Asia show more interest in converged services than those living in other regions.

Figure 2-4: Customers' willingness to increase spending on converged services



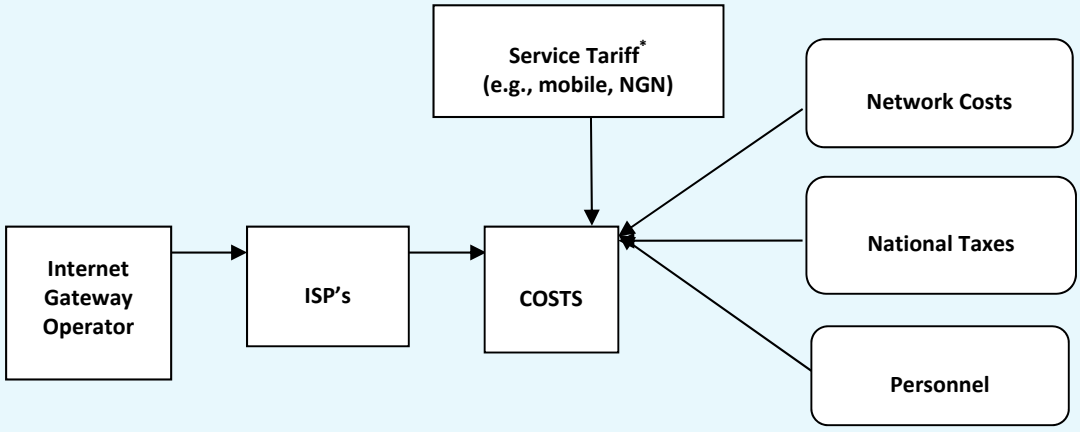
Annex 2: Tariff Considerations for Data Services including NGN

In the voice market, the tariffs are determined by competition. The Regulator sets a uniform interconnection rate across all networks and allows the operators to come up with their own end user rates which are to a large extent determined by competition allowing price differences between the operators. However, tariffs for data services with the advent of NGN's is different, since data services are, in general today, supported by internet interconnected through the gateway.

[Note: In some countries (for example The Gambia), the gateway is still in a monopoly under the incumbent, thus other providers such as mobile operators still need to go through an ISP to get connected to the gateway.]

As regards voice services each operator has the liberty to charge as low as possible to be competitive in price without having to worry much about covering costs. In the case of data services it is not that easy. The extent to which data service prices can be lowered is constrained by the price of bandwidth from the incumbent to the ISP and from the ISP to the other operators, such as mobile operator, in addition to all other network operational costs. The following figure shows this relationship for pricing of data services.

Figure 2-1: An example of pricing on data services



* *This block has been modified from "GSM/NGN tariff" to "service Tariff (e.g., mobile and NGN), because this block shows an input to the costs from other service aspects.*

Annex 3: NGN Functional Architecture/Security

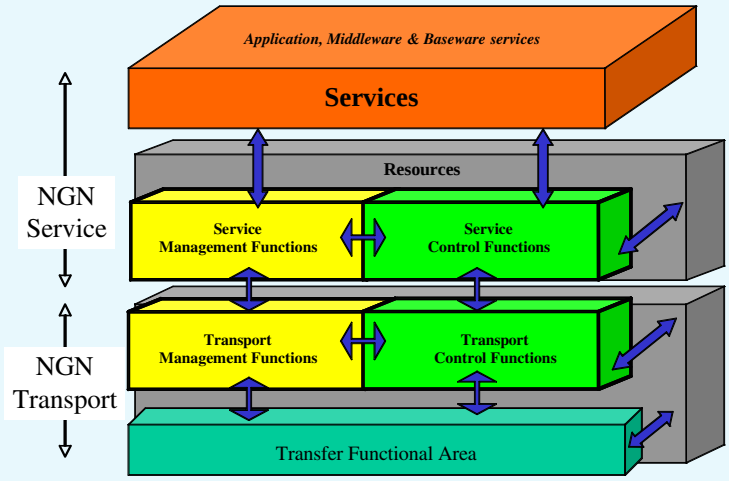
1 NGN Functional Architecture

1.1 General Principles and Reference Architecture Model

As far as NGN systems (non-OSI systems) are concerned, all or some of the following situations may be encountered when considering the OSI 7-layer basic reference model (OSI BRM):

- The number of layers may not equal seven;
- The functions of individual layers may not correspond to those of the OSI BRM;
- Certain prescribed or proscribed conditions/definitions of the OSI BRM may not be applicable;
- The protocols involved may be other than OSI protocols (one notable example being the IP);
- The compliance requirements of the OSI BRM may not be applicable.

Figure 1-1: General functional model of NGN



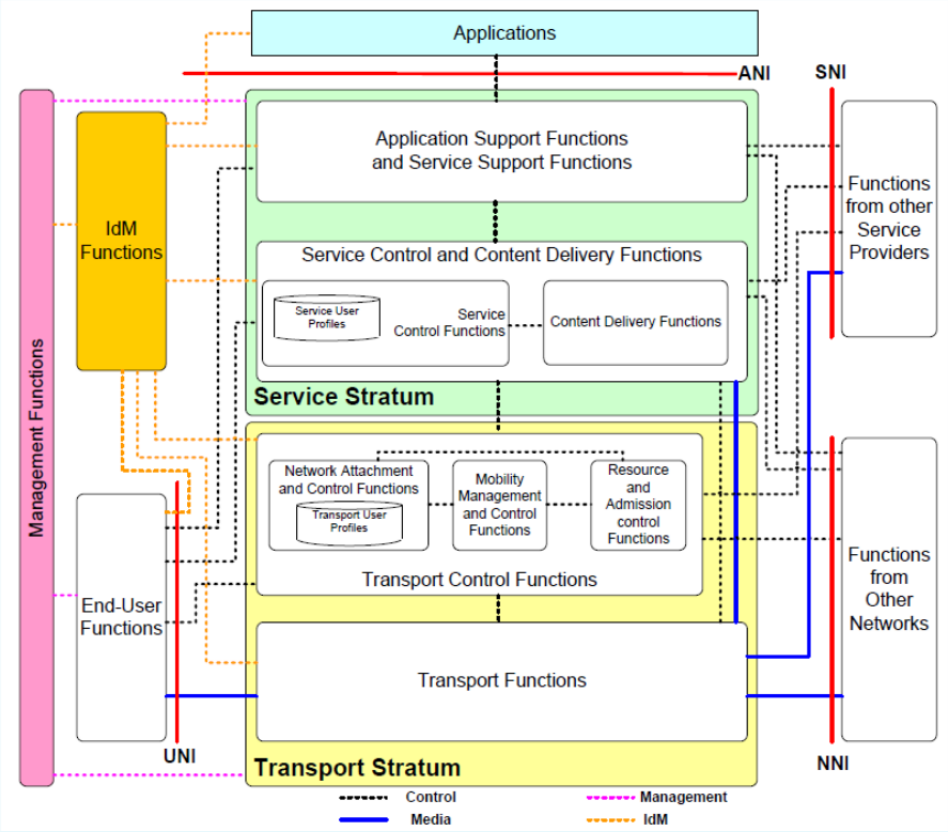
The services and functions are related to each other, since functions are used to build services. It is convenient to assemble functions into two distinct groups, or planes, one comprising all control functions and the other comprising all management functions. The grouping of functions of the same type (i.e., control or management) allows the functional inter-relationships within a given group to be defined, as well as the information flows between functions in the given group.

With this in mind, ITU-T Recommendation Y.2011 goes on to consider the functional aspects of systems implementation. In particular, it develops the following high-level model, which shows how functions may be grouped for the purposes of systems development. The functional blocks shown in Figure 1-1, can then be further decomposed in sub-groups to represent grouping convenient for implementation and distributed system depiction.

1.2 NGN Functional Architecture

NGN services include session-based services, such as IP telephony, video conferencing, and video chatting, and non session-based services, such as video streaming and broadcasting. Moreover, NGN supports PSTN/ISDN replacement.

Figure 1-2: Abstracted NGN functional architecture



The NGN architectural overview shown in Figure 1-2 comes from ITU-T Recommendation Y. 2012. The NGN functions are divided into service functions and transport functions. According to ITU-T Recommendation Y.2011, it is called the functional categories strata.

Customer networks and terminals are connected by UNI. Other networks are interconnected through NNI. Clear identification of UNI and NNI is important to accommodate a wide variety of off-the-shelf customer equipment while maintaining business boundaries and demarcation points for the NGN environment.

1.2.1 Transport Stratum Functions

Transport stratum functions identified in ITU-T Recommendation Y.2012 provide connectivity for all components and physically separated functions within the NGN. IP is recognized as the most promising technology for NGN. Thus, the transport stratum provides IP connectivity for both end-user equipment outside the NGN and controllers and enablers, which usually reside on the servers inside the NGN. The transport stratum is responsible for providing end-to-end QoS, which is a desirable feature of the NGN. The transport stratum is divided into access networks and the core network, with a function linking the two transport network portions.

- **Transport functions**: The transport functions provide the connectivity for all components and physically separated functions within the NGN. These functions provide support for the transfer of media information, as well as the transfer of control and management information. Transport functions include access network functions, edge functions, core transport functions, and gateway functions.
- **Transport control functions**: The transport control functions include Resource and Admission Control Functions, Network Attachment Control Functions and Mobility management and Control Functions.

  a) Network attachment control functions (NACF): The network attachment control functions provide registration at the access level and initialization of end-user functions for accessing NGN services. The functions provide network level identification/authentication, manage the IP address space of the access network, and authenticate access sessions. The functions also announce the contact point of the NGN Service/Application functions to the end user. That is, the functions assist end-user equipment to register and start the use of the NGN.

  b) Resource and Admission Control Functions (RACF): In the NGN Architecture, the RACF provides QoS control (including resource reservation, admission control and gate control), NAPT and/or FW traversal control Functions over access and core transport networks. Admission control involves checking authorization based on user profiles, SLAs, operator specific policy rules, service priority, and resource availability within access and core transport. Within the NGN architecture, the RACF act as the arbitrator for resource negotiation and allocation between Service Control Functions and Transport Functions.

  c) Transport User Profile functions: These functions take the form of a functional database representing the combination of a user's information and other control data into a single "user profile" function in the transport stratum. This functional database may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

  d) Mobility Management and Control Functions (MMCF): The MMCF provide functions for the support of IPbased mobility in the transport stratum. These functions allow the support of mobility of a single device. The MMCF provides mechanisms to achieve seamless mobility if network conditions permit, but does not provide any mechanism to deal with service adaptation if the post-handover quality of service is degraded from the quality of service before handover. The MMCF assumes that mobility is a service, explicitly specified by parameters in the user service profile. The MMCF is not dependent on specific access technologies, and supports handover across different technologies.

1.2.2 Service Stratum Functions

The service stratum functions provide session-based and non session-based services including subscribe/notify for presence information and the message method for instant message exchange.

- **Service control and content delivery functions** (SC&CDF): The SC&CDF includes service control functions and content delivery functions

  a) Service Control Functions (SCF): The SCF includes resource control, registration, and authentication and authorization functions at the service level for both mediated and non-mediated services.. They can also include functions for controlling media resources, i.e., specialized resources and gateways at the service-signalling level. Regarding the authentication, mutual authentication between end user and the service is performed. The service control functions accommodate service user profiles which represent the combination of user information and other control data into a single user profile function in the service stratum, in the form of functional databases. These functional databases may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

  b) Service user profile functions: The service user profile functions represent the combination of user information and other control data into a single user profile function in the service stratum, in the form of a functional database. This functional database may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

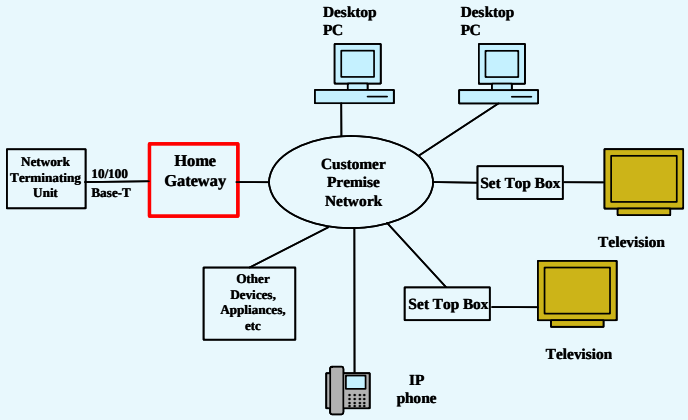
  c) Content Delivery Functions (CDF): The CDF receives content from the application support functions and service support functions, store, process, and deliver it to the end-user functions using the capabilities of the transport functions, under control of the service control functions.

- **Application/Service support functions**: The application/service support functions include functions such as the gateway, registration, authentication and authorization functions at the application level. These functions are available to the “Third-Party Applications” and “End-User” functional groups. The Application/Service support functions work in conjunction with the SCF to provide end-users and third party application providers with the value added services they request. Through the UNI, the Application/Service support functions provide a reference point to the end-user functions. The Third-party applications’ interactions with the Application/Service support functions are handled through the ANI reference point.

1.2.3 End User Functions

No assumptions are made about the diverse end-user interfaces and end-user networks that may be connected to the NGN access network. Different categories of end-user equipment are supported in the NGN, from single-line legacy telephones to complex corporate networks. End-user equipment may be either mobile or fixed.

Figure 1-3: Overall configurations of end systems in NGN



1.2.4 Management Functions

Support for management is fundamental to the operation of the NGN. These functions provide the ability to manage the NGN in order to provide NGN services with the expected quality, security, and reliability. These functions are allocated in a distributed manner to each functional entity (FE), and they interact with network element (NE) management, network management, and service management FEs. Further details of the management functions, including their division into administrative domains, can be found in ITU-T recommendation M.3060. Management functions apply to the NGN service and transport strata. For each of these strata, they cover the FCAPS.

The accounting management functions also include charging and billing functions (CBF). These interact with each other in the NGN to collect accounting information, in order to provide the NGN service provider with appropriate resource utilization data, enabling the service provider to properly bill the users of the system.

2 Security in NGN

2.1 Security threats and risks

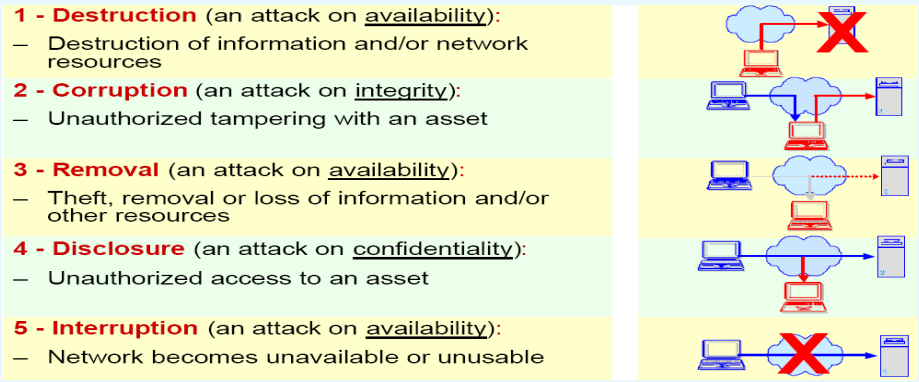
The systems, components, interfaces, information, resources, communications (i.e., signalling, management and data/bearer traffic) and services that make up an NGN will be exposed to a variety of security threats and risks. Those threats and risks will depend on a variety of factors. In addition, end users will also be exposed to certain threats (e.g., unauthorized access to private information). Figure 2-1 illustrates threat model based on Rec. X.800.

Threats to the NGN:

- unauthorized reconnaissance, such as the remote analysis of the system to determine points of weakness (these may include scans, sweeps, port interrogation, route tables, etc.);
- break-in/device takeover resulting in loss of control of the device, anomalies and errors in the configuration audits;
- destruction of information and/or other resources;
- corruption or modification of information;
- theft, removal or loss of information and/or other resources;

- disclosure of information; and
- interruption of services and denial of services.

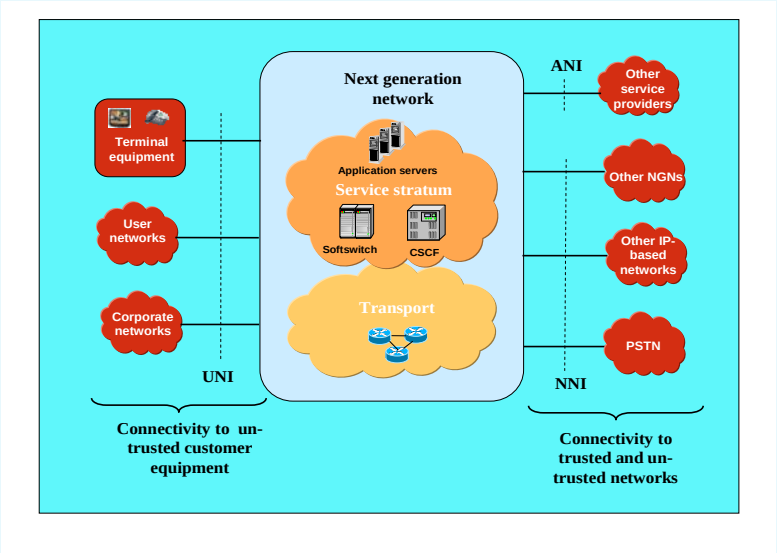
Figure 2-1: X.800 threat model



Further, it is clear that NGNs will be operating in an environment different from the PSTN environment and may therefore be exposed to different types of threats and attacks from within or externally. NGNs will have direct or indirect connectivity to un-trusted and trusted networks and terminal equipment, and therefore will be exposed to security risks and threats associated with connectivity to un-secure networks and customer premises equipment. For example, a provider's NGN may have direct or indirect (i.e., through another network) connectivity to the following as shown in Figure 2-2.

- other service providers, and their applications;
- other NGNs;
- other IP-based networks;
- public switched telephone network (PSTN);
- corporate networks;
- user networks;
- terminal equipment;
- other NGN transport domains.

Figure 2-2: Connectivity to networks and users



In the evolving environment, security across multiple network provider domains relies on the aggregation of what all providers elect to do for securing their networks. Unauthorized network access into one provider's network can easily lead to exploitation of an interconnected network and its associated services. This is an example of the exploitation of the weakest link that can threaten a provider network's integrity and service continuity along with a host of various types of attacks.

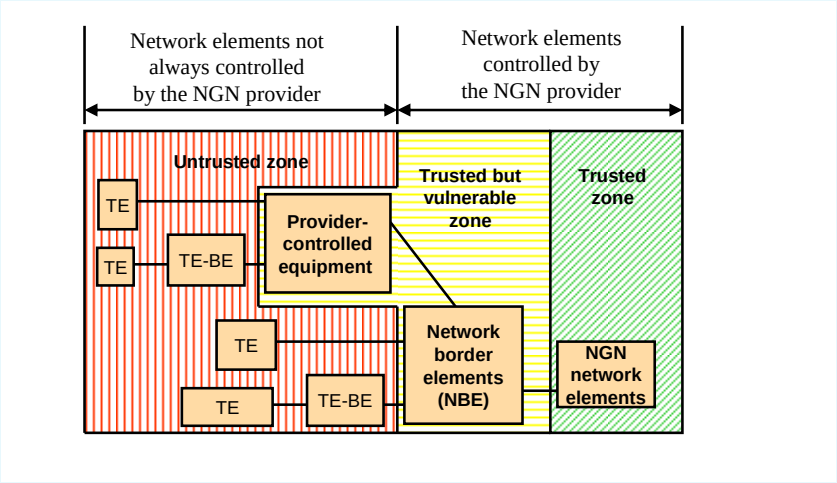
Each NGN provider is responsible for security within its domain. Each NGN provider is responsible for designing and implementing security solutions using network specific policy for trust relations, to meet its own network-specific needs and to support global end-to-end security objectives across multiple network provider domains.

2.2 Security trust model

The NGN functional reference architecture defines functional entities (FEs). However, since network security aspects depend heavily on the way that FEs are bundled together, the NGN security architecture is based on physical network elements (NEs), i.e., tangible boxes that contain one or more FEs. The way these FEs are bundled into NEs will vary, depending on the vendor.

- **Single network trust model**: Three security zones (trusted, trusted but vulnerable, and un-trusted) are dependent on operational control, location, and connectivity to other device/network elements. These three zones are illustrated in the security trust model shown in Figure 2-3.

Figure 2-3: Security trust model



a) "trusted network security zone" or "trusted zone": It is a zone where a NGN provider's network elements and systems reside and never communicate directly with customer equipment or other domains. The "trusted zone" will be protected by a combination of various methods. Some examples are physical security of the NGN network elements, general hardening of the systems, use of secure signalling, security for OAMP messages separate VPN within the (MPLS/)IP network for communication within the "trusted" zone and with NGN network elements in the "trusted-but-vulnerable" zone.

b) "trusted but vulnerable network security zone", or "trusted but vulnerable zone": It is a zone where the network elements/devices are operated (provisioned and maintained) by the NGN provider. The equipment may be under the control by either the customer/subscriber or the NGN provider. In addition, the equipment may be located within or outside the NGN provider's premises. Their major security function is to protect the NEs in the trusted zone from the security attacks originated in the un-trusted zone.

c) "un-trusted zone": It includes all network elements of customer networks or possibly peer networks or other NGN provider domains outside of the original domain, which are connected to the NGN provider's network border elements. In the "un-trusted zone", comprised of terminal equipment, equipment may not be under the control of NGN providers and it may be impossible to enforce provider's security policy on user.

- **Peering network trust model**: When an NGN is connected to another network, the trust depends on:

  a) physical interconnection, where the interconnection can range from a direct connection in a secure building to via shared facilities;

  b) peering model, where the traffic can be exchanged directly between the two NGN service providers, or via one or more NGN transport providers;

  c) business relationships, where there may be penalty clauses in the SLA agreements, and/or a trust in the other NGN provider's security policy;

  d) in general, NGN providers should view other providers as un-trusted.

2.3 Design Principles for NGN Security

2.3.1 Objectives and requirements

- **General security objectives**: The following is a list of general security objectives used to guide the requirements in this Recommendation.

  a) NGN security features should be extensible, and flexible enough to satisfy various needs.

  b) Security requirements should take the performance, usability, scalability and cost constraints of NGN into account.

  c) Security methods should be based on existing and well-understood security standards as appropriate.

  d) The NGN security architecture should be globally scalable (within network provider domains, across multiple network provider domains, in security provisioning).

  e) The NGN security architecture should respect the logical or physical separation of signalling and control traffic, user traffic, and management traffic.

  f) NGN security should be securely provisioned and securely managed.

  g) An NGN should provide security from all perspectives: service, network provider and subscriber.

  h) Security methods should not generally affect the quality of provided services.

  i) Security should provide simple, secure provisioning and configuration for subscribers and providers (plug & play).

  j) Appropriate security levels should be maintained even when multicast functionality is used.

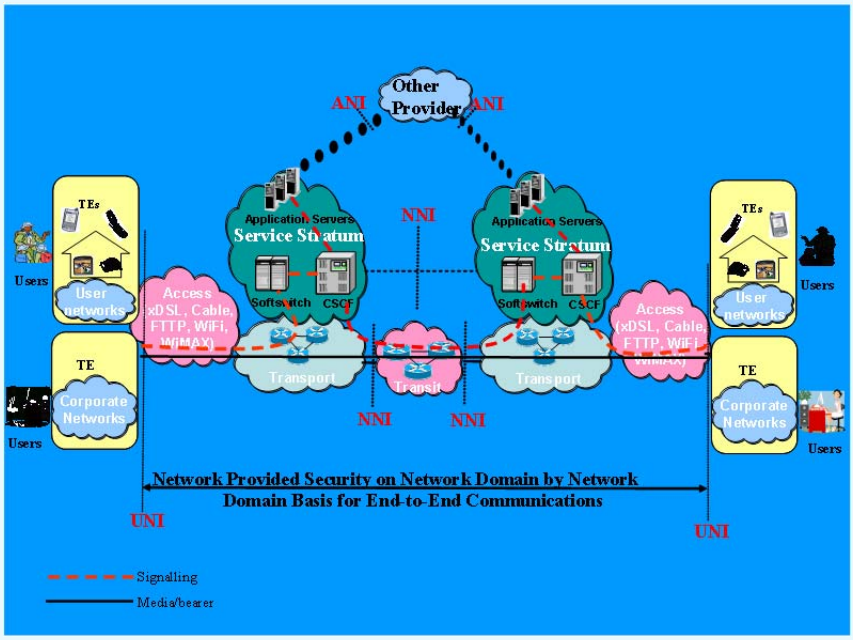
  k) The service discovery capabilities should support a variety of scoping criteria (e.g., location, cost, etc.) to provide appropriate scaling, with appropriate mechanisms to ensure security and privacy.

  l) The address resolution system should be a special system used only by this network, and certain security measures are required to be in place. This system may use databases that are internal or external of a domain.

  m) The principles and general security objectives for secure TMN management should be followed.

- **Objectives for security across multiple network provider domains**: The general objective is to provide network-based security for end-to-end communications across multiple provider domains. This is achieved by providing security of the end-to-end communication on a hop-by-hop basis across the different provider's domains. Figure 2-4 shows the general concept of network provided security for end-to-end communications between end users. Each network segment has specific security responsibilities within its security zone to facilitate security and availability of NGN communications across multiple networks.

Figure 2-4: Security of communications across multiple networks



- **Requirements specific for security dimensions**: The objectives described here are specific to particular security dimensions, such as authentication. They are common to all interfaces.

  a) Access control: NGN providers are required to restrict access to authorized subscribers. Authorization may be given by the provider providing the access or by other providers after validation by an authentication and access control processes. The NGN is required to prevent unauthorized access, such as by intruders masquerading as authorized users.

  b) Authentication: NGN providers are required to support capabilities for authenticating subscribers, equipment, network elements and other providers.

  c) Non-repudiation: This document does not specify any non-repudiation security requirements.

  d) Data confidentiality: NGN providers are required to protect the confidentiality of subscriber traffic by cryptographic or other means. NGN providers are required to protect confidentiality of control messages by cryptographic or other means if security policy requests it. NGN providers are required to protect the confidentiality of management traffic by cryptographic or other means.

  e) Communication security: NGN providers are required to provide mechanisms for ensuring that information is not unlawfully diverted or intercepted.

  f) Data integrity: NGN providers are required to protect the integrity of subscriber traffic by cryptographic or other means. NGN providers are required to protect integrity of control messages by cryptographic or other means if security policy requests it. NGN providers are required to protect the integrity of management traffic by cryptographic or other means.

g) Availability: NGN is required to provide security capabilities to enable NGN providers to prevent or terminate communications with the non-compliant end-user equipment. These capabilities may be suspended to allow emergency communications. NGN internal network elements may also be susceptible to viruses, worms and other attacks. Similar measures to quarantine network components are also required. An NGN should provide provision of security capabilities to enable a NGN provider to filter out packets and traffic that is considered harmful by the respective security policy. NGN is required to provide capabilities for the support of disaster recovery functions and procedures.

h) Privacy: NGN is required to provide capabilities to protect the subscriber's private information such as location of data, identities, phone numbers, network addresses or call-accounting data according to national regulations and laws. Specific requirements for privacy are a national matter and are outside the scope of this Recommendation.

2.3.2 Specific security requirements

This clause introduces the specific requirements for security for each of the network elements within the NGN infrastructure.

- **Common security requirements for NGN elements**

a) Security policy: NGN providers shall prepare appropriate security policy and shall be responsible for applying it to all NEs and devices under its control.

b) Hardening and service disablement: All NGN elements are required to be capable of being configured to support the minimum services needed to support the NGN provider NGN infrastructure. Any service or transport layer port that is not required for the correct operation of the NGN element is required to be disabled on all systems and network elements. In addition, applications are required to run under minimum privileges (e.g., on "UNIX/Linux" platforms applications should not run as root if root privileges are not indispensable). The base operating system (OS) supporting any NGN element is required to be capable of being specifically configured for security and appropriately hardened. No "backdoors" are permitted (software access which would circumvent usual access control mechanisms) into any NGN element. In addition to hardening, physical and logical access controls are required to be put in place to meet industry best-practices.

c) Audit trail, trapping and logging: All NGN elements are required to be capable of creating an audit trail that maintains a record of security related events in accordance with NGN provider's security policy. Mechanisms to prevent unauthorized or undetected modification are required. The audit trail is required to be capable of being managed and is required to allow old data in the audit trail to be placed on other media, e.g., removable media, for long-term storage. This interface is required to allow authorized administrators to move old data out of the audit trail onto removable media. This ability is required to be protected by a specific authorization to manage the audit trail.

d) Time stamping and time source: The NGN element is required to support the use of a trusted time source for both system clock and audit trail item stamping. A trusted time source in this case means a time source that can be verified to be resistant to unauthorized modification. Transitive trust is acceptable, i.e., a time source that relies on a trusted time source is itself an acceptable trusted time source.

e) Resource allocation and exception handling: Each NGN element is required to provide the capability to limit the amount of its own important resources (e.g., memory allocation) it allocates to servicing requests. Such limits can minimize negative effects of denial of service attacks. Resources used to service requests compete with other resource utilization requests on the system. In addition, each specific NGN application is required to have the ability to limit its own usage of important resources that it allocates for satisfying requests.

f) Code and system integrity and monitoring: The network element is required to be capable of monitoring 1) its configuration and software and 2) any changes to detect unauthorized changes, both based on the security policy. Any unauthorized changes are required to create a log entry and cause an alarm to be generated. Based on the security policy, the network element is required to do the following. The element is required to be capable of periodically scanning its resources and software for malicious software, e.g., a virus. The element is required to generate an alarm if malicious software is discovered during a scan.

g) Patches, hotfixes and supplementary code: To trust signals generated by NGN provider NGN elements within un-trusted networks, say terminal. It is a requirement that software on the system is not compromised. NGN provider network elements and systems are required to provide a capability to verify and audit all their software. The audit results are to be accessible to an OSS. This would allow for an analysis of the security posture of the NGN provider NGN infrastructure and provide guidance to administrators and providers with respect to where mitigation is necessary.

h) Access to OAMP functions in devices: In order to safeguard the OAMP infrastructure, each internal NGN network element is required to be managed through a separate IP address allocated from a separate address block. The NGN network element is required to silently discard all packets received over the non-OAMP interface with source addresses assigned to OAMP traffic. Access to OAMP functions is required to be capable of being controlled by authentication. OAMP traffic is required to be securely protected.

- **Requirements for NGN elements in the trusted zone**: The NGN Release 1 element in the "trusted" zone is to be assigned an IP address in the block reserved for internal NGN elements. All signalling is required to use this address. The NGN Release 1 element is also required to be assigned an IP address in the block reserved for OAMP, and all OAMPs are required to use this address.
- **Requirements for NGN border elements in the "trusted-but-vulnerable" domain**: The network border element is required to support multiple IP addresses, or multiple network interfaces. The NBE is required to silently discard any media packets received that do not correspond to an active session. The NBE is also required to verify that the packet rate is consistent with the negotiated session parameters. The NBE is required to authenticate all requests if required by the service agreement with the customer.
- **Requirements for TE border elements in the "un-trusted" domain**: Physical security is a challenge for equipment placed on customer site. Ultimately, it must be accepted that, to a large extent, the security of these devices is dependent on the customer. In order to preserve the confidentiality of customer communication against eavesdropping on the signalling traffic, signalling messages are required to use a secure signalling connection between the TE-BE and the NBE.
- **Security recommendations for terminal equipment in the "un-trusted" domain**: The terminal equipment (TE) is often outside the control of the NGN provider. Therefore it is not required for the NGN provider to place requirements on its security features or policies, rather it is the function of the various network border elements to adapt to whatever policies are chosen by the customer and to provide the best service under those conditions. Media traffic should be protected from eavesdropping or modification.

2.3.3 NGN security mechanisms and procedures

This clause highlights some important security mechanisms that can be used to realize the requirements in ITU-T Recommendation Y.2701 in each NGN Network Element, and specifies a suite of options to be used for the mechanisms to avoid the mismatch of options.

- **Identification, Authentication and Authorization**: There are identification, authentication and authorization mechanisms, in particular, those concerning SIP-based services.
- **Transport Security for Signaling and OAMP**: Transport security is used in the NGN infrastructure to achieve confidentiality and integrity guarantees of the signalling data and the OAMP messages. It is

required to specify profile of TLS and IPsec to be used by the NGN infrastructure network elements as two of the important mechanisms.

- **Media Security**: Media encryption is not required within the NGN infrastructure, but it may be required to be supported for customers that desire its use. Such support may include the support of media encryption protocols, SRTP [RFC3711]. Network Border Elements (i.e., the edge of the network provider's domain) are assumed to implement encryption/decryption although it is possible to do the same in a separate platform shared among NBEs. In either case, the encryption and decryption is required to be collocated with other media processing capabilities such as Dual-Tone Multi-Frequency (DTMF) detection and transcoding.
- **Audit Trail, Trapping, and Logging Systems**: An audit trail is taken all OAMP access attempts (whether successful or not), all OAMP changes made, and all OAMP signoffs. In addition events considered significant by the NGN provider's policy are logged.
- **Provisioning of equipment in untrusted zone**: All customer premise equipments are configured by the TE Provisioning Element. TE Provisioning Element resides in the trusted zone and may only communicate with the TEs via the Network Border Element (NBE). A TE or TE-BE may authenticate and establish a security association with the NBE before it can obtain configuration file from TE Provisioning Element. NBE may support both TLS and IPsec for establishing SA with the TEs (including TE-BE).

2.3.4 Application model for AAA in NGN

Based on security requirements for NGN in Y.2701 and the NGN authentication reference model in Y.2702, the NGN authentication reference model (Figure 2-5) depicts eight authentication reference points. Reference points (1) and (4) refer to transport of user traffic and may be viewed as depending on "horizontal" access control at the transport control level, whereas reference points (2) and (8) may be viewed as depending on control data between the transport and service control layers and therefore as being "vertical." This relationship is displayed in Figure 2-6.

Figure 2-5: End-to-end Reference Architectural Model (Y.2702 NGN Authentication)

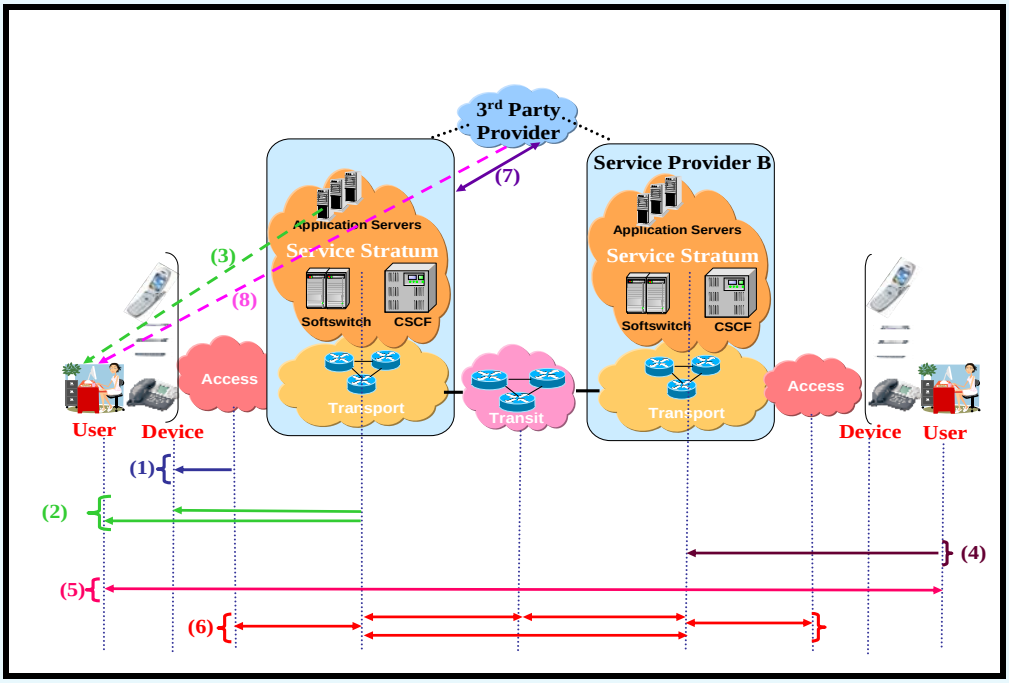
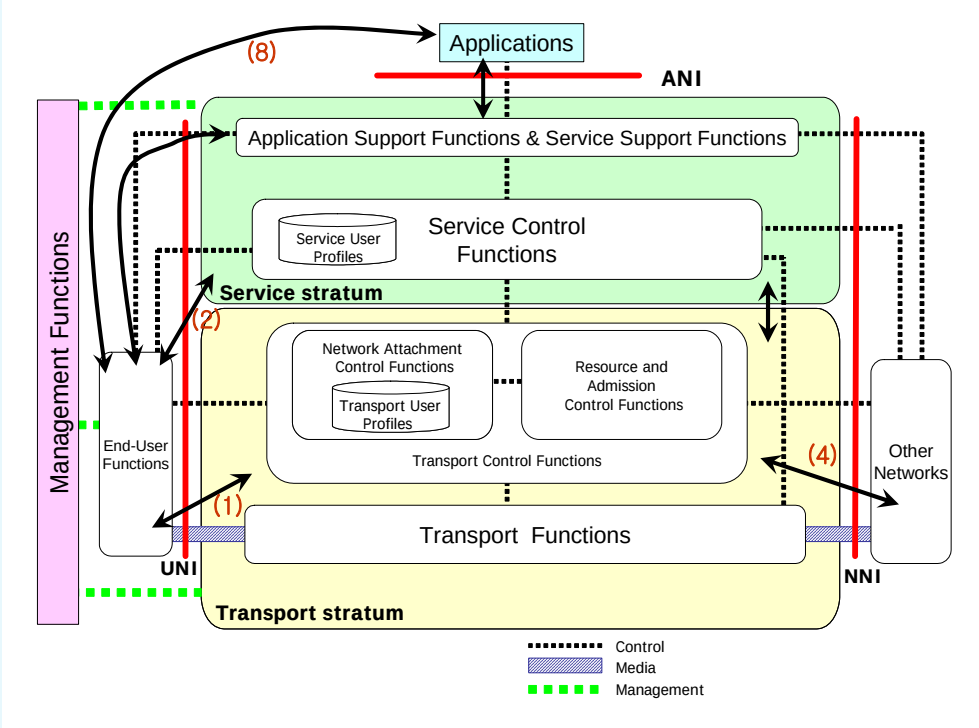


Figure 2-6: NGN Architecture and AAA related domains (Y.2702 NGN Authentication)

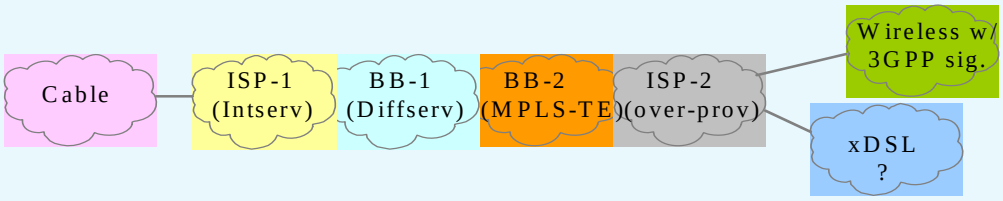


Annex 4: Quality of Service in NGN

1 Overview of QoS and NP in NGN

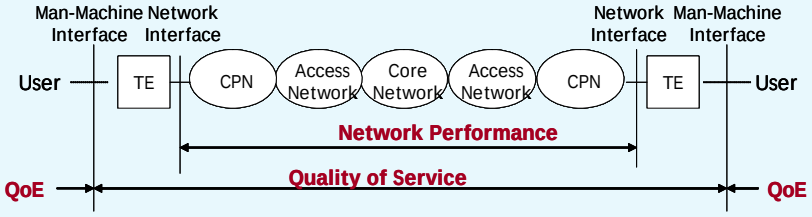
One of the key elements of NGN, which should be based on IP, is the guaranteeing of requested Quality of Services (QoS). The NGN have access and transport agnostic features which should be assumed in heterogeneous environments, so complexity of supporting the QoS is much more complicated. Figure 1-1 shows an example of this complexity.

Figure 1-1: QoS Complexity in Heterogeneous Network Environment



The general aspects of Quality of Service and network performance in NGN are developed to provide descriptions of NGN Quality of Service, Network Performance and Quality of Experience. Figure 1-2 shows the meaning and scope of QoS, QoE and NP with brief explanation about their features.

Figure 1-2: QoE, QoS and NP in NGN environment



Quality of Experience	Quality of Service	Network Performance
User oriented		Provider oriented
User behavior attribute	Service attribute	Connection/Flow element attribute
Focus on user-expected effects	Focus on user-observable effects	Focus on planning, development (design), operations and maintenance
User subject	Between (at) service access points	End-to-end or network elements capabilities

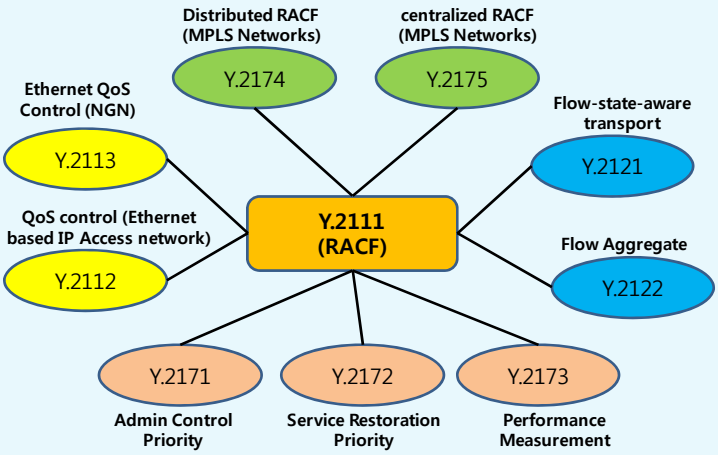
The NGN illustrates how these descriptions are applied in an NGN environment, describe performance aspects of NGN (including performance of service and transport stratum) and provide a basis for common understanding of performance concepts (useful to users and to the industries that compose the NGN – e.g., Fixed & mobile telecommunications, broadcasting, etc.). NGN defines the application QoS classes of the NGN.

The NGN determines the requirements to support QoS across multiple heterogeneous service providers. Existing standards specify several metrics and measurement methods for point to point performance. Notable are ITU-T Recommendations, Y.1540 and Y.1541 standards and the IETF IP Performance Metrics (IPPM) Working Group standards. The NGN considers the options and parameters left unspecified, taking into account the concatenation of performance over multiple network segments, allocation of impairment budgets, mapping between IP and non-IP metrics, accuracy, and data handling.

The network performance parameters of non-homogeneous networks in NGN are developed through the description of performance aspects of the transport layer in NGN. The NGN identifies general performance principles and frameworks that can be applied to the development of specific performance descriptions to support continuing evolution of the NGN. NGN defines the relationship among individual networks' performance which may be observed at physical interfaces between a specific network and associated terminal equipment, and at physical interfaces between specific networks.

A QoS Framework for IP based access networks is also developed in ITU-T through NGN-GSI. Reference architecture for IP access networks for QoS support is provided as well as detailed QoS requirements and validation procedures. The reference model would be part of the overall NGN framework with the service and transport layers, functional entities in each layer, and interfaces between the functional entities, in particular, the functional entities to facilitate interworking with the QoS functionality in the core network as well as that specific to each type of access networks.

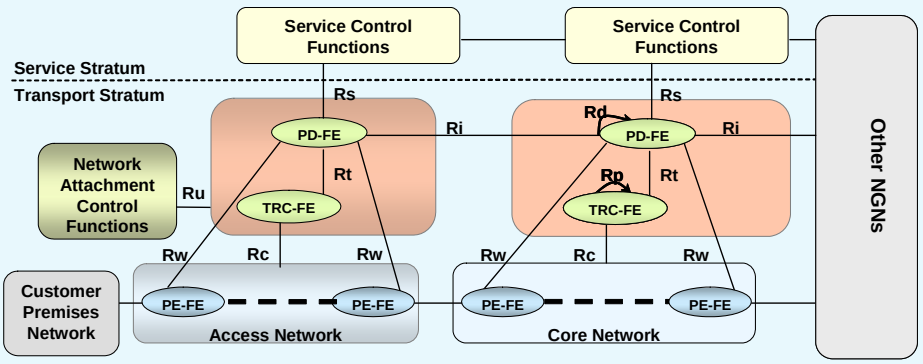
Figure 1-3: ITU-T NGN QoS related standards



2 Resource and Admission Control in NGN

Functional requirements and architecture for resource and admission control in NGN are developed to provide high-level requirements, scenarios and functional architecture. The decomposition to functional entities is specified to provide reference points and interfaces for the control of Quality of Service (QoS), Network Address and Port Translator (NAPT) and/or Firewall (FW) traversal are described.

Figure 2-1: Resource and Admission Control architecture model of NGN



- **QoS capability of CPE**: According to the capability of QoS negotiation, the CPE can be categorized as follows:

  a) Type 1 – CPE without QoS negotiation capability (e.g., vanilla soft phone, gaming consoles)

  The CPE does not have any QoS negotiation capability at either the transport or the service stratum. It can communicate with the SCF for service initiation and negotiation, but cannot request QoS resources directly.

  b) Type 2 – CPE with QoS negotiation capability at the service stratum (e.g. SIP phone with SDP/SIP QoS extensions)

  The CPE can perform service QoS negotiation (such as bandwidth) through service signalling, but is unaware of QoS attributes specific to the transport. The service QoS concerns characteristics pertinent to the application.

  c) Type 3 – CPE with QoS negotiation capability at the transport stratum (e.g. UMTS UE)

  The CPE supports RSVP-like or other transport signalling (e.g. GPRS session management signalling, ATM PNNI/Q.931). It is able to directly perform transport QoS negotiation throughout the transport facilities (e.g. DSLAM, CMTS, SGSN/GGSN).

  Note that the SCF shall be able to invoke the resource control process for all types of CPE.

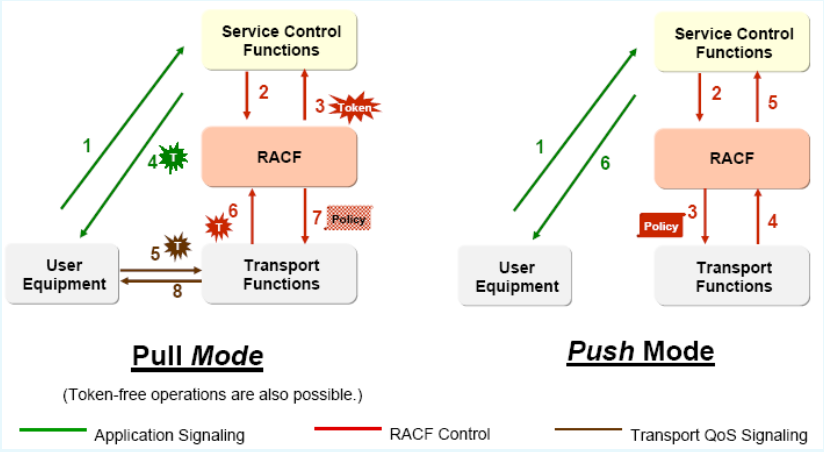
- **Resource control modes**: In order to handle different types of CPE and transport QoS capabilities, the RACF shall support the following QoS resource control modes as part of its handling of a resource request from the SCF:

  a) Push Mode: The RACF makes the authorization and resource control decision based on policy rules and autonomously instructs the transport functions to enforce the policy decision.

  b) Pull Mode: The RACF makes the authorization decision based on policy rules and, upon the request of the transport functions, re-authorizes the resource request and responds with the final policy decision for enforcement.

The Push mode is suitable for the first two types of CPE. For type 1 CPE, the SCF determines the QoS requirements of the requested service on behalf of the CPE; for type 2 CPE, the SCF extracts the QoS requirements from service signalling. The Pull mode is suitable for type 3 CPE, which can explicitly request QoS resource reservation through transport QoS signalling.

Figure 2-2: Pull and Push mode of RACF operation



- **Resource control states**: Regardless of the QoS negotiation capability of a particular CPE and the use of a particular resource control mode, the QoS resource control process consists of three logical states:

  a) Authorization (Authorized): The QoS resource is authorized based on policy rules. The authorized QoS bounds the maximum amount of resource for the resource reservation.

  b) Reservation (Reserved): The QoS resource is reserved based on the authorized resource and resource availability. The reserved resource can be used by best effort media flows when the resource has not yet committed in the transport functions.

  c) Commitment (Committed): The QoS resource is committed for the requested media flows when the gate is opened and other admission decisions (e.g. bandwidth allocation) are enforced in the transport functions.

  d) The general resource control criteria shall be:

  e) The amount of committed resources is not greater than the amount of reserved resources.

  f) The amount of reserved resources is not greater than the amount of authorized resources.

Note that the amount of committed resources typically equals the amount of reserved resources.

- **Resource control schemes**: Given the variety of application characteristics and performance requirements, the RACF supports three resource control schemes:

  a) Single-Phase Scheme: Authorization, reservation and commitment are performed in a single step. The requested resource is immediately committed upon successful authorization and reservation. The Single-Phase Scheme is suitable for client-server-like applications to minimize the delay between the service request and the ensuing reception of content.

  b) Two-Phase Scheme: Authorization and reservation are performed in one step, followed by commitment in another step. Alternatively authorization is performed in one step, followed by reservation and commitment in another step. The Two-Phase Scheme is suitable for interactive applications, which have stringent performance requirements and need to have sufficient transport resources available.

  c) Three-Phase Scheme: Authorization, reservation and commitment are performed in three steps sequentially. The Three-Phase Scheme is suitable for network-hosted services in an environment where transport resources are scarce.

- **Information for resource control**: The RACF shall perform the resource control based on the following information:

  a) Service Information: A set of data provided by the SCF for a resource control request, derived from service subscription information, service QoS requirement and service policy rules.

  b) Transport Network Information: A set of data collected from the transport networks, which may consist of transport resource admission decisions and network policy rules.

  c) Transport Subscription Information: A set of data for the transport subscription profile such as the maximum transport capacity per subscriber.

- **Policy rules for the enforcement of resource control results**: The RACF may assist the installation of two types of policy rules related to the enforcement of resource control results:

  a) Policy Decision: A set of policy conditions and actions for the enforcement of resource control results on a per flow basis, which is produced dynamically upon the individual resource request from the SCF. The RACF shall make policy decisions based on the information for resource control described in above paragraph and install the policy decisions to the transport functions autonomously or upon the request of the transport functions. The policy decision can be modified and updated within the lifetime of a resource control session.

  b) Policy Configuration: A set of static policy rules for default network resource configuration. The policy configuration is pre-defined by network operators and does not vary from the individual resource request. The policy configuration can be pre-provisioned statically in transport functions, e.g. mapping rules of the IP layer QoS to link layer QoS. In some cases, the RACF may help install the initial policy configuration for resource control, such as default resource control configuration (e.g. default gate setting).

Note that the RACF may use the soft-state (state that has a lifetime and requires renewal to keep alive) or hard-state (state that is persistent until explicitly removed) approach in support of transport resource control.

Annex 5: NGN Management

1 Objectives of NGN Management

The objectives of the management is to facilitate the effective interconnection between various types of Operations Systems (OSs) and/or resources for the exchange of management information using an agreed architecture with standardized interfaces including protocols and messages. Many network operators and service providers have a large infrastructure of OSs, telecommunications networks and equipment already in place, and which must be accommodated within the architecture in terms of managements. Management also provides capabilities for end-users with access to, and display of, management information, and end-user-initiated business processes. By considering these, it is noted that a management framework contributes to increase customer satisfaction and at the same time underpins a significant reduction in operating costs through new technologies and operational methods.

Within the context of NGN, management functionality refers to a set of management functions to allow for exchanging and processing of management information to assist network operators and service providers in conducting their business efficiently. NGN management (NGNM) provides management functions for NGN resources and services, and offers communications between the management plane and the NGN resources or services and other management planes.

This document introduces summary information about the NGN management based on Recommendation ITU-T M.3060 developed by SG2. M.3060 identifies the management architecture needs to address followings:

- Administrative boundaries amongst operator domains;
- Processes amongst operators across the domain boundaries;
- Processes between Operators and their suppliers' equipments;
- Reference points between the logical functions for Provider and Consumer;
- Provider and Consumer Interfaces between the physical entities used to realize the provider and consumer reference points;
- Information model concepts used to support logical functions.

In addition to this, M.3060 also identifies objectives of NGN management as following:

- minimize mediation work between different network technologies through management convergence and intelligent reporting;
- minimize management reaction times to network events;
- minimize load caused by management traffic;
- allow for geographic dispersion of control over aspects of the network operation;
- provide isolation mechanisms to minimize security risks;
- provide isolation mechanisms to locate and contain network faults;
- improve service assistance and interaction with customers;
- layering of services to enable a provider to provide the building blocks for services and others to bundle the services and its implications on the management architecture;
- business processes as defined in the M.3050.x series and how they would be used in NGN;
- support of applications, both on the same distributed computing platform and those distributed throughout the network.

The following areas are identified for further study issues.

- implications of the need to manage end-to-end services;

- implications of home networks and customer premises equipment.

2 Architecture of NGN Management

2.1 NGN Management Requirements

NGN management supports the monitoring and control of the NGN services and relevant resources for the service and transport via the communication of management information across interfaces between NGN resources and management systems, between NGN-supportive management systems, and between NGN components and personnel of service providers and network operators. NGN management supports the aims of the NGN based on Recommendation ITU-T Y.2201. Followings are key summary of NGN management requirements:

- Providing the ability to manage NGN system resources, both physical and logical including resources in the core network, access networks, interconnect components, and customer networks and their terminals;
- Providing the ability to manage NGN Service Stratum resources and enabling organizations offering NGN end-user services including the ability to personalize end-user services and customer self-service (e.g., provision of service, reporting faults, online billing reports);
- Supporting eBusiness Value Networks based upon concepts of business roles including support of B2B processes;
- Allowing an enterprise and/or an individual to adopt multiple roles in different value networks and also multiple roles within a specific value network;
- Integrating an abstracted view on Resources (network, computing and application);
- Supporting the collection of charging data for the network operator regarding the utilization of resources in the network;
- The ability to provide survivable networks in the event of impairment and proactive trend monitoring;
- Enable service providers to reduce the time-frame for the design, creation, delivery, and operation of new services;
- The ability to manipulate, analyse and react to management information in a consistent and appropriate manner.

2.2 NGN Management Architecture

The NGN management plane is the union of the NGN service stratum management plane and the NGN transport stratum management plane following the basis of NGN functional architecture. It may include joint management functions, i.e., functions used to manage entities in both strata plus functions required to support this management.

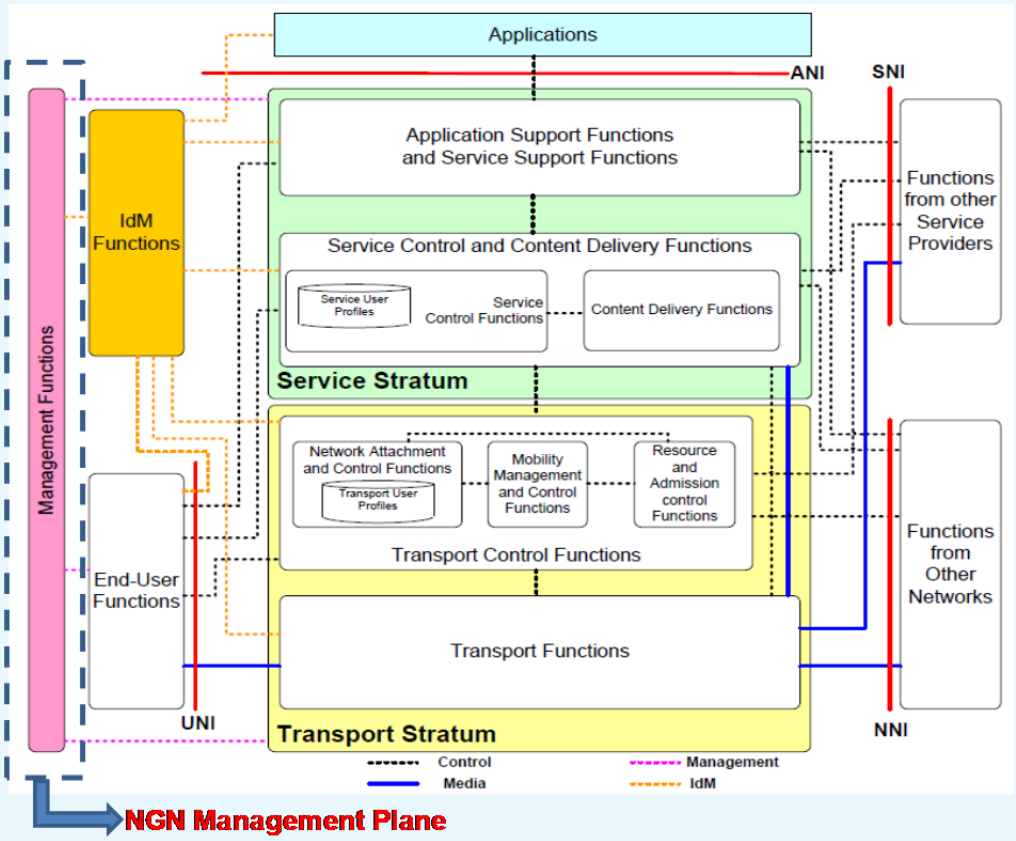
Referring to Recommendation ITU-T Y.2011 as shown in Figure 2-1, NGN management plane places to cover both transport and service strata as well as other functions such as IdM functions and End-user functions.

The NGN Management architecture will be divided into four different architectural views as shown in Figure 2-2 as followings:

- Business Process View: The business process view, based on the eTOM model (ITU-T Rec. M.3050.x-series), provides a reference framework for categorizing the business activities of a service provider;

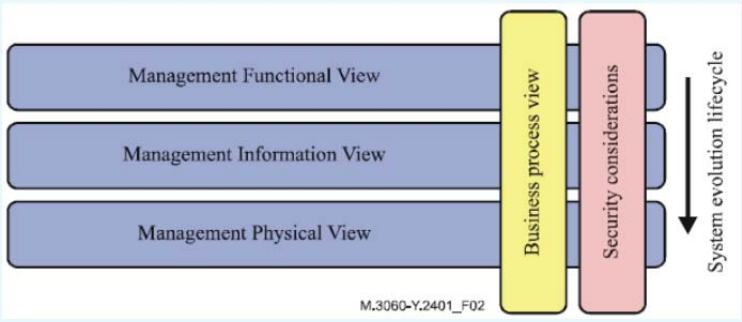
- Management Functional View: The functional view permits the specification of what functions have to be achieved in the management implementation;
- Management Information View: The information view characterizes the management information required for communication between the entities in the functional view to enable the performance of the functions to be achieved in the management implementation;
- Management Physical View: The physical view describes the varied ways that management functions can be implemented. They may be deployed in a variety of physical configurations using a variety of management protocols.

Figure 2-1: NGN management plane in the NGN architecture



Each view shows a different perspective into the architecture. These four architecture views also take security into consideration. Figure 2-2 describes the workflow in the creation of management specifications, where first the functional view is defined, followed by the information view and finally the physical view. The Business Process is an influence throughout the lifecycle. Note that, in practice, this process is iterative to enable all aspects of the architecture to evolve over time as required.

Figure 2-2: NGN management architecture



2.3 Relationship to service-oriented architecture (SOA)

One of the architectural principles used in the management architecture for NGN is that of being a Service-Oriented Architecture (SOA). A SOA is software architecture of services, policies, practices and frameworks in which components can be reused and repurposed rapidly in order to achieve shared and new functionality. This enables rapid and economical implementation in response to new requirements thus ensuring that services respond to perceived user needs.

SOA uses the object-oriented principle of encapsulation in which entities are accessible only through interfaces and where those entities are connected by well-defined interface agreements or contracts.

Major goals of an SOA in comparison with other architectures used in the past are to enable:

- faster adaptation to changing business needs;
- cost reduction in the integration of new services, as well as in the maintenance of existing services.

SOA provides open and agile business solutions that can be rapidly extended or changed on demand. This will enable NGN Management to support the rapid creation of new NGN services and changes in NGN technology.

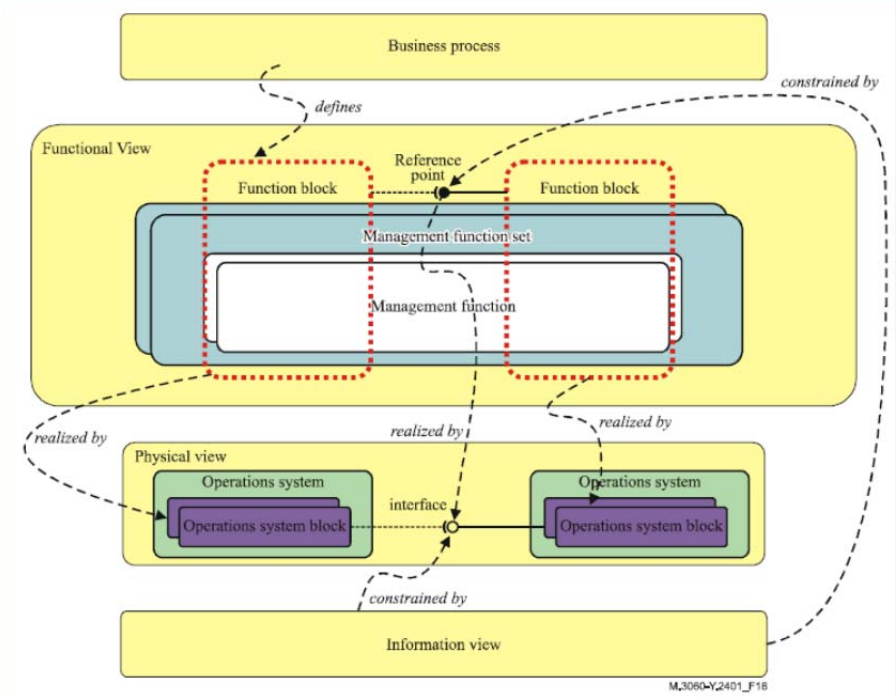
The main features of SOA are:

- loosely coupled, location independent, reusable services;
- any given service may assume a client or a server role with respect to another service, depending on situation;
- the "find-bind-execute" paradigm for the communication between services;
- published contract-based, platform and technology-neutral service interfaces. This means that the interface of a service is independent of its implementation;
- encapsulating the lifecycle of the entities involved in a business transaction; and exposing a coarser granularity of interfaces than OOA.

3 Relationships between management views

A business process provides a set of requirements that defines management functionality in the functional view. This management functionality is composed of management function sets that are composed of management functions. Operations systems realize a number of functional blocks, deployable units of management functionality, in the physical view. The functional view defines reference points that involve interaction between functional blocks. The information view constrains the data and interaction patterns of the interface between operations systems components that are physical realizations of functional blocks. Figure 3-1 shows this relationship between management views and their components.

Figure 3-1: Relationship of management views and their constructs



The management implementation is realized from four different, but interrelated views. These are the business process, functional, information and physical views. Three of these views (business process, functional and information) provide a framework that allows requirements to be documented about what a management implementation should do. The business process view, based on the eTOM model, provides a reference framework for categorizing the business activities of a service provider. The functional view framework permits the specification of what functions have to be achieved in the management implementation. The information view permits the specification of what information (i.e., data) has to be stored so that the functions defined in the functional view can be achieved in the management implementation. The management implementation, that meets the requirements of the management functional and information specifications, may vary greatly from one management solution to another. Management implementations are not currently a subject for standardization.

Annex 6: NGN Testing

1 Background

According to the transition of public telecommunication networks migration from digital circuit-switched to packet switching networks, especially aiming for IP-based network infrastructure, the testing of NGN including equipment testing become of primary importance. Ideally the operator expects to be offered equipment of high quality from the industry. But rapid growth of new technologies and the increase of equipment complexity, it is not easy to confirm the satisfaction of interesting in both operators and industries. However integral testing performed on operator networks is quite costy and it would not be reasonable to wait for external events like incidents affecting the operator networks in order to test them. It seems that the methodology of integral testing may be complemented and updated by the creation of model networks to perform equipment compatibility tests, followed by subsequent resource integration of the model networks to ensure full-fledged integral testing taking into account the interworking testing results.

By considering above, it is required that the study should be covered both compatibility and interoperability testing of various vendors' NGN equipment including new services with the existing ones in the process of NGN equipment operation. ITU-T, especially SG11 is being involved in this study as well as ETSI. This annex introduces summary information about the NGN testing based on Recommendations ITU-T Q.3900 (2006) and Q.3909 (2011) developed by SG11.

2 Technical means and functions to be tested

2.1 NGN technical means to be tested

NGN technical means which identifies as the NGN basic equipment to serve for building NGN solutions including for application shall be implemented taking into account the mandatory NGN function set. It is noted that, at the same time, the composition and number of protocols and interfaces in the specified functionality may be implemented by the manufacturer. For the purposes of standards development, the technical means functionality implemented by the manufacturer, including the requirements for the protocols and interfaces to be implemented in the specified functionality, are assumed to be in complete conformance with the functionality and purpose defined in the NGN requirements (see [ITU-T Y.2012] and [ITU-T Y.2201]).

Recommendation ITU-T Q.3900 introduces following classifications of NGN technical means in public networks as shown in Table 2-1.

Table 2-1: Classification of NGN technical means

System	NGN Technical Means
Call session control system	Media gateway controller (MGC)
	Proxy server SIP (PS)
	IP multimedia subsystem (IMS)
Voice and signalling transmit system	Media gateway (GW)
	Signalling gateway (SG)
	Transport network environment (TNE)
Application servers	Application server (AS)
	Media server (MDS)
	Messaging server (MeS)

System	NGN Technical Means
Management and billing system	NGN management system (NMS)
	Billing system (BS)
Access environment	NGN integrated access devices (NGN-IAD)
	Media gateway for legacy terminal equipment (GW-LTE)

Recommendation ITU-T Q.3900 identifies more details about functionality of the key NGN technical means from above means used in public networks as shown in Table 2-2.

Table 2-2: Functionality of key NGN technical means to be tested

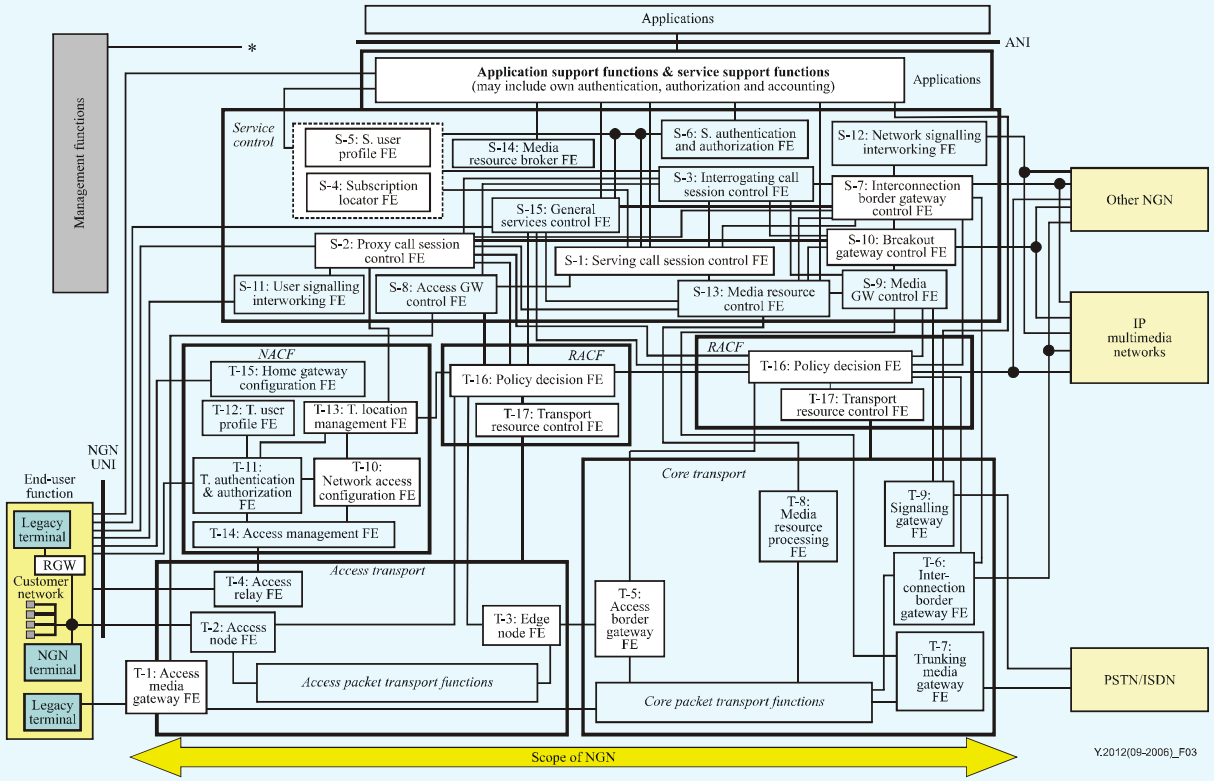
Technical means	Functionality
Media gateway controller (MGC)	• controls the calls among the PSTN subscribers; • provide for a basic part of functionality while controlling the communication sessions (transfer of routing tables, reconfiguring the numbering systems among various numbering plan formats, Media Gateway controlling by means of the signalling protocols (MGCP, H.248/Megaco, H.323, SIP) and etc; • is a main component of softswitch as a part of main switching device in the NGN.
Application server (AS)	• a software server providing new services to the users; • provisioning of new services, for example, e-commerce and electronic trade; • functionally perform as most of the NGN network components in the field of COMMUNICATION SESSION AND SERVICES CONTROL AREA; • a more flexible management of network capabilities and the creation of new and promising network scenarios.
Media server (MDS)	• provides services of interaction between the user and application or other additional communication services by means of voice and DTMF instructions. The MDS architecturally may be divided into: 1) A Media Resource Control Unit ensuring DTMF recognition, speech synthesis, speech recognition, etc; 2) A Service Control Unit ensuring forwarding messages into the message line, message recording, transfer of facsimile services, arranging conference communication, etc; • may be implemented on various software and hardware platforms based on the VoiceXML languages and so on.
Messaging server (MeS)	• responsible for message saving and message transfer to the users; • provide users with additional communication services.
Media gateway (GW)	• provides the functions of transforming the voice information into a digital format and its transfer through the NGN; • performs coding of the amplitude-frequency signals through integrated codecs (G.711, G.723, G.726, G.729, etc.), as well as transfer of digitized signals with the aid of transport protocols RTP/RTCP; • implemented, at least, one of the assortment of protocols (H.323, MGCP, H.248/Megaco, SIP) to establish connection within the GW; • used for the arrangement of interaction on the level of voice circuits between a Circuit Switched Network and NGN.
Signalling Gateway (SG)	• allows to convert and send a signalling load of the PSTN network to the MGC and converts such signalling types as ISDN, SS7, etc; • transfer of the SIGTRAN-stack protocols is effected over the SCTP transport protocol; • used at the boarder of the NGN and the PSTN including the arrangement of interaction.
Configuration	• provide management and control of all the NGN technical means;

Technical means	Functionality
and management system (MS)	• construct with the use of distributed and object-oriented structure with multi-protocol; • interfaces should be open using standard protocols (IIOP, CMIP, SNMP, FTP, FTAM, etc.) and the usage of formal languages for description of standard interfaces (CORBA IDL, JAVA, GDMO, ASN.1, etc.).

2.2 NGN functions to be tested

The main NGN functions to be tested as mandatory are classified as Transport stratum functions, Service stratum functions, End-user functions and Management functions. To test such functions, it is necessary to understand in more detail their internal functionality, to determine the purpose and degree of their responsibility (see Recommendation ITU-T Y.2012). An NGN functional architectures showing the detailed functionality is given in Figure 2-1.

Figure 2-1: NGN functional architecture



The presented NGN technical means may implement, within their composition, several functions at a time. The function sets implemented in particular technical means will be defined as following:

1) Transport functions:

- User connection to the NGN (Access Transport Functions (ATF): T-1, T-2, T-4);
- Transfer of traffic from the access network to the common transport network with the support of ATF and an additional routing capability (Edge&Access Border Gateway Functions: T-3, T-5);

- Transfer and management of all types of information (media streams, signalling messages and control system signals) being transmitted over the transport network (Core Transport Functions: T-8, T-9, T-6, T-7).

2) Transport control functions:

- QoS management including resource management, management of Network Address and Port Translation (NAPT) and NAPT Traversal at the access and transport layer. Testing should be divided for each layer separate with tests both for Access Transport Resource Control (ATRC) and for Core Transport Resource Control (CTRC). Testing of the resource control function should incorporate: packet filtering, traffic classification, service priority policies, passband reservation, network address translation, Firewall (RACF: T-17 for both access and core);
- Control of user access to the network resources (Admission Control Function) such as user authorization based on the profile should be checked (SLA, service priority, access policies determined by the type of the model network used for testing) and the access and/or transport resources available to the user (RACF: T-16 for both access and core);
- Control of user access to NGN services such as dynamic allocation of IP addresses and additional configuration parameters needed for user identification/authentication, at the network layer, for access to the network and user localization (NACF: T-10, T-11, T-13, T-14) ;
- Control of home gateway (HGW) configuration functionality such as configuration of a firewall internally in the HGW, QoS marking of IP packets, etc. (NACF: T-15).

3) Transport user profile functions: checking the possibility of configuring and modifying the information contained in the user profile at the transport layer (Transport stratum: T-12);

4) Service control functions:

- User registration and authorization at the service layer (S-6);
- Management media streams, terminal equipment and gateways (S-1, S-11, S-8, S-2, S-3, S-12, S-7, S-10, S-9, S-13).

5) Application/Service support functions:

- User registration and authorization at the application layer, for user access to the telecommunication services provided by application servers (S-4, S-5, S-6);
- Management of media streams and telecommunication services (S-14, S-15).

6) Service user profile functions: checking the capability of configuring and modifying the information contained in the user profile at the service control layer and checking the capability of interaction with the user-profile databases of other NGN architecture layers;

7) End-user functions: checking the capabilities of the terminal equipment from the gateway, to which conventional telephone sets are connected, to the multipurpose sets designed specifically for NGN networks include checking codecs, echo-cancellation systems, signalling systems and functions of interaction with the relevant NGN layers;

8) Management functions:

- Error processing management;
- Equipment configuration management;
- Billing system management;
- Service management;
- Security management.

2.3 Conformance of NGN functions to NGN technical means to be tested

The technical means used in NGN networks may implement the functionalities within their composition as shown in Table 2-3.

Table 2-3: Conformance of NGN technical means into NGN functionality

NGN technical means	NGN functionality
Call session control system	
Media gateway controller (MGC)	S-3, S-7, S-9, S-10, S-12 T-10, T-11, T-12, T-13
Proxy server SIP (PS)	S-2, S-3, S-7, S-11, S-12 T-10, T-11, T-12, T-13
IP multimedia subsystem (IMS)	S-1, S-3, S-6, S-7, S-8, S-10, S-12, S-13 T-10, T-11, T-12, T-13, T-14, T-15, T-16, T-17
Voice and signalling transmit system	
Media gateway (GW)	T-7, T-8
Signalling gateway (SG)	T-8, T-9
Transport network environment (TNE)	T-5, T-6, T-8
Application servers	
Application server (AS)	S-4, S-5, S-6, S-14, S-15
Media server (MDS)	S-4, S-5, S-6, S-14, S-15
Messaging server (MeS)	S-4, S-5, S-6, S-14, S-15
Management and billing system	
Management system (MS) Billing system (BS)	– Error processing management – Equipment configuration management – Billing system management – Service management – Security management
Access environment	
NGN integrated access devices (NGN-IAD)	T-2, T-4, T-3, T-5, T-15, T-14
Media gateway for legacy terminal equipment (GW-LTE)	T-1, T-2, T-3, T-4, T-5

3 Model networks for NGN testing

There are two types of model networks for NGN testing: dedicated model and distributed model networks. It should be noted that, although creation of model networks appears to be a promising testing method, not all countries are in a position to implement them to the necessary extent desired. Hence, it is reasonable to create regional model networks whose resources could be employed for testing by various countries located in the given region.

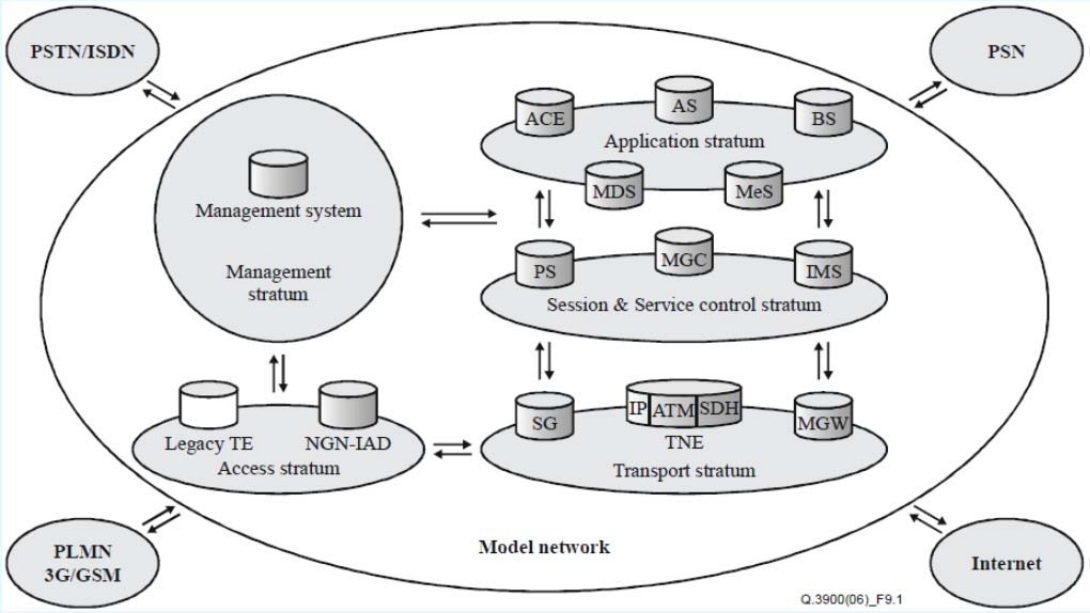
Device Under Test (DUT) may be accessed by the NGN test lab through dedicated model or distributed model. One basic requirement for such a remote testing is that the DUT must appear to the tester as it is connected directly. This is possible by creating a tunnel between the tester and the DUT using appropriate tunneling technology. Tunneling technology can be used, along with pseudo –wire capability in routers, to send the test packets directly to the remotely placed DUT. The available test suits thus become suitable for remote testing.

3.1 Dedicated model network

A dedicated model is a fragment network which is not connected to other model networks and used to perform testing for compatibility and, if possible, for interaction with the technical means employed prior to the NGN development period. The dedicated model network can be connected to a public telecommunication network and/or corporate network.

The basic architecture of a dedicated model network is shown following Figure 3-1.

Figure 3-1: Basic architecture of a model network (form of a dedicated model)



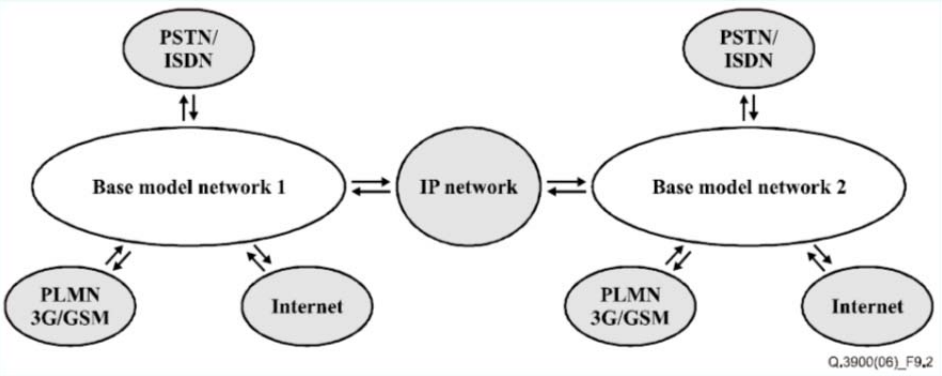
3.2 Distributed model network

A distributed model network is composed of several dedicated model networks, two as a minimum, and should be interconnected by the dedicated Intranet network such as VPN. The distributed model networks can also be connected to public telecommunication networks and/or corporate networks. The distributed model networks are used to perform complex tests for compatibility and interworking as well as to check quality of service parameters, information security requirements and interworking with the technical means. The minimum-size configuration of the model network should have:

- four nodes of the public telecommunication network (three of them should be of different types and two, as a minimum, should originate from different vendors);
- the communication networks inside the dedicated model networks provide internal communication (of the SDH, ATM or IP level) without limitation in types and manufacturers;
- four media gateways, the minimum of three of which should be of different types and the minimum of two should come from different manufacturers;
- four signalling gateways meeting the same different-type and manufacture brand requirements;
- four application servers, out of which at least two should be of different types;
- additional NGN technical means.

The basic architecture of a distributed model network is shown in Figure 3-2.

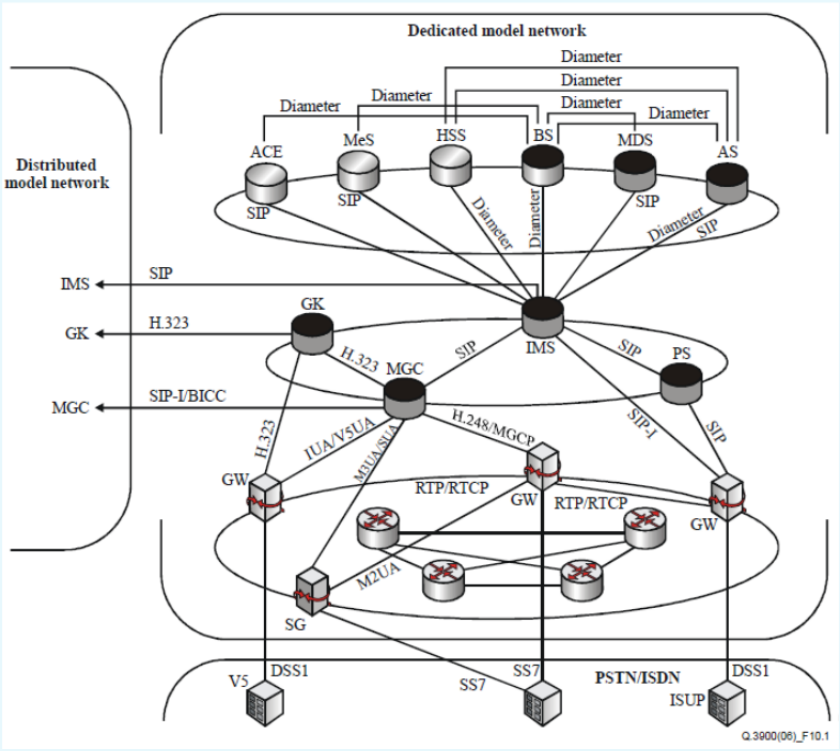
Figure 3-2: Architecture of a distributed model network in minimum-size configuration



3.3 Protocol configuration of model network

The protocols scheme of dedicated and distributed model networks must be realized in accordance with the scheme illustrated in Figure 3-3.

Figure 3-3: Protocol configuration of model network



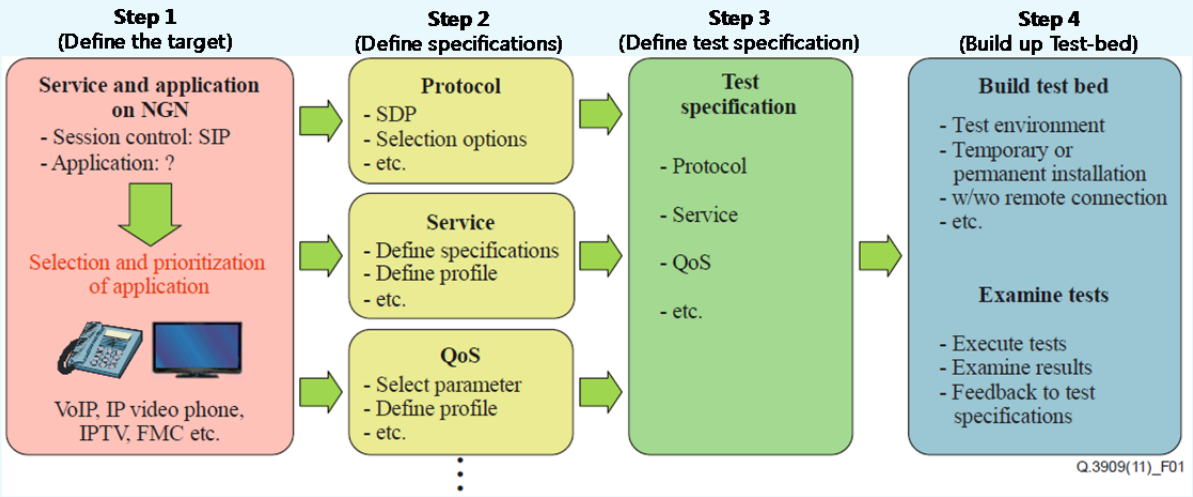
4 NGN conformance testing and interoperability testing

There are two tests to confirm the function of NGN standards: one is for conformance testing and the other is for interoperability testing. NGN conformance testing is able to show that a particular

implementation complies with the protocol requirements specified in the associated base standard. However, it is difficult for such testing to be able to prove that the implementation will interoperate with similar implementations in other products. On the other hand, NGN interoperability testing can clearly demonstrate that two or more implementations will cooperate to provide the specified end-to-end functions, but cannot easily prove that either of them conforms to the detailed requirements of the protocol specification. The purpose of interoperability testing is not only to show that target products from different manufacturers can work together, but also to show that these products can interoperate using a specific protocol.

Figure 4-1 shows a four-step approach on the specification process for NGN conformance testing and interoperability testing.

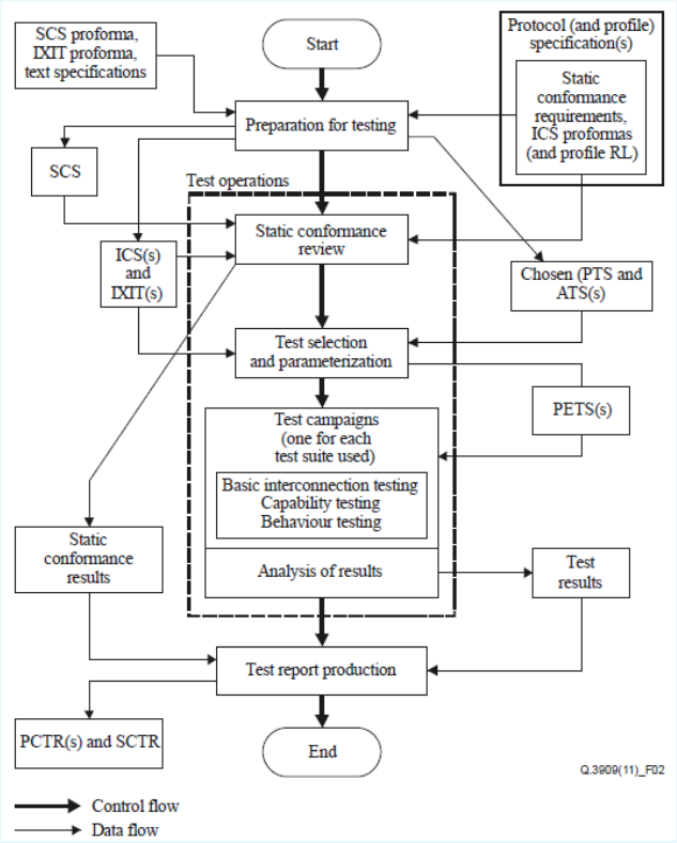
Figure 4-1: Typical NGN conformance and interoperability test specification process



4.1 NGN conformance testing

A conformance testing is performed on a product or a system to confirm that the protocol implemented in the target product (or system) is in accordance with the protocol specification described in specific Recommendations. Therefore NGN conformance testing is performed on NGN systems with relevant Recommendations. It is possible to refer to part of a procedure of the ITU-T X.29x-series as a procedure for NGN conformance testing. Figure 4-2 illustrates the overview of conformance testing of the execution procedure in [ITU-T X.290].

Figure 4-2: ITU-T X.290 conformance assessment process overview



NGN conformance testing should consider specifications on:

- the test subject which is connected to the tester or reference machine and examines conformity with reference Recommendations;
- certifications or the type of approval which may be given to the products passed by the testing authority (this is not a mandatory function of conformance testing);
- test specifications for the conformance testing which are specified in the test specification language (e.g., PICS, PIXIT).

The conformance assessment process involves following three phases: preparation, operation and reporting.

1st phase is the preparation for testing as following step:

1-1) Set the test object, target interface and target Recommendations,

1-2) Set the physical configuration and target products, and

1-3) Define the test scenarios.

2nd phase is for test operations with following step:

2-1) Static conformance review,

2-2) Test selection and parameterization,

2-3) Test campaigns (examine the conformance testing according to the scenarios) and,

2-4) Analysis of results.

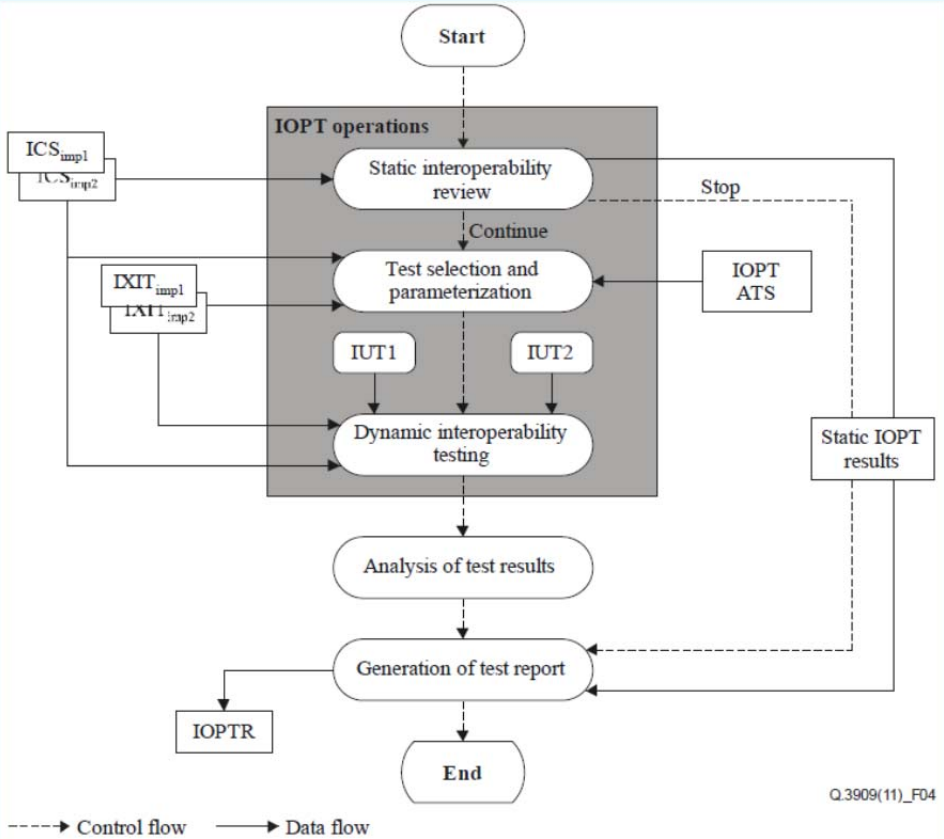
Finally 3rd phase is production of the test report.

4.2 NGN interoperability testing

Interoperability testing for NGNs is performed on two or more products. Its objective is to check the ability and performance of the products implemented by mutually exchanging information. The interoperability testing procedures of [ITU-T X-Sup.4] and [ITU-T X-Sup.5] may be referenced when undertaking NGN interoperability testing,

Figure 4-3 shows the overview of the execution procedure for interoperability testing which identified in [ITU-T X-Sup.4] and [ITU-T X-Sup.5].

Figure 4-3: Interoperability testing procedure



The execution procedure of interoperability testing in [ITU-T X-Sup.4] and [ITU-T X-Sup.5] is described as follows:

- The test operator should receive the information conformance statement (ICS) and implementation extra information for testing (IXIT), described in the applicable reference Recommendations;
- A static interoperability review is executed according to the content described in the ICSs and IXITs;
- If after review of the static interoperability test results, it is judged that interoperability testing does not need to be executed, then the test operation will be ended;

- When it is necessary to execute the tests, the settings of the test method, the test environment architecture and the test specification will be explained in detail during the process of test selection and parameterization;
- Dynamic interoperability testing is executed according to the procedure of the prepared test specification that is built in two or more implementations under test (IUTs) which, as target products, connected mutually;
- The test output in dynamic interoperability testing would be analyzed and the test result report would be generated.

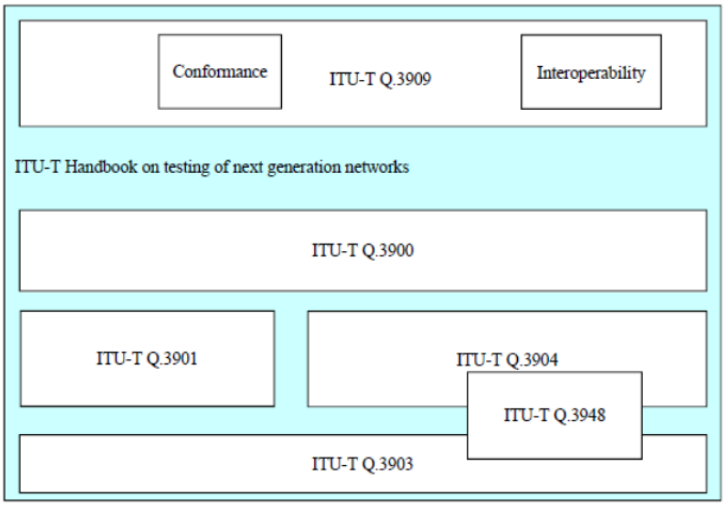
Interoperability testing for NGNs should consider specifications on multiple products from multiple vendors that are connected and tested for interoperability at the service and transport level, or both. And NGN interoperability testing should be conducted in the following steps:

1) Preparation for testing
   - 1-1) Set the test object, target interface and target Recommendations
   - 1-2) Set the physical configuration and target products
   - 1-3) Define the test scenarios.
2) IOPT operations
   - 2-1) Static interoperability review
   - 2-2) Test selection and parameterization
   - 2-3) Dynamic interoperability testing (examine the interoperability testing according to the test scenarios).
3) Analysis of test results.
4) Generation of test report.

4.3 Positioning map of NGN testing specification documents

A number of ITU-T Recommendations contain NGN testing specifications. Following Table 4-4 shows the relationship between the ITU-T Handbook on testing of NGN and ITU-T Recommendations specifying NGN testing.

Table 4-4: Recommendations for NGN tests

	NGN TM local testing			NUT testing					
Level	1.1	1.2	1.3	2.1	2.2	2.3	2.4	2.5	2.6
	Func-tional testing	Load and stress testing	Confor-mance testing	NUT func-tional testing	Inter-connect testing	Service testing	end-to-end testing	QoS testing	Mobility and roaming testing
Specifica-tion process									
General Procedure									
Methodo-logy									
Model network configura-tion									
Test scenarios									
Formalized results									

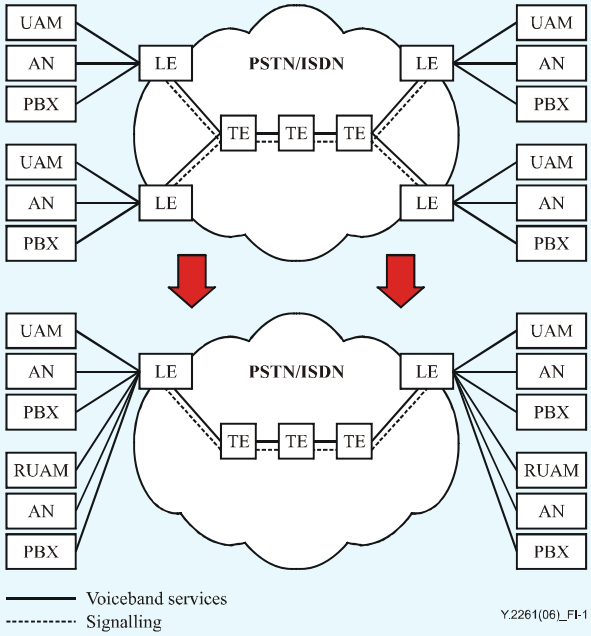
Annex 7: Examples of Migration Scenarios

1 Core Network migration to NGN

1.1 Consolidation of local and remote exchanges for migration to NGN

In order to prepare the PSTN/ISDN for the migration to a NGN, and as an initial step, some of the LEs (Local Exchanges) can be removed and all their functionalities such as control, accounting, etc. transferred to those remaining LEs. The affected UAMs (User Access Modules), PBXs, and ANs (Access Networks) are connected to the remaining LEs. Further consolidation occurs when UAMs become RUAMs (Remote UAMs), which are connected to the remaining LEs. Figure 1-1 shows this preparatory step.

Figure 1-1: Preparation for migration to NGN

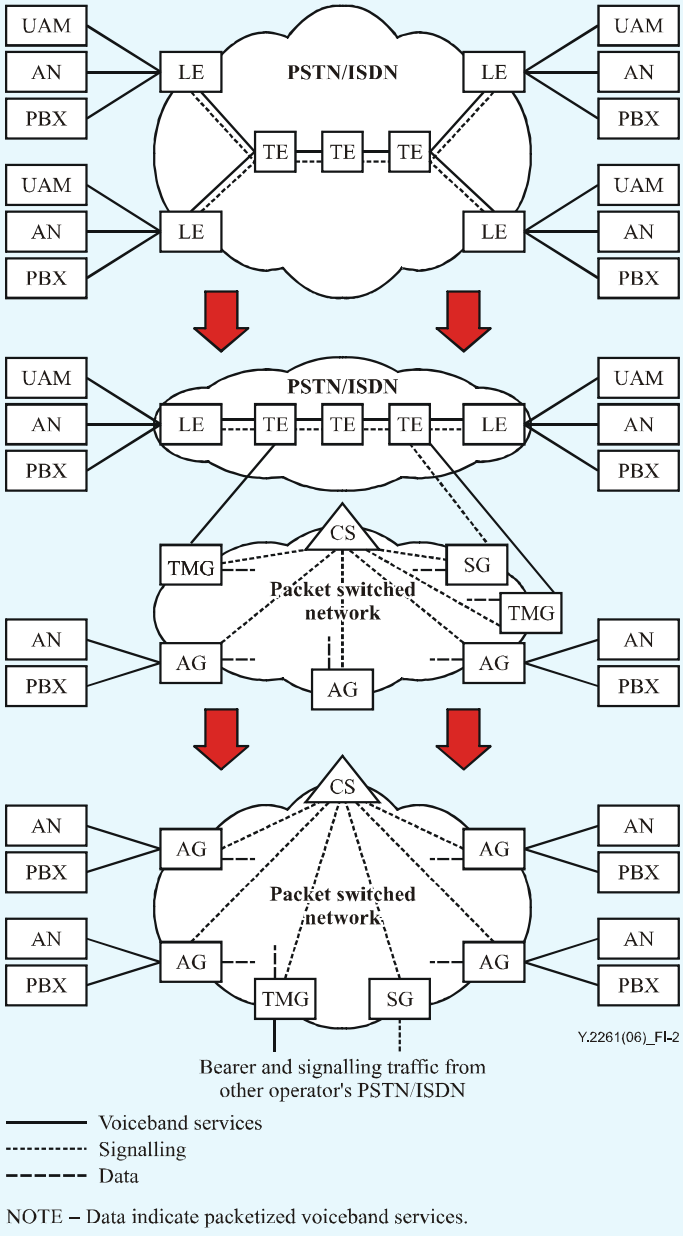


1.2 Scenario 1 – PSTN/ISDN and NGN initially co-exist

In the most likely initial approach for migration of PSTN/ISDN to the NGN, the PSTN/ISDN will co-exist with the NGN during a transition period. There are two steps in this scenario.

- Step 1: In this step, some of the LEs are replaced by AGs (Access Gateways). Functions originally provided by the removed LEs are now provided by the AGs and the CS. In addition, some of the access elements such as UAMs, RUAMs, and PBXs, which were originally connected to the removed LEs, are now directly connected to AGs. Additional AGs may also be deployed to support new subscribers that directly connect to them. The TMGs (Trunking Media Gateways) and SGs (Signaling Gateways) are deployed for interconnection between the NGN and the TEs of the legacy network as well as other operators' PSTNs/ISDNs. The AGs and TMGs are all controlled by the CS.
- Step 2: In this step, the remaining LEs are replaced by the AGs, and the TEs are removed and their control functions are performed by CS. The TMGs and SGs are deployed for interconnection between PSN and other operators' PSTNs/ISDNs. The AGs and TMGs are all controlled by the CS.

Figure 1-2: Realization of scenario 1



NOTE – Data indicate packetized voiceband services.

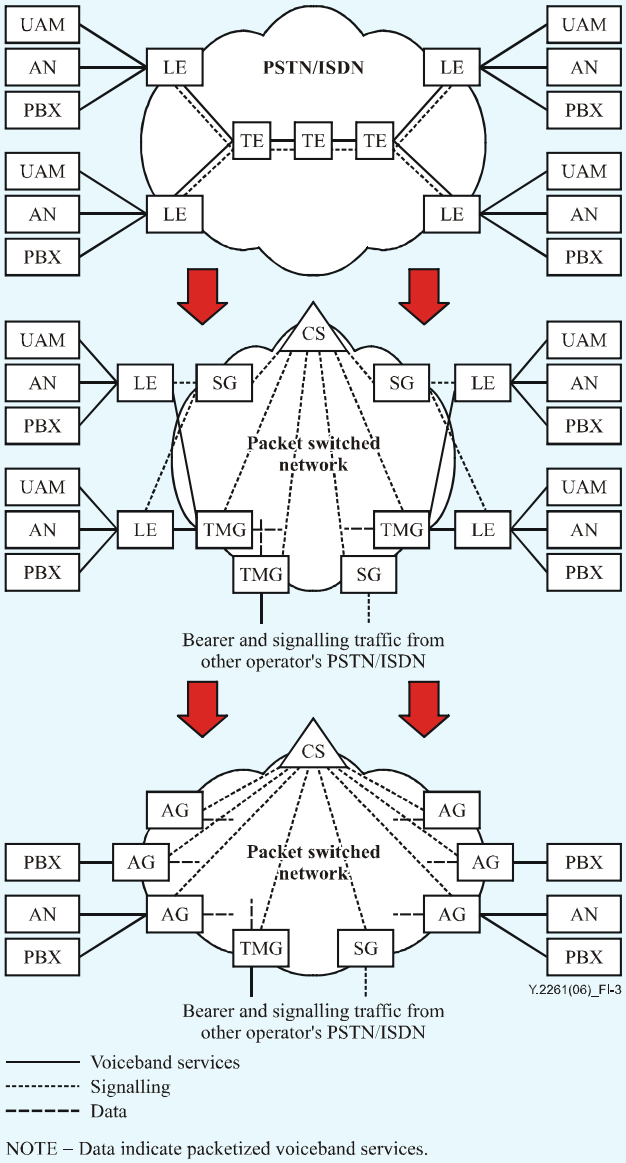
1.3 Scenario 2 – Immediate use of NGN, initially via SGs and TMGs

In this scenario, the PSTN/ISDN is immediately replaced by the NGN. As a first step, the LEs are connected to SGs and TMGs, while later on they are eliminated.

- Step 1: In this step, PSTN/ISDN is replaced by NGN and the TE functions are performed by the TMGs and the SGs under the control of the CS. The LEs are connected to the NGN via TMGs and SGs. The TMGs and SGs are also deployed for interconnection between NGN and other operators' PSTNs/ISDNs.

- Step 2: In this step, the LEs and some of the access elements such as UAMs and RUAMs are removed and their functions are provided by the AGs and CS. The PBXs are directly connected to the AGs. The ANs are either replaced by the AGs or are connected to the AGs. The TMGs and SGs are deployed for interconnection between NGN and other operators' PSTNs/ISDNs. The AGs and TMGs are all controlled by CS.

Figure 1-3: Realization of scenario 2

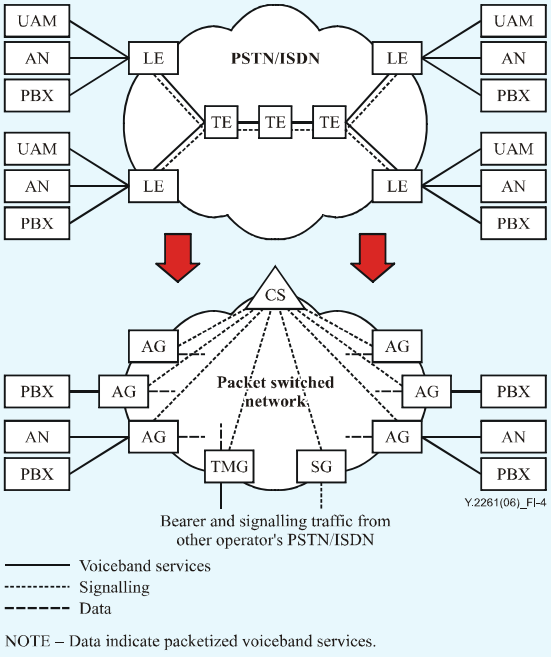


NOTE – Data indicate packetized voiceband services.

1.4 Scenario 3 – The one-step approach

In this scenario, the PSTN/ISDN is replaced with NGN in only one step. The LEs are replaced by AGs and their functions are divided between the AGs and the CS. Specifically, the call control and accounting functions are all transferred to the CS. All access elements such as UAMs, RUAMs, and PBXs are connected to AGs. The ANs are either replaced by the AGs or are connected to NGN through the AGs. The TMGs under the control of the CS, and the SGs, are deployed to replace the TE functions and provide interconnection between NGN and other operators' PSTNs/ISDNs.

Figure 1-4: Realization of scenario 3

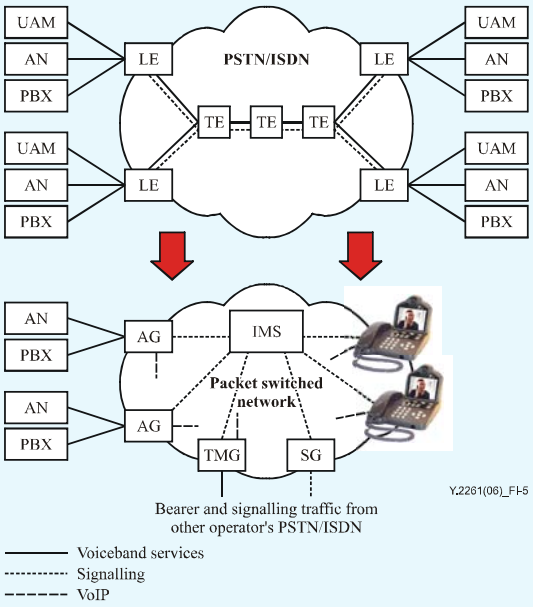


NOTE – Data indicate packetized voiceband services.

1.5 IMS-based migration to NGN

In the case of where PSTN/ISDN evolves directly to a NGN based on the IMS core network architecture, the end-users access the network using NGN user equipment or legacy user equipment connected via an AG. The TMGs and SGs are deployed for interconnection between the NGN and other operators' PSTNs/ISDNs.

Figure 1-5: IMS-based PSTN/ISDN migration to NGN

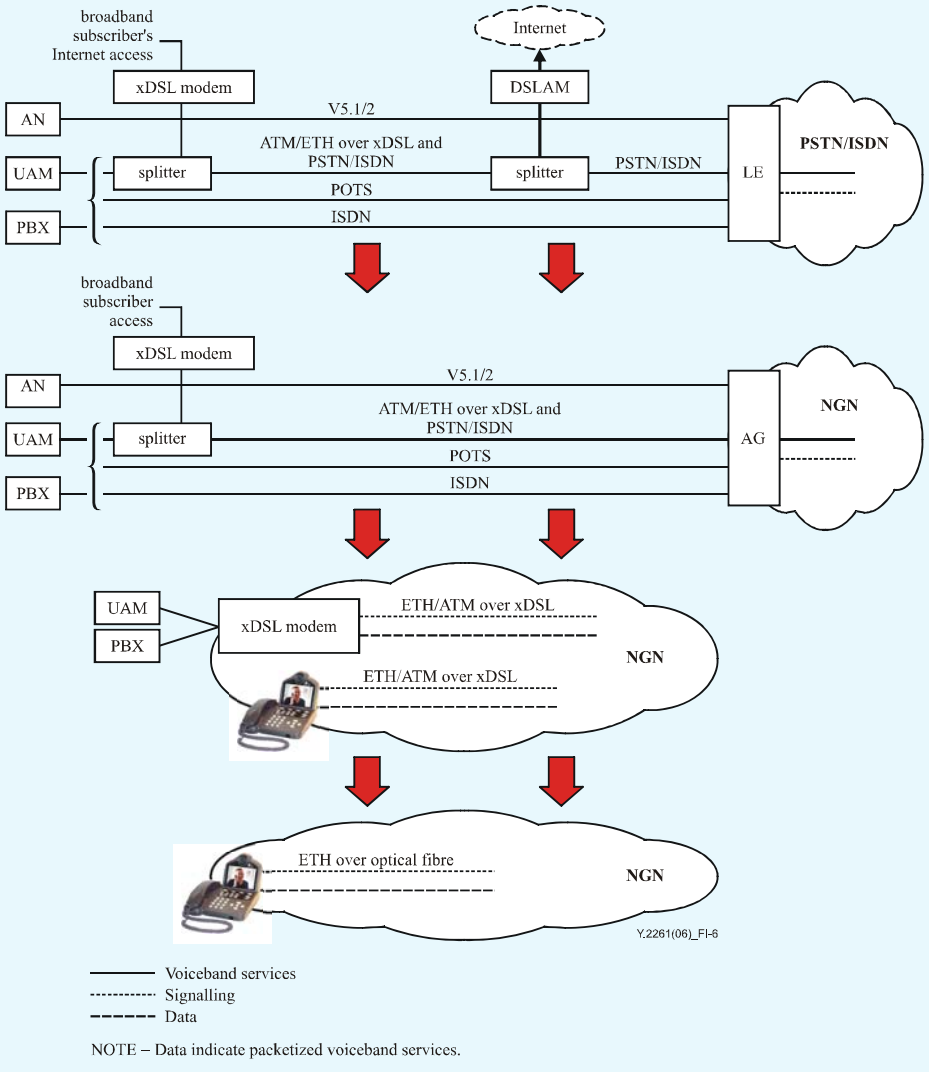


2 Access network migration to NGN

Legacy voice users may also have access to broadband services for example via xDSL (see [G.995.1]). In this case, the customer-located equipment is an xDSL modem and the service provider equipment is a digital subscriber line access multiplexer (DSLAM). Since xDSL interfaces enable users to connect to the Internet, these interfaces may be utilized to connect such users to NGNs. AN, for another user domain with V5.x [G.964] and [G.965] interface can be left as it is shown in Figure 5-6 or it can be completely replaced by AG connected to NGN directly. Migration of access network is shown in three possible steps.

- Step 1: Traditional AN/UAM interfaces include: POTS, ISDN and V5.1/2 [G.964] and [G.965]. Such interfaces connect subscribers to the core PSTN/ISDN via LE.
- Step 2: An IP user may also use xDSL interface as the transport medium to an NGN. Protocol for xDSL interface may be Ethernet which enables broadband data flows and services, e.g., VoD, IPTV, VoIP and Internet.
- Step 3: In this step, the legacy end systems are replaced by NGN end systems and twisted copper lines are replaced by optical fibre, either fibre-to-the-curb (FTTC) or fibre-to-the-home (FTTH) to increase transmission speed.

Figure 2-1: Migration of xDSL access to NGN



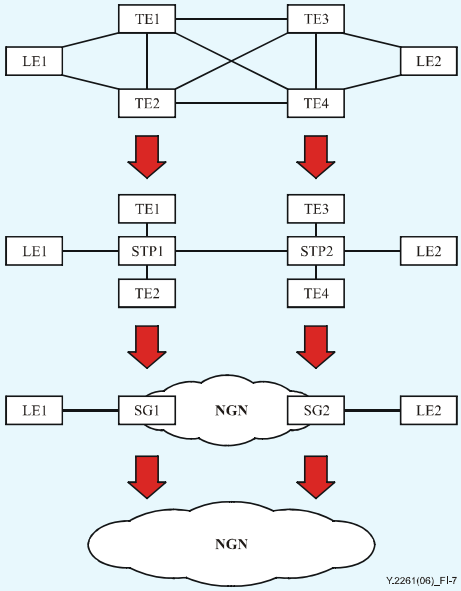
NOTE – Data indicate packetized voiceband services.

3 Signaling and control scenarios

A possible scenario for migration of signalling in the core network consists of following three steps.

- Step 1: In this step, signalling functions are transferred from the TEs to the independent units creating an STP mesh network (partial or complete).
- Step 2: In this step, STPs are upgraded to the SGs and are placed on the edge between PSTN/ISDN and NGN. In this case, both the legacy network and NGN co-exist with each other.
- Step 3: In this step, all LEs and TEs are replaced by NGN.

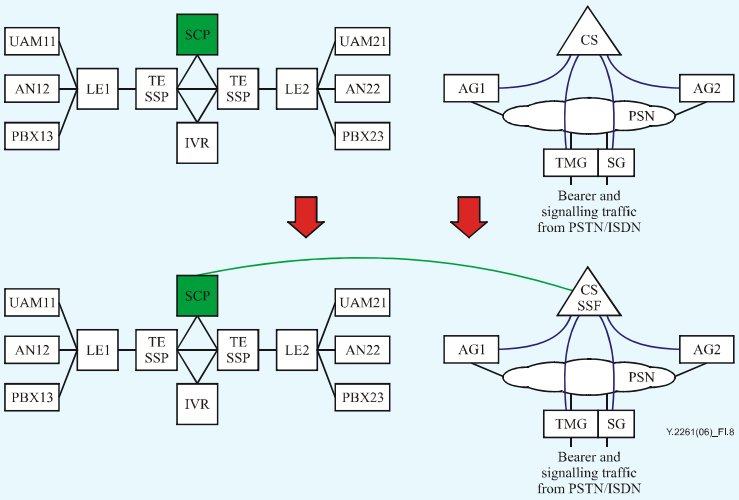
Figure 3-1: Realization of signalling migration scenario



4 Services migration scenarios

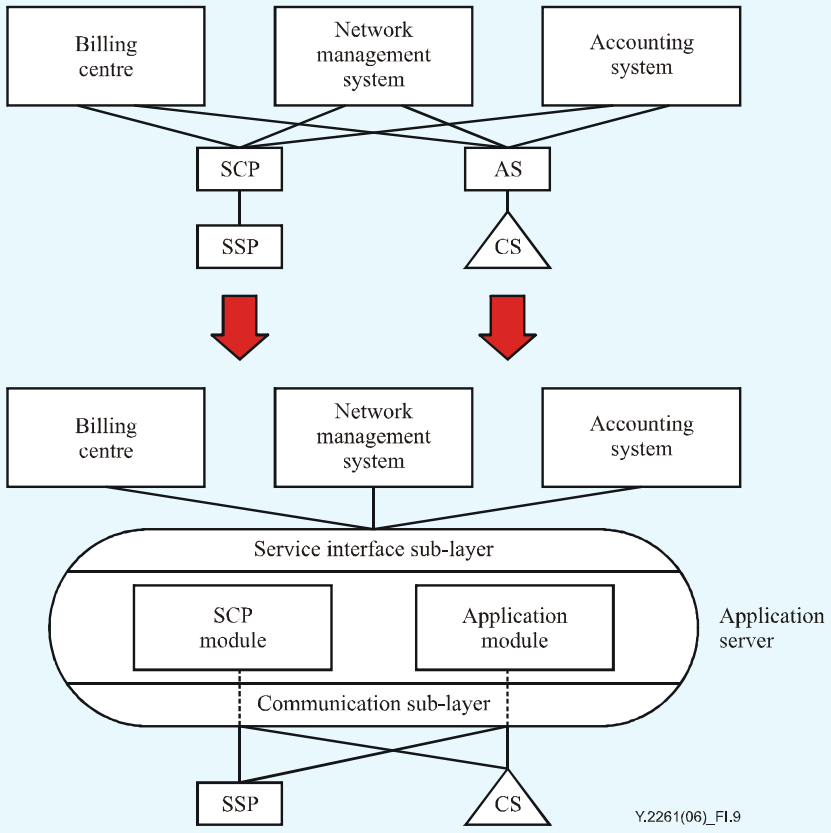
- Scenario 1: In this scenario, existing IN services are reused in NGN by implementing SSF in the CS. Both PSTN/ISDN and NGN exist.

Figure 4-1: Realization of scenario 1



- Scenario 2: In this scenario, the SCP is integrated to the application server. The communication sub-layer is a uniform communication layer which may provide connection between SSP, CS, SCP and the application server. The services created by the service creation environment (SCE) in the IN may be directly loaded into the SCP module of the AS. The SCP and the application module may be connected through a service interface sub-layer to operation and maintenance and external systems (e.g., billing centre, network management centre, accounting system).

Figure 4-2: The SCP is integrated to the application server as a whole

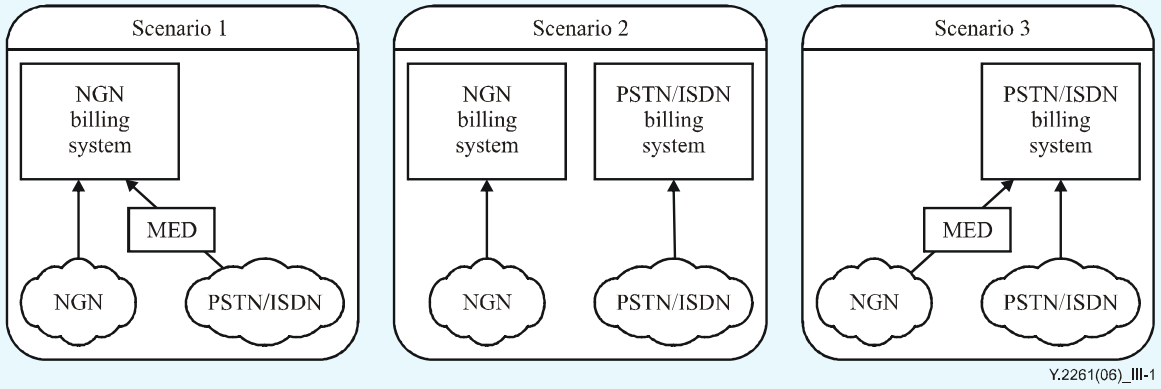


5 Billing system migration scenarios

The following three scenarios are considered when migration to NGN. The timing or preference for selection of these scenarios is service provider dependent. Mediation (MED) is an entity which allows transfer and processing of call detail records (CDRs) from the PSTN/ISDN to the NGN billing system, or from the NGN to the PSTN/ISDN billing system.

- Scenario 1: For this scenario, an NGN billing system is considered to handle both the PSTN/ISDN and the NGN. For this case, all accounting aspects are affected.
- Scenario 2: For this scenario, a new billing system is developed for the NGN, while keeping the existing PSTN/ISDN billing system. For this case, all accounting aspects are to be considered for NGN.
- Scenario 3: For this scenario, a legacy billing system is considered to handle both the PSTN/ISDN and the NGN. For this case, all accounting aspects are affected.

Figure 5-1: Billing system migration scenarios



Annex 8: NGN Issues

NGN should continuously evolve to build up "Connected World" providing more convenient ways to use services and application including to use of relevant network resources allowing from other providers such as 3rd party providers. Another important aspect is that NGN should support Ubiquitous Networking which will represent the situation of "Connect to Anything" in other words called IoT “Internet of Things”. For these, service platform aspects and capabilities to support ubiquitous networking of NGN have been seriously considered and developed during the last few years, especially in ITU-T NGN-GSI.

1 Service Integration and Delivery Environments in NGN

NGN-GSI in ITU-T studied on service platform aspects which should support multi-fold telecommunication business model and through this, NGN enhances NGN end-users access to applications. ITU-T Recommendation Y.2240 (approved at January 2011, formerly known as Y. NGN-SIDE) identifies service delivery platform called NGN-SIDE can be viewed as the next generation service delivery platform (SDP) and its framework can conceptually be applicable to other telecommunication environments (e.g. mobile networks).

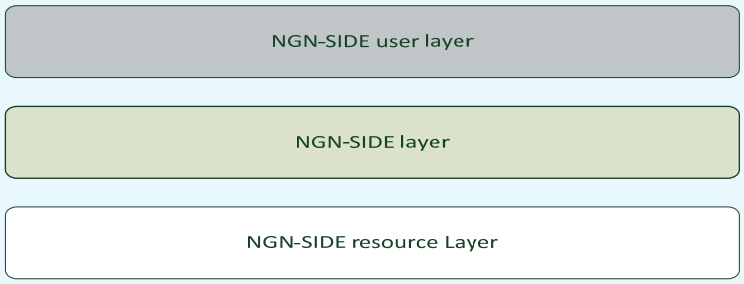
NGN-SIDE is defined as “an open environment in NGN integrating resources from different domains and delivering integrated services to applications over NGN.” Here, domains include, but are not limited to, telecommunication domain (e.g. fixed and mobile networks), Internet domain, Broadcasting domain and Content Provider domain.

The following main functionalities are supported in the NGN-SIDE ecosystem:

- integration of resources from different domains (e.g. telecommunication domain (fixed and mobile networks), broadcasting domain, internet domain or content provider domain) over NGN;
- adaptation, including abstraction and virtualization, of resources from different domains;
- resource brokering for mediation among applications and resources;
- support of application development environment for application developers;
- support of different service interfaces across ANI, UNI, SNI and NNI for exposure of NGN-SIDE capabilities and access to resources in different domains;
- provision of mechanisms for the support of diverse applications including cloud services, machine to machine, and ubiquitous sensor network applications;
- provision of mechanisms for the support of applications making usage of context based information;
- provision of mechanisms for content management.

NGN-SIDE has a layered architecture as shown in the following Figure 1-1:

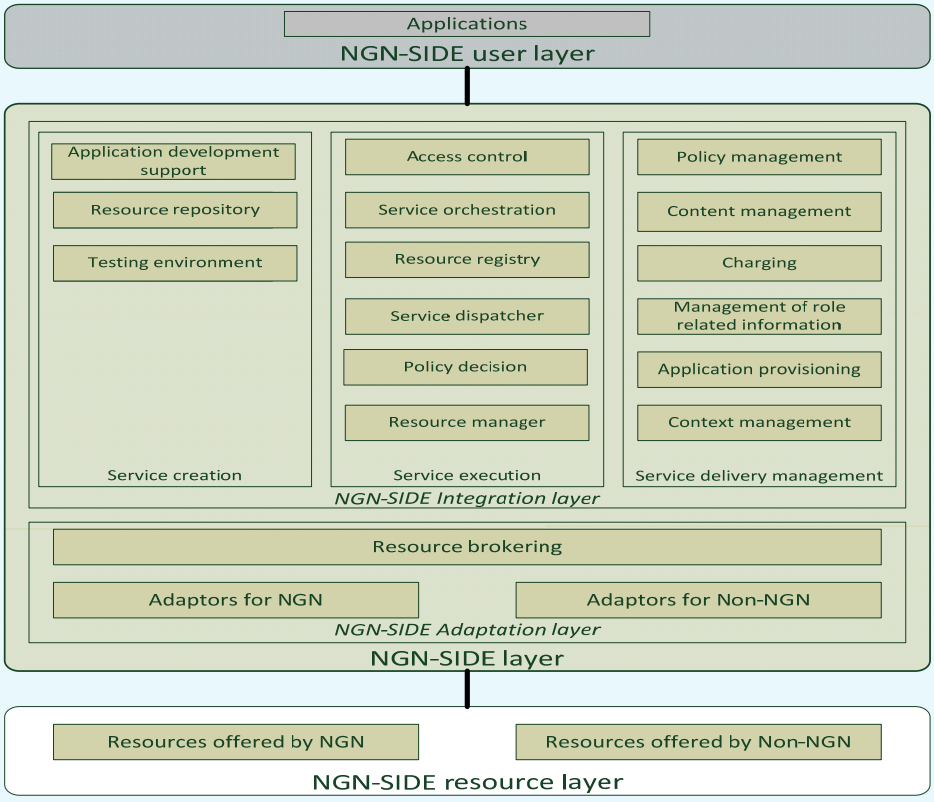
Figure 1-1: Layered View of NGN-SIDE



- The NGN-SIDE user layer uses the services offered by the NGN-SIDE layer, including resource exposure. It includes users accessing the NGN-SIDE, such as applications and other users.
- The NGN-SIDE layer corresponds to NGN-SIDE.
- The NGN-SIDE resource layer includes resources accessible by NGN-SIDE, such as applications, service enablers, network capabilities, connectivity, computing, storage, and content.

The following Figure 1-2 shows a functional view of NGN-SIDE according to the above described layers, the NGN-SIDE layer being comprised of the NGN-SIDE integration layer and the NGN-SIDE adaptation layer:

Figure 1-2: Functional View of NGN-SIDE



In order to reduce the complexity of integrating resources, the NGN-SIDE integration layer provides a unified way for the NGN-SIDE users to access the resources offered by NGN and Non-NGN. It supports the service creation functional group, the service execution functional group and the service delivery management functional group:

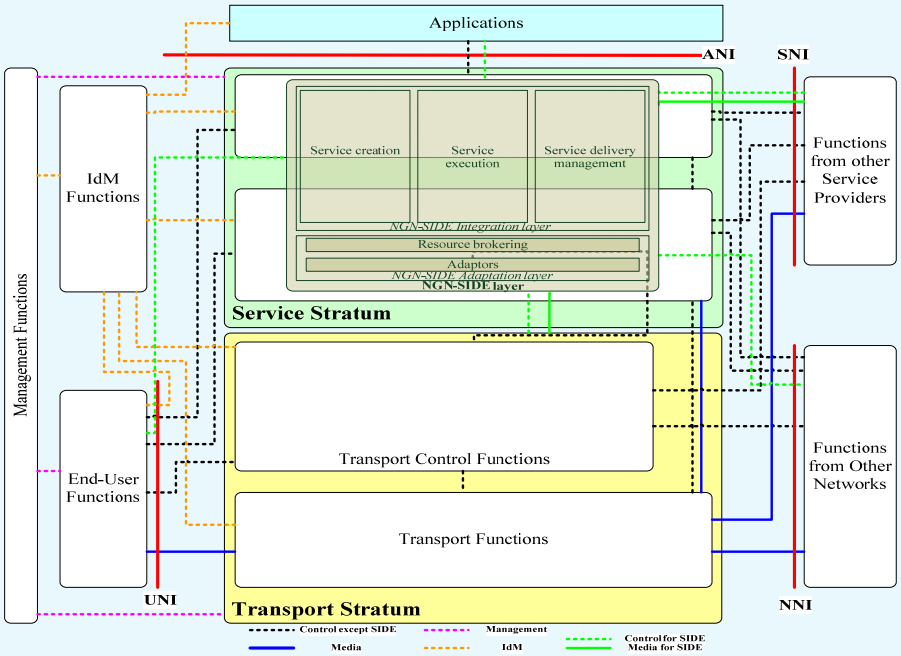
- the service creation functional group provides capabilities to realize an application development environment for application developers;
- the service execution functional group provides capabilities to support the service execution environment;
- the service delivery management functional group provides capabilities to realize the management of different aspects, provisioning of applications and charging for ensuring proper functioning of the service creation and service execution functional groups and providing associated delivery functionalities.

The NGN-SIDE adaptation layer adapts resources offered by NGN-SIDE resource providers such as their own service logic and service control, and related protocols, in order to provide uniformly adapted resources (e.g. control and media format) for interaction with the NGN-SIDE integration layer. NGN-SIDE resource providers use standardized or proprietary interfaces called "NGN-SIDE resource interfaces" to offer resources to NGN-SIDE and these interfaces are adapted by NGN-SIDE.

NGN-SIDE positioning within the NGN reference architecture is shown in the following Figure 1-3:

The NGN-SIDE functional components are positioned inside the NGN service stratum. The NGN-SIDE adaptation layer enables the abstraction of resources, including the resources of the NGN transport stratum (e.g. transport control functions and transport functions related resources) and the NGN service stratum (e.g. service control functions and content delivery functions related resources).

Figure 1-3: NGN-SIDE positioning within the NGN reference architecture



2 Open Service Environments in NGN

Another important aspect of NGN in the sense of services is that enabling new capabilities and supports a wide range of emerging services with advanced and complex functionalities for application providers such as 3rd party providers. In response to a drive from application providers and/or developers to develop new applications and capabilities accessible via standard interfaces, NGN providers should cooperate in the development of standard application network interfaces (ANI) including software reusability and portability. An open service environment (OSE) within NGN aims to provide efficient and flexible capabilities based on the use of standard interfaces to NGN applications thereby enabling applications to take full advantage of the NGN capabilities. Two ITU-T Recommendations address this OSE as follows:

- ITU-T Recommendation Y.2234 (approved at 2008): defines the requirements that are divided into service requirements and functional requirements.
- ITU-T Recommendation Y.2020 (2011): defines the OSE architecture for NGN based on ITU-T Y.2234 and ITU-T Y.2201.

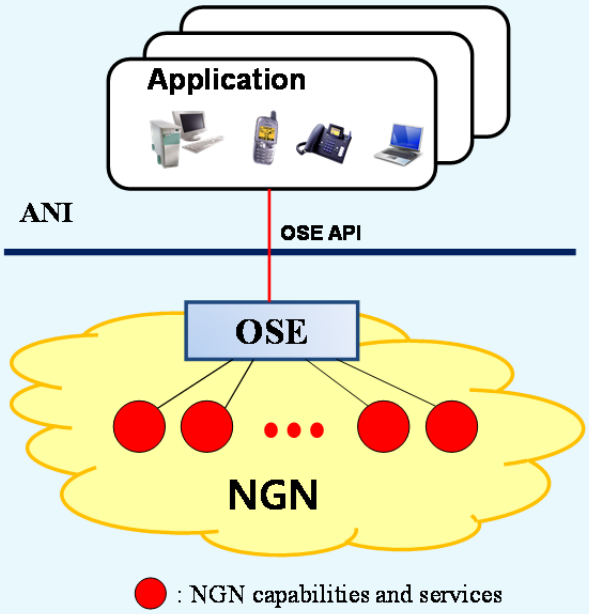
Open service environment provides capabilities to enable flexible and agile service creation, execution and management based on the use of standards interfaces. The use of standard interfaces will ensure NGN OSE based service reusability and portability across networks, as well as accessibility by application providers and/or developers.

OSE capabilities have the following characteristics:

- Flexible development of applications and capabilities by NGN providers, application providers, and other service providers;
- Exposure of capabilities via standard application network interfaces (ANI);
- Portability and re-usability of capabilities across networks (and from other network to NGN or from NGN to other network);
- Leveraging new capabilities enabled by technologies from non-NGN environments

The OSE allows applications to make use of NGN capabilities and/or services offered through the application network interface (ANI) as shown in Figure 2-1. Application providers and/or developers will be able to create and provide new applications via standard interfaces at the ANI as shown OSE API regardless of the type of underlying network and/or equipment.

Figure 2-1: Open service environment capabilities in NGN



Service requirements of NGN-OSE capabilities are defined as followings:

- Provide standard APIs for application providers and/or developers to create and introduce applications quickly and seamlessly;
- Provide the service level interoperability among different networks, operating systems and programming languages (e.g. Web Services are an example of enabling technology for providing service level interoperability);
- Support service independence from NGN provider and manufacturers [ITU-T Y.2201]:
- Support OSE capabilities based on NGN providers' capabilities. However, OSE capabilities based on application providers' capabilities are not supported in this version of the document;
- Support location, network and protocol transparency [ITU-T Y.2201]:
- Provide capabilities for coordinating services among themselves and services with applications;
- Support service discovery capabilities to allow users and their devices to discover the services, applications, and other network information and resources of their interest [ITU-T Y.2201]. In addition, discovery mechanisms for services or components of multiple application providers are recommended to be provided;
- Provide the means to manage the registration of capabilities, services and applications. The technology choice is required to ensure functions for service registration and deregistration, including configuration, activation, publication [ITU-T Y.2201];
- Provide the service management capabilities such as service tracking, update management, auditing, version control, logging, e.g. provide a record of the history of services, access control management, statistical analysis of service registration and utilization.
- Support NGN services reuse by providing service composition capability;
- Support of a service composition language;

- Offer a development support environment which supports construction, trialing, deployment, and removal of applications [ITU-T Y.2201];
- Allow interworking with service creation environments and network entities for creation and provisioning of applications and services [ITU-T Y.2201];
- Provide a secure access to the NGN capabilities in alignment with the general NGN security requirements as specified in clause 5.13 of [ITU-T Y.2201];
- Support policy enforcement capability for resources protection and management, and service personalization.

The functions to support of the NGN-OSE are consisted with service coordination, service discovery, service registration, service management, service composition, service development support, interworking with service creation environments and policy enforcement. In each function has more detail requirements as following:

The NGN service coordination functions are required to:

- Provide coordination of applications and services with capabilities;
- Provide the tracking of NGN capabilities or service components from various application providers, and the relationship between these capabilities or service components;
- Support the information on state change of capabilities or service components for applications and services.

The NGN service discovery functions are required to:

- Provide service discovery for physically distributed NGN services;
- Support a variety of discovering criteria (e.g. specific field based discovery, classification system based discovery). An example of discovering criteria is implemented in the Universal Discovery, Description and Integration (UDDI) specification of Web Services framework;
- Use user and device profile information for discovering the proper service;
- Allow users to discover user-interest services, device-interest services and network information;
- Support a variety of scoping criteria (e.g. location and cost) to provide appropriate scaling, with appropriate mechanisms to ensure security and privacy (This allows support of customized discovery for a wide range of scenarios.);
- Use a variety of approaches for discovering services such as client-server, P2P, combination of client-server and P2P;
- Support appropriate mechanisms to ensure security and privacy;
- Take into account scalability (e.g. broadcast mechanisms are recommended to be avoided).

The NGN service registration functions are required to:

- Provide service registration, including configuration, activation, publication and service deregistration;
- Provide a variety of service registration features (e.g. manual, autonomous) for NGN services;
- Support a variety of registration parameters, including mandatory and optional parameters.

The NGN service registration functions may support:

- Registration services in centralized and de-centralized ways;
- Multiple concurrent service registrations.

The NGN service management functions are required to:

- Provide a monitoring function of registered services for availability and predicted response time. NGN services and user applications might need to use monitoring information for the availability or predicted response time of target services before executing services;
- Provide managing functions of QoS information about registered NGN services such as accessibility, performance, integrity, reliability, etc.;
- Provide a version management function to NGN services for interoperability;
- Provide notification service functions for updated services;
- Provide failure detection and recovering functions for unexpected failures;
- Provide service tracking management functions to capture and log all relevant information for each component within a service chain. Service tracking is recommended to allow for an association among the captured data associated with a specific service. Service tracking is required to enable tracking of capabilities or components of multiple third parties, and the relationships between these capabilities or components;
- Provide a service substitution function that considers various kinds of factors to users. It is required to provide mechanisms to capture a set of information including terminal capability, network situation, user preference and substitution policy; and judge whether to substitute the service or not based on the captured information. If there is a need to substitute the service, this function will substitute it;
- Provide service access control functions to control the accessibility of a specific service by applications. (The service access control function provides the necessary authentication and authorization actions required to ensure that the application has appropriate access rights for the requested service.);
- Provide statistical analysis functions to analyze service registration and utilization information (e.g. number of registered services, utilization frequency of registered services, and number of applications using registered services.);
- Provide an auditing function to review the overall operations of open service environment capabilities during a specific period required by the auditor.

The NGN service composition functions are required to:

- Provide a composition language that describes the interaction among services. Additionally, the composition language is recommended to support expression capabilities for describing the composition logic among services;
- Support the composition of services statically or dynamically (i.e. for the static type, the services are composed during service design; while for the dynamic type, the services are composed during service runtime).

The NGN service development support functions are required to:

- Support services re-use and allow for services interchangeability;
- Support mixing-and-matching of services by management of interfaces and consistent semantics of shared data/schema across these services
- Support the full life cycle of services, ranging from installation, configuration, administration, publishing, versioning, maintenance and removal;
- Support delivery-agnostic application designs to allow applications to be implemented without requiring re-design for each subsequent development scenario;
- Support tracking of dependencies among services.

The NGN service creation environment interworking functions are required to:

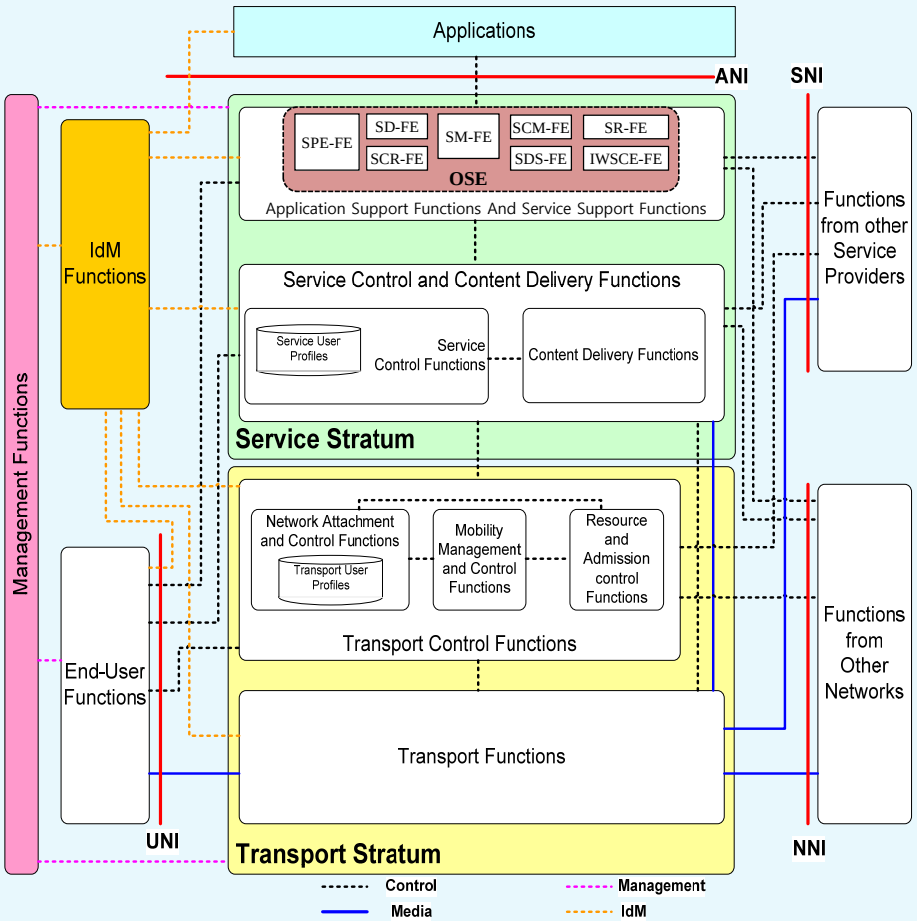
- Support the following three classes of service creation environments

The NGN policy enforcement functions are required to:

- Provide a description language to express various kinds of policy rules such as those related to authorization, charging, service level agreement and logging. This language is recommended to support policy re-use;
- Provide a policy execution framework to interpret and execute the policies;
- Protect services from unauthorized users' requests and manage requests based on the policy rules;
- Support the selection of appropriate services for service composition to respond to the needs and preferences of a user or a group of users.

Figure 2-2 shows the extended NGN architecture overview [ITU-T Y.2012] in order to illustrate the positioning of the OSE functional group.

Figure 2-11: OSE positioning in the NGN architecture



3 Next Generation Ubiquitous Networking (NGUN)

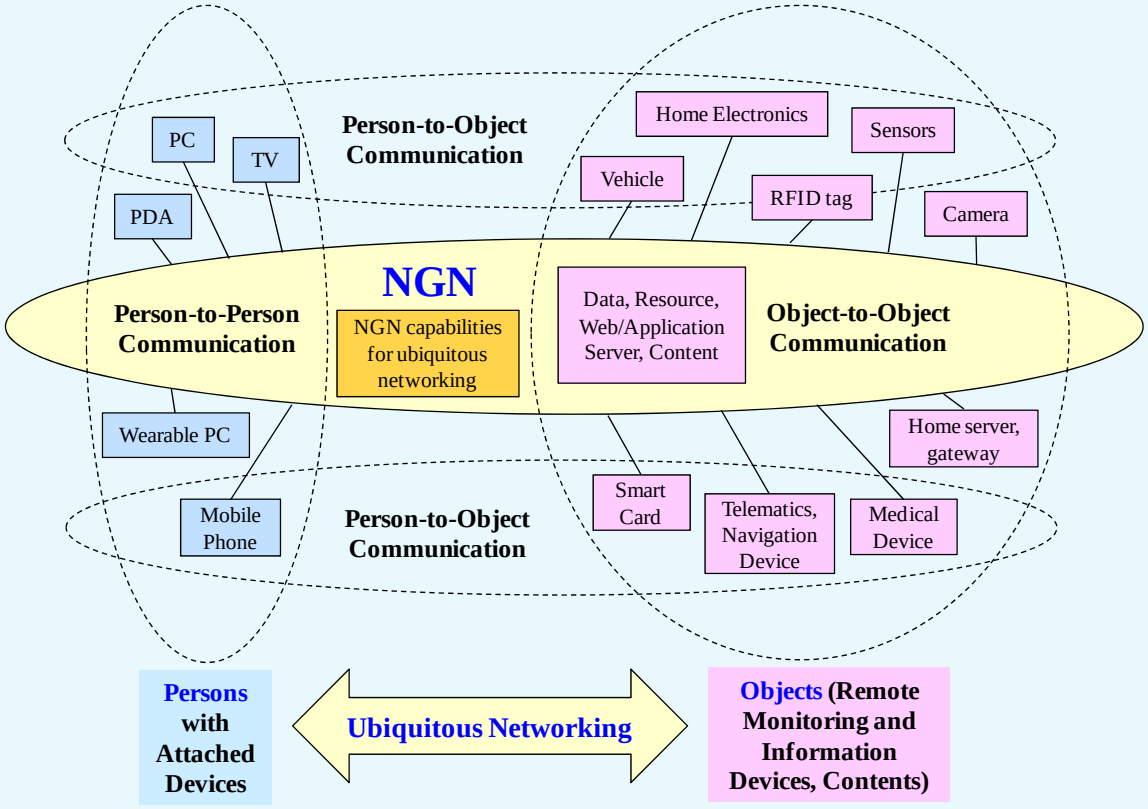
To realize the vision of "Connect to Anything" or in other words IoT “Internet of Things”, networks should have capabilities of Ubiquitous Networking. It is not easy to define of “Ubiquitous Networking” because of the conceptual features of “Ubiquitous” or “Ubiquity”. ITU-T developed a recommendation to specify the “Ubiquitous” features as a networking capability of NGN. The ITU-T Recommendation Y.2002 (10/2009) specifies “Next Generation Ubiquitous Networking” as a part of NGN recommendations.

In this recommendation, “Ubiquitous Networking” identifies as “The ability for persons and/or devices to access services and communicate while minimizing technical restrictions regarding where, when and how these services are accessed, in the context of the service(s) subscribed to”. Based on this definition, this recommendation identifies fundamental characteristics of ubiquitous networking as followings:

- IP connectivity: IP connectivity will allow objects involved in ubiquitous networking to communicate with each other within a network and/or when objects have to be reachable from outside their network. Particularly, as many new types of objects will be connected to networks, IPv6 will play a key role in object-to-object communications
- Personalization: Personalization will allow to meet the user’s needs and to improve the user’s service experience since delivering appropriate contents and services to the user. User satisfaction is motivated by the recognition that a user has needs, and meeting them successfully is likely to lead to a satisfying client-customer relationship and re-use of the services offered
- Intelligence: Intelligence which enables network capabilities to provide user-centric and context-aware service is essential to meet numerous network requirements in terms of data handing and processing capabilities. Introduction of artificial intelligence techniques in networks will help to accelerate the synergies and ultimately the “fusion” between the involved industries
- Tagging objects: Tag-based solutions on ubiquitous environment will allow to get and retrieve information of objects from anywhere through the network. Radio frequency identifier (RFID) is one of tag-based solutions for enabling real-time identification and tracking of objects. As active tags have networking capabilities, a large number of tags will need network addresses for communications. As IP technology will be used for ubiquitous networking, it is essential to develop mapping solutions between tag-based objects (e.g. RFIDs) and IP addresses
- Smart devices: Smart devices attached to networks can support multiple functions including camera, video recorder, phone, TV, music player. Sensor devices which enable detection of environmental status and sensory information can utilize networking functionalities to enable interconnection between very small devices, so-called ‘smart dusts’. Specific environments such as homes, vehicles, buildings will also require adaptive smart devices

Figure 3-1 illustrates the different types of communications for ubiquitous networking.

Figure 3-1: Ubiquitous networking communication types



Note: objects include all of things which are attached in the network. Some objects can be attached with persons and others can be located remotely with persons. "person-to-person" communication relies on a "object-to-object" communication.

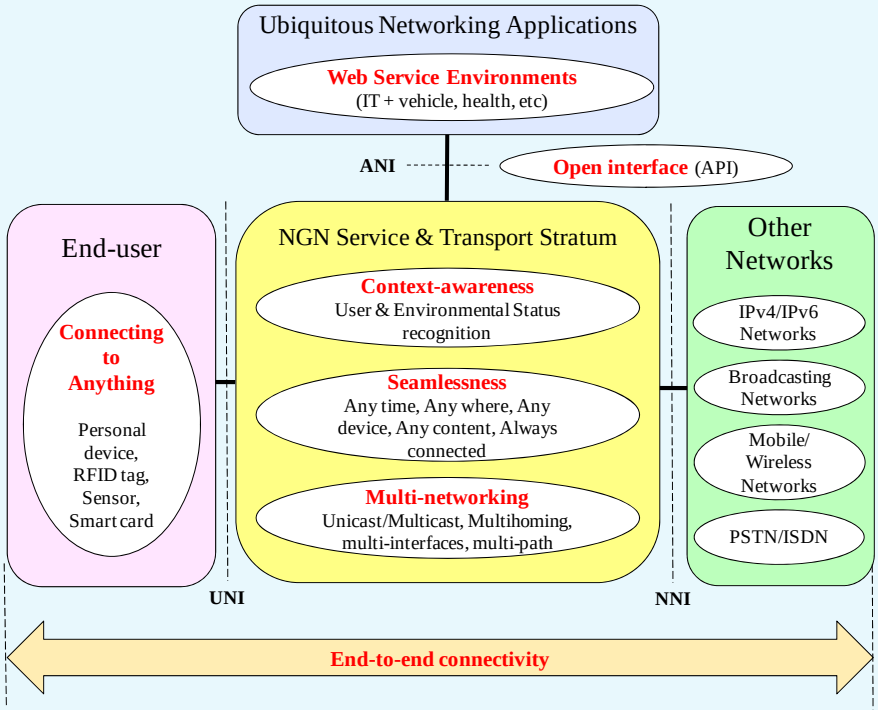
Figure 3-1 makes a distinction between the following users of ubiquitous networking: persons (using attached devices such as PC, PDA, mobile phones) and objects (such as remote monitoring and information devices, contents) and shows three different types of communications:

- Person-to-Person Communication: persons communicate with each other using attached devices (e.g. mobile phone, PC);
- Person-to-Object Communication: persons communicate with a device in order to get specific information (e.g., IPTV content, file transfer);
- Object-to-Object Communication: an object delivers information (e.g. sensor related information) to another object with or without involvement of persons.

Ubiquitous networking aims to provide seamless communications between persons, between objects as well as between persons and objects while they move from one location to another.

Figure 3-2 shows the high-level architectural model for ubiquitous networking in NGN. This model is based upon the NGN overall architecture as described in [ITU-T Y.2012] showing the necessary capabilities to support of ubiquitous networking.

Figure 3-2: High-level architectural model for ubiquitous networking in NGN



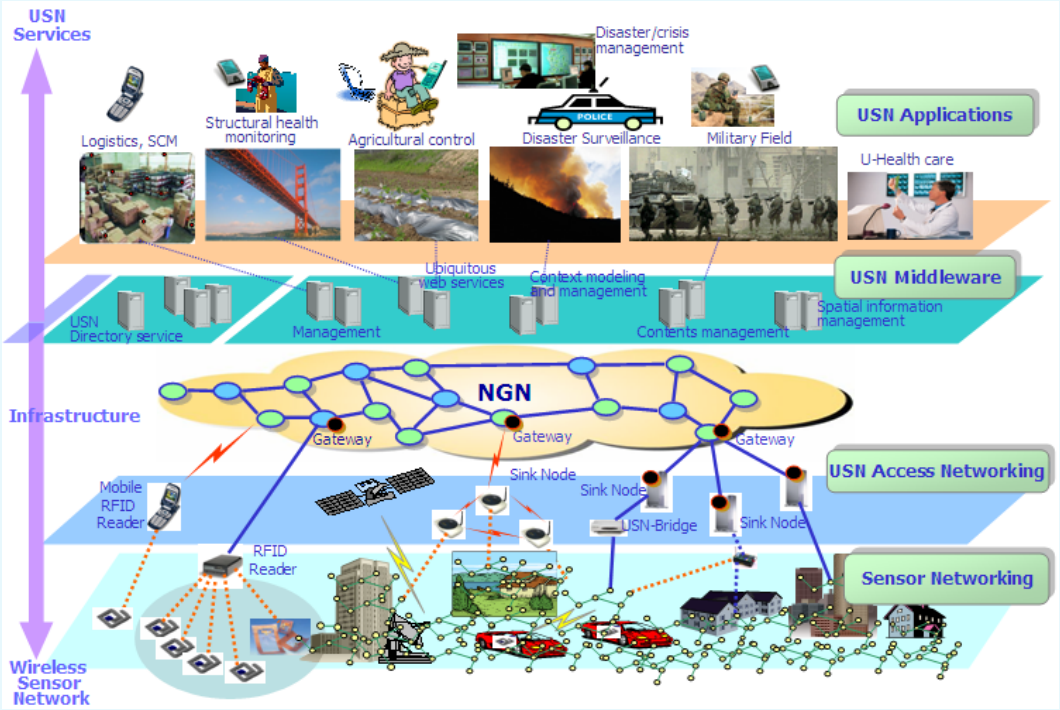
4 Ubiquitous Sensor Networks (USN)

The technology using sensors has huge potential as it could generate applications in a wide range of fields, including ensuring safety and security, environmental monitoring, promoting personal productivity and enhancing national competitiveness. The term of "Ubiquitous Sensor Networks" (USN) is used to describe a network which is configured with sensors that could provide ubiquitous connectivity.

ITU-T Recommendation Y.2221 provides a description and general characteristics of USN and their applications and services. This recommendation also analyzes service requirements of USN applications and services, and specifies extended or new NGN capability requirements based on the service requirements. The main components of a USN, as described in Figure 4-1 are:

- Sensor Networking: Comprising sensors which are used for collecting and transmitting information about their surrounding environment and an independent power source (e.g., battery, solar power);
- USN Access Networking: Intermediary collection of information from a group of sensors through "sink nodes" and facilitating communication with a control centre or with external entities;
- Network Infrastructure: Next Generation Network (NGN);
- USN Middleware: Software for the collection and processing of large volumes of data;
- USN Applications Platform: A technology platform to enable the effective use of a USN in a particular industrial sector or application.

Figure 4-1: Schematic Layers of a Ubiquitous Sensor Network



Sensor is a device that captures a physical stimulus such as temperature, sound, light, pressure, heat, vibration, or magnetism. Sensor data has to be transmitted to users for data processing and corresponding reactions.

Sensor networks can be established by wire-line or wireless. Typical wire-line networking techniques are RS-232, RS-422, RS-485, Power Line Communication, etc. A variety of wireless networking techniques has been used. But nowadays standardized ways have emerged as hot topics and a new term, WSN (Wireless Sensor Network), was made for technology and business marketing. Typical wireless PHY/MAC networking solutions are IEEE 802.15.4, IEEE 802.15.3, Bluetooth, etc. Multi-hop networking solutions over these wireless networks are ZigBee, 6LoWPAN, etc.

5 Cloud Computing

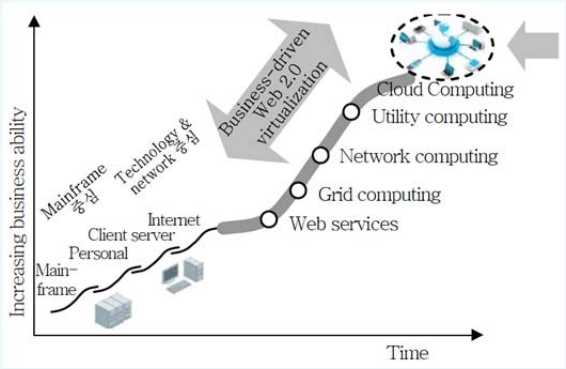
5.1 Background and definition of Cloud Computing

The background history about the cloud computing may back to the dates when mainframe became available in academia and corporations, accessible via dumb terminals which were used for communications but had no internal computational capacities. Thus it had been required to share main-frame with multiple users by multiple terminals in terms of physical access to the computer as well as to share the CPU time such as time-sharing. In the 1990s, telecommunications with offering virtual private network (VPN) services with comparable quality of service, but at a lower cost, it began to use the cloud symbol to denote the demarcation point between providers including users. Cloud computing extends this boundary to cover servers as well as the network infrastructure. Following Figure 5-1 shows brief summary of such history about cloud computing developments.

According to the developments of computing capabilities, users such as scientists and technologists explored ways to make large-scale computing power available to more users over time sharing, optimal

use of the infrastructure, platform and prioritized access to the CPU. In addition, the ubiquitous availability of networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, autonomic, and utility computing have led to growth of cloud computing.

Figure 5-1: History of computing



Cloud computing is defined as a model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or resource pooling provider interaction. Cloud computing enables cloud services which identified as a service that is delivered and consumed on demand at any time, through any access network, using any connected devices using cloud computing technologies. It is considered from a telecommunication perspective that users are not buying resources but cloud services that are enabled by cloud computing environments.

The cloud computing model promotes availability and is composed of six essential characteristics, five cloud service categories and four deployment models as followings:

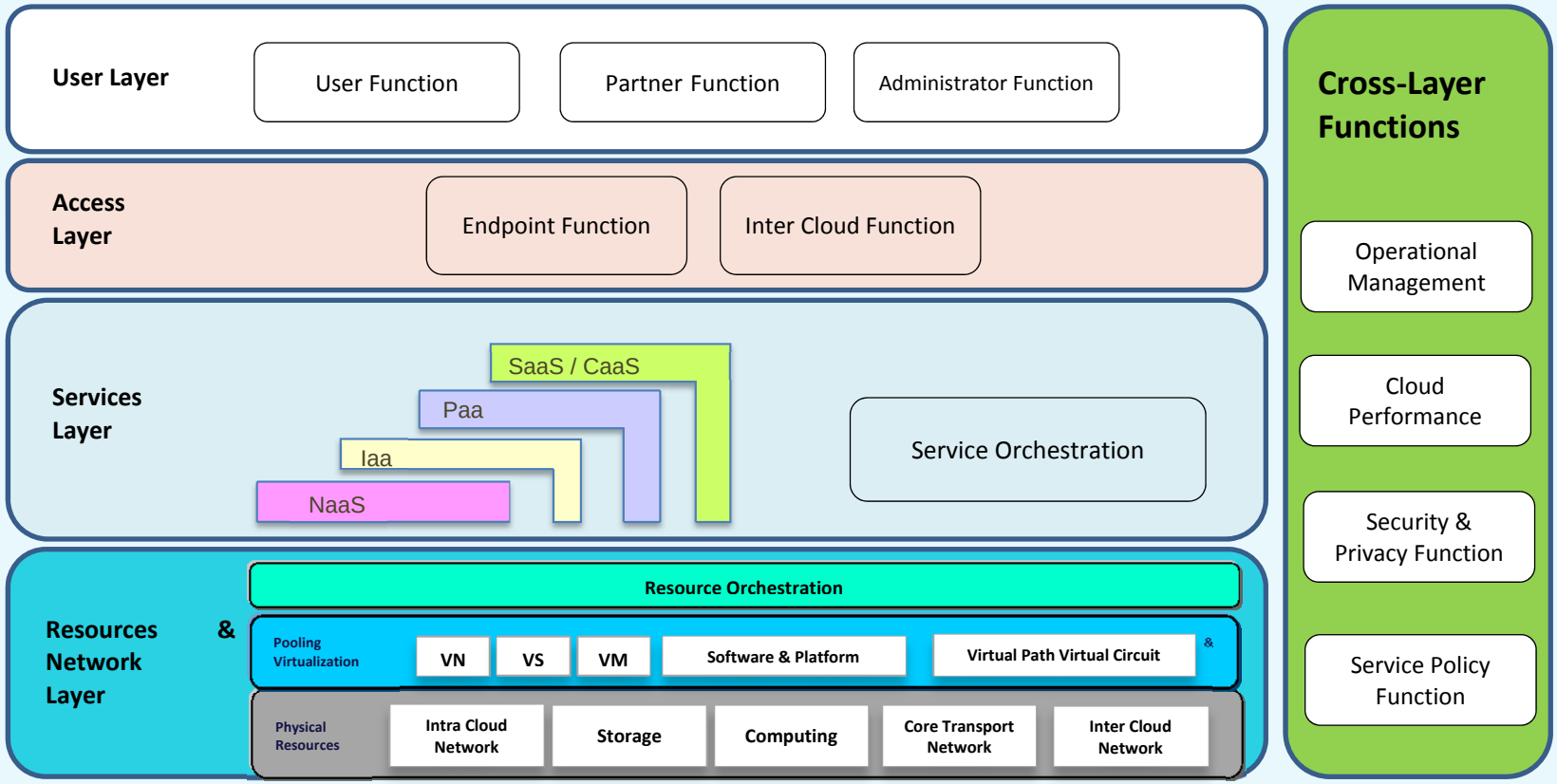
- On-demand self-service: A cloud service user can unilaterally provision computing capabilities, such as server time, network storage and communication and collaboration services, as needed automatically without requiring human interaction with each service's cloud service provider.
- Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- Resource pooling: The cloud service provider's computing resources are pooled to serve multiple users or organisations using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to user demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify the location at a higher level of abstraction (e.g., country, state, data center). Examples of resources include storage (typically on hard or optical disc drives), processing, memory (typically on DRAM), network bandwidth, and virtual machines.

- Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the cloud service user, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- Measured Service: Cloud systems automatically control and optimize resource use (e.g., storage, processing and bandwidth) by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., the number of active user accounts). Resource usage can be monitored, controlled, and reported. It provides transparency for both cloud service provider and cloud service users.
- Multi-tenancy: A characteristic of cloud in which resources are shared amongst multiple cloud tenants. Tenant is intended here as any Cloud Service User (CSU) workload that has unique requirements and/or a unique operating agreement with the Cloud Service Provider (CSP). There is an expectation on the part of the cloud tenant that its use of the cloud is isolated from other tenants' use in the same share resource pool; that tenants in the cloud are restricted from accessing or affecting another tenant's assets; that the cloud tenant has the perception of exclusive use of, and access to, any provisioned resource. The means by which such isolation is achieved vary in accordance with the nature of the shared resource, and can affect security, privacy and performance.

5.2 Architecture model

Figure 5-1 shows a functional architecture model of cloud computing. These functional layers in the architecture are derived by grouping cloud related functions.

Figure 5-1: Functional Architecture Model of Cloud Computing



- User Layer: performs interaction between the cloud service user and the underlying cloud architecture layers. The User Layer is used to setup secure mechanism with cloud computing, send cloud service requests to cloud and receive cloud services from cloud, perform cloud service access, administrate and monitor cloud services;
- Access Layer: provides a common interface for both manual and automated cloud service capabilities and service consumption;
- Services Layer: the cloud service provider orchestrates and exposes services of the five cloud service categories. The Cloud Services Layer manages the cloud components required for providing the services, runs the software that implements the services and arranges to offer the cloud services to the cloud service user;
- Resources & Network Layer: The Resources and Network layer is where the physical resources reside including equipment typically used in a data centre such as servers, networking switches and routers, storage, etc, and the corresponding non-cloud-specific software that runs on the servers and other computers such as host operating systems, hyper-visors, device drivers, generic systems management software, etc;
- Cross-Layer Functions: perform overall system management (i.e., operations, administration, maintenance and provisioning (OAM&P)) and monitoring, and provide secure mechanisms.

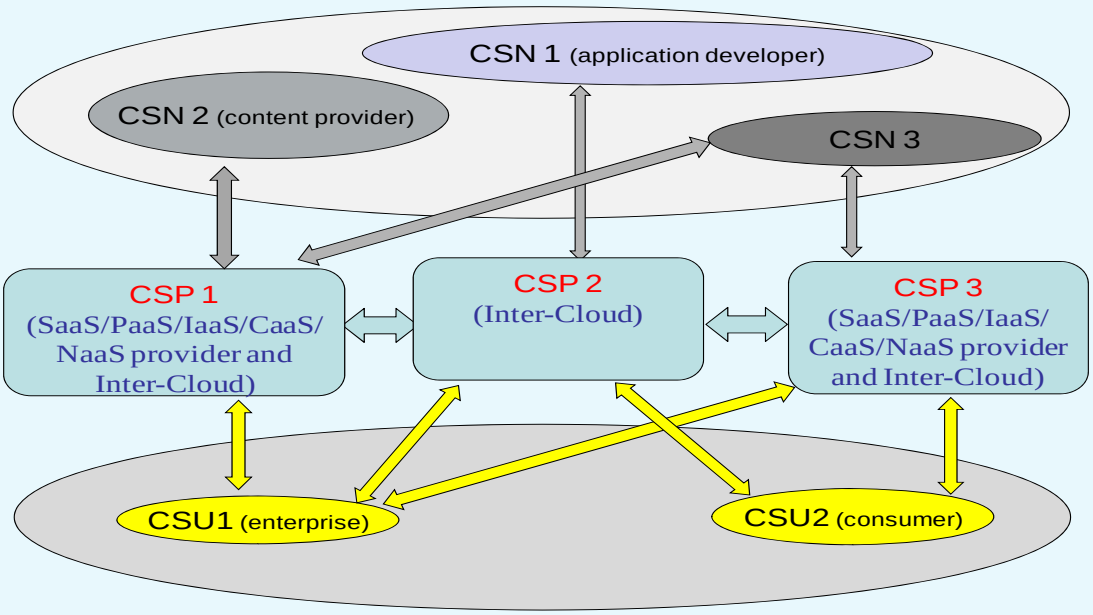
5.3 Cloud Computing Eco-systems

A cloud computing business ecosystem (cloud ecosystem) is a business ecosystem of interacting organizations and individuals - the actors of the cloud ecosystem - providing and consuming cloud services. The following actors are identified in a cloud ecosystem:

- Cloud service users (CSU): A person or organization that consumes delivered cloud services;
- Cloud service providers (CSP): An organization that provides and maintains cloud services to be delivered and consumed;
- Cloud service partners (CSN): A person or organization that provides support to the building of the service offer of a cloud service provider (e.g. service integration).

Figure 5-2 depicts the actors with some of their possible roles in a cloud ecosystem.

Figure 5-2: Actors with possible roles in a cloud ecosystem



5.4 Cloud Service categories

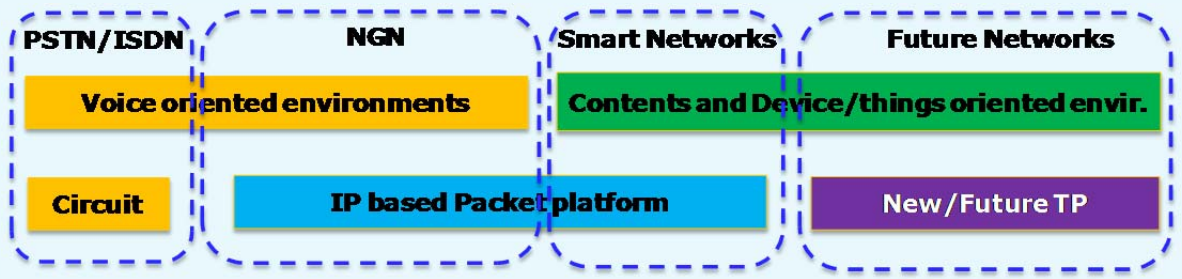
One of the key features of the cloud computing is “Anything as a Service” so called “XaaS”. There are plenty of candidate issues to be part of “as a Service”, but at this stage, ITU-T, especially SG13 is being discussed about following five services as key service categories.

- Cloud Software as a Service (SaaS): A category of cloud services where the capability provided to the cloud service user is to use the cloud service provider’s applications running on a cloud resources;
- Communications as a Service (CaaS): A category of cloud services where the capability provided to the cloud service user is to use real time communication and collaboration services. NOTE - Communication and collaboration services include voice over IP, instant messaging, video conferencing, for different user devices;
- Cloud Platform as a Service (PaaS): A category of cloud services where the capability provided to the cloud service user is to deploy user-created or acquired applications onto the cloud resources using platform tools supported by the cloud service provider;
- Cloud Infrastructure as a Service (IaaS): A category of cloud services where the capability provided by the cloud service provider to the cloud service user is to provision processing, storage, intra-cloud network connectivity services (e.g. VLAN, firewall, load balancer, application acceleration), and other fundamental computing resources of the cloud resources where the cloud service user is able to deploy and run arbitrary application;
- Network as a Service (NaaS): A category of cloud services where the capability provided to the cloud service user is to use transport connectivity services and/or inter-cloud network connectivity services.

6 Future study direction of NGN

Considering this, ITU-T based on the NGN-GSI is continuing of their developments for the NGN will play a crucial role in a future environment as well. For this, as shown in Figure 6-1, ITU-T NGN GSI will continue their study covering various technical subjects. Recently one of the important subjects is providing smart and intelligent capabilities into the NGN as well as its beyond. This issue has been raised mainly from network providers considering the difficulties to provide better services to meet end user's requirements taking into account the status of network resources. Under this subject, NGN-GSI is now develop various solutions and mechanisms to resolve "smart usage of network resources" and "being pipeline of networks" This study will contribute in the development of called "Future Networks" which is being developed as a new paradigm of networks (for example, could be not use of IP).

Figure 6-1: Future study direction of NGN



Annex 9: ITU NGN standards

Internet Protocol Aspects

1 General aspect of IP based networks

Y.1001: IP framework – A framework for convergence of telecommunications network and IP network technologies

2 Architecture, access, network capabilities and resource management

Y.1221: Traffic control and congestion control in IP-based networks

Y.1222: Traffic control and congestion control in Ethernet-based networks

Y.1223: Interworking guidelines for transporting assured IP flows

Y.1231: IP Access Network Architecture

Y.1241: Support of IP-based services using IP transfer capabilities

Y.1242/G.769: Circuit multiplication equipment optimized for IP-based networks

Y.1251: General architectural model for interworking

Y.1261: Service requirements and architecture for voice services over Multi-Protocol Label Switching

Y.1271: Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks

Y.1281: Mobile IP services over MPLS

Y.1291: An architectural framework for support of Quality of Service in packet networks

Y.1292: Customizable IP networks (CIP): Framework for the requirements and capabilities related to the customization of IP service networks by customers

3 Transport

Y.1310: Transport of IP over ATM in public networks

Y.1311: Network-based VPNs – Generic architecture and service requirements

Y.1311.1: Network-based IP VPN over MPLS architecture

Y.1321/X.85: IP over SDH using LAPS

Y.1370/G.8110: MPLS layer network architecture

Y.1370.1/G.8110.1: Architecture of Transport MPLS (T-MPLS) layer network

Y.1371/G.8112: Interfaces for the Transport MPLS (T-MPLS) hierarchy

Y.1374/G.8151: Management aspects of the T-MPLS network element

Y.1381/G.8121: Characteristics of Transport MPLS equipment functional blocks

Y.1382/G.8131: Linear protection switching for transport MPLS (T-MPLS) networks

4 Interworking

Y.1401: Principles of interworking

Y.1402/X.371: General arrangements for interworking between Public Data Networks and the Internet

Y.1411: ATM-MPLS network interworking – Cell mode user plane interworking

Y.1412: ATM-MPLS network interworking – Frame mode user plane interworking

Y.1413: TDM-MPLS network interworking – User plane interworking

Y.1414: Voice services – MPLS network interworking

Y.1452: Voice trunking over IP networks

Y.1453: TDM-IP interworking – User plane interworking

Y.1454: Tandem free operation (TFO) – IP network interworking – User plane interworking

5 QoS and Network Performance

Y.1501/G.820/I.351: Relationships among ISDN, IP-based network and physical layer performance Recommendations

Y.1530: Call processing performance for voice service in hybrid IP networks

Y.1531: SIP-based call processing performance

Y.1540: Internet protocol data communication service – IP packet transfer and availability performance parameters

Y.1541: Network performance objectives for IP-based services

Y.1542: Framework for achieving end-to-end IP performance objectives

Y.1543: Measurements in IP networks for inter-domain performance assessment

Y.1544: Multicast IP performance parameters

Y.1560: Parameters for TCP connection performance in the presence of middleboxes

Y.1561: Performance and availability parameters for MPLS networks

6 Operation, administration and maintenance

Y.1704/G.7713: Distributed call and connection management (DCM)

Y.1704.1/G.7713.1: Distributed Call and Connection Management (DCM) based on PNNI

Y.1704.2/G.7713.2: Distributed Call and Connection Management: Signalling mechanism using GMPLS RSVP-TE

Y.1704.3/G.7713.3: Distributed Call and Connection Management: Signalling mechanism using GMPLS CR-LDP

Y.1710: Requirements for Operation & Maintenance functionality in MPLS networks

Y.1711: Operation & Maintenance mechanism for MPLS networks

Y.1712: OAM functionality for ATM-MPLS interworking

Y.1713: Misbranching detection for MPLS networks

Y.1714: MPLS management and OAM framework

Y.1720: Protection switching for MPLS networks

7 IPTV

Y.1901: Requirements for the support of IPTV services

Y.1902: Framework for multicast-based IPTV content delivery

Y.1910: IPTV functional architecture

Y.1911: IPTV services and nomadism: Scenarios and functional architecture for unicast delivery

Y.1991: Terms and definitions for IPTV

Next Generation Networks

1 Frameworks and functional architecture models

Y.2001: General overview of NGN

Y.2002: Overview of ubiquitous networking and of its support in NGN

Y.2006: Description of capability set 1 of NGN release 1

Y.2007: NGN capability set 2

Y.2011: General principles and general reference model for Next Generation Networks

Y.2012: Functional requirements and architecture of next generation networks

Y.2013: Converged services framework functional requirements and architecture

Y.2014: Network attachment control functions in next generation networks

Y.2015: General requirements for ID/locator separation in NGN

Y.2016: Functional requirements and architecture of the NGN for applications and services using tag-based identification

Y.2017: Multicast functions in next generation networks

Y.2018: Mobility management and control framework and architecture within the NGN transport stratum

Y.2019: Content delivery functional architecture in NGN

Y.2020: Open service environment functional architecture for next generation networks

Y.2021: IMS for Next Generation Networks

Y.2022: Functional architecture for the support of host-based ID/locator separation in NGN

Y.2023: Functional requirements and architecture for the NGN for multimedia communication centre serviceY.2031: PSTN/ISDN emulation architecture

Y.2051: General overview of IPv6-based NGN

Y.2052: Framework of multi-homing in IPv6-based NGN

Y.2053: Functional requirements for IPv6 migration in NGN

Y.2054: Framework to support signalling for IPv6-based NGN

Y.2055: Framework of object mapping using IPv6 in next generation networks

Y.2056: Framework of vertical multi-homing in IPv6-based NGN

Y.2057: Framework of node identifier and routing locator separation in IPv6-based next generation networks

Y.2058: Roadmap for IPv6 migration from the perspective of the operators of next generation networks

Y.2062: Framework of object-to-object communication for ubiquitous networking in NGN

Y.2091: Terms and definitions for next generation networks

2 Quality of Service and performance

Y.2111: Resource and admission control functions in next generation networks

Y.2112: A QoS control architecture for Ethernet-based IP access networks

Y.2113: Ethernet QoS control for next generation networks

Y.2121: Requirements for the support of flow-state-aware transport technology in NGN

Y.2122: Flow aggregate information exchange functions in NGN

Y.2171: Admission control priority levels in Next Generation Networks

Y.2172: Service restoration priority levels in Next Generation Networks

Y.2173: Management of performance measurement for NGN

Y.2174: Distributed RACF architecture for MPLS networks

Y.2175: Centralized RACF architecture for MPLS core networks

3 Service aspects

Y.2201: Requirements and capabilities for ITU-T NGN

Y.2205: Next Generation Networks – Emergency telecommunications – Technical considerations

Y.2206: Requirements for distributed service networking capabilities

Y.2211: IMS-based real-time conversational multimedia services over NGN

Y.2212: Requirements of managed delivery services

Y.2213: NGN service requirements and capabilities for network aspects of applications and services using tag-based identification

Y.2214: Service requirements and functional models for customized multimedia ring services

Y.2215: Requirements and framework for the support of VPN services in NGN, including the mobile environment

Y.2216: NGN capability requirements to support the multimedia communication centre service

Y.2221: Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment

Y.2232: NGN convergence service model and scenario using web services

Y.2233: Requirements and framework allowing accounting and charging capabilities in NGN

Y.2234: Open service environment capabilities for NGN

Y.2235: Converged web-browsing service scenarios in NGN

Y.2236: Framework for NGN support of multicast-based services

Y.2237: Functional model and service scenarios for QoS-enabled mobile VoIP service

Y.2240: Requirements and capabilities for next generation network service integration and delivery environment

Y.2251: Multi-connection requirements

Y.2261: PSTN/ISDN evolution to NGN

Y.2262: PSTN/ISDN emulation and simulation

Y.2271: Call server-based PSTN/ISDN emulation

Y.2281: Framework of networked vehicle services and applications using NGN

Y.2291: Architectural overview of next generation home networks

4 Network Management

Y.2401/M.3060: Principles for the Management of Next Generation Networks

5 Security

Y.2701: Security requirements for NGN release 1

Y.2702: Authentication and authorization requirements for NGN release 1

Y.2703: The application of AAA service in NGN

Y.2704: Security mechanisms and procedures for NGN

Y.2705: Minimum Security Requirements for Interconnection of Emergency Telecommunication Services (ETS)

Y.2720: NGN identity management framework

Y.2721: NGN identity management requirements and use cases

Y.2722: NGN identity management mechanisms

Y.2740: Security requirements for mobile remote financial transactions in next generation networks

Y.2741: Architecture of secure mobile financial transactions in next generation networks

Y.2760: Mobility security framework in NGN

Y.2770: Requirements for Deep Packet Inspection in Next Generation Networks

6 Generalized Mobility

Y.2801/Q.1706: Mobility management requirements for NGN

Y.2802/Q.1762: Fixed-mobile convergence general requirements

Y.2803/Q.1763: FMC service using legacy PSTN or ISDN as the fixed access network for mobile network users

Y.2804/Q.1707: Generic framework of mobility management for next generation networks

Y.2805/Q.1708: Framework of location management for NGN

Y.2806/Q.1709: Framework of handover control for NGN

Y.2807: MPLS-based mobility capabilities in NGN

Y.2808: Fixed mobile convergence with a common IMS session control domain

Y.2809: Framework of mobility management in the service stratum for next generation networks

Y.2810: Mobility management framework for IP multicast communications in NGN

7 Supplements and Handbooks on NGN (use cases)

Y Suppl. 1: ITU-T Y.2000 series – Supplement on NGN release 1 scope

Y Suppl. 2: ITU-T Y.2012 – Supplement on session/border control (S/BC) functions

Y Suppl. 3: ITU-T Y.2000 series – Supplement on service scenarios for convergence services in a multiple network and application service provider environment

Y Suppl. 4: ITU-T Y.1300 series – Supplement on transport requirements for T-MPLS OAM and considerations for the application of IETF MPLS technology

Y Suppl. 5: ITU-T Y.1900-series – Supplement on IPTV service use cases

Y Suppl.6: ITU-T Y.2000-series – Supplement on the use of DSL-based systems in next generation networks

Y Suppl.7: ITU-T Y.2000-series – Supplement on NGN release 2 scope

Y Suppl. 8: ITU-T Y.2000-series – Supplement on a survey of global ICT forums and consortia

Y Suppl. 9: ITU-T Y.2000-series – Supplement on multi-connection scenarios

Y Suppl. 10: ITU-T Y.2000-series – Supplement on distributed service network (DSN) use cases

Y Suppl. 12: ITU-T Y.2720 – Supplement on NGN identity management mechanisms

Y Suppl. 13: ITU-T Y.2000-series - Scenarios for the evolution of NGN network capabilities to include information storage, processing and delivery

Y Suppl. 14: ITU-T Y.2000-series – Supplementary service scenarios for fixed-mobile convergence

Y Suppl. 15: ITU-T Y.2000-series – Profile-based application adaptation service using NGN

Y Suppl. 16: ITU-T Y.1900-series – Guidelines on deployment of IP multicast for IPTV content deliveryHandbook: Converging networks (2010)

NGN Related ITU-T SG11 Approved Q-Series Supplements

1 Network signalling and control functional architecture

Q.3030: Signalling architecture for the NGN service control plane

Q.3040: Signalling architecture for IPTV control plane

2 Bearer Control Signalling

Q.3150/Y.1416: Use of virtual trunks for ATM/MPLS client/server control plane interworking

Q.3151/Y.1417: ATM and frame relay/MPLS control plane interworking: Client-server

3 Signalling and control requirements and protocols to support attachment in NGN environments

Q.3201: EAP-based security signalling protocol architecture for network attachment

Q.3202.1: Authentication protocols based on EAP-AKA for interworking among 3GPP, WiMax, and WLAN in NGN

Q.3203: Signalling requirements and architecture of network attachment control functions to support IP mobility

Q.3220: Architectural framework for NACF signalling interface Recommendations

Q.3221: Requirements and protocol at the interface between the service control entity and the transport location management physical entity (S-TC1 interface)

Q.3222: Requirements and protocol at the interface between transport location management physical entities (Ng interface)

Q.3223: Requirements and protocol for the interface between a transport location management physical entity and a policy decision physical entity (Ru Interface)

4 Resource control protocols

Q.3300: Architectural framework for the Q.33xx series of Recommendations

Q.3301.1: Resource control protocol No. 1, version 2 – Protocol at the Rs interface between service control entities and the policy decision physical entity

Q.3302.1: Resource control protocol No. 2 (rcp2) – Protocol at the Rp interface between transport resource control physical entities

Q.3303.0: Resource control protocol No. 3 – Protocols at the Rw interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE): Overview

Q.3303.1: Resource control protocol No. 3 – Protocol at the interface between a Policy Decision Physical Entity (PD-PE) and a Policy Enforcement Physical Entity (PE-PE): COPS alternative

Q.3303.2: Resource control protocol No. 3 – Protocol at the interface between a Policy Decision Physical Entity (PD-PE) and a Policy Enforcement Physical Entity (PE-PE) (Rw interface): H.248 alternative

Q.3303.3: Resource control protocol No. 3 – Protocols at the Rw interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE): Diameter

Q.3304.1: Resource control protocol No. 4 (rcp4) – Protocols at the Rc interface between a transport resource control physical entity (TRC-PE) and a transport physical entity (T-PE): COPS alternative

Q.3304.2: Resource control protocol No. 4 (rcp4) – Protocols at the Rc interface between a transport resource control physical entity (TRC-PE) and a transport physical entity (T-PE): SNMP alternative

Q.3305.1: Resource control protocol No. 5 (rcp5) – Protocol at the interface between transport resource control physical entity and policy decision physical entity (Rt interface): Diameter-based

Q.3306.1: Resource control protocol No. 6 (rcp6) - Protocol at the interface between intra-domain policy decision physical entities (PD-PE) (Rd interface)

Q.3307.1: Resource control protocol No.7 - Protocol at the interface between inter-domain policy decision physical entities (Ri interface)

Q.3308.1: Resource control protocol 8 (rcp8) Protocol at the interface between Resource Admission Control Physical Entity (RAC-PE) and CPN Gateway Policy Enforcement Physical Entities (CGPE-PE) (Rh interface): COPS alternative

Q.3309: QoS coordination protocol

Q.3311: Enhancement of resource and admission control protocols to use pre-congestion notification

Q.3312: Use of the access node control protocol on the Rp interface

Q.3313: Signalling protocols and procedures relating to flow state aware QoS control in a bounded subnetwork of a next generation network

5 Service and session control protocols

Q.3401: NGN NNI signalling profile (protocol set 1)

Q.3402: NGN UNI signalling profile (Protocol set 1)

6 Service and session control protocols – supplementary services

Q.3610: Signalling requirements and protocol profiles for customized ring-back tone service

Q.3611: Signalling requirements and protocol profiles for NGN customized ringing tone service

Q.3612: Signalling requirements and protocol profiles for IP Centrex service

7 Testing for NGN networks

Q.3900: Methods of testing and model network architecture for NGN technical means testing as applied to public telecommunication networks

Q.3901: Testing topology for networks and services based on NGN technical means

Q.3902: Operational parameters to be monitored when implementing NGN technical means in public telecommunication networks

Q.3903: Formalized presentation of testing results

Q.3904: Testing principles for IMS model networks, and identification of relevant conformance, interoperability and functionality tests

Q.3906.1: Test scenarios and catalogue for testing fixed-broadband access networks using a model network - Part I

Q.3909: The framework and overview of NGN conformance and interoperability testing

Q.3910: Parameters for monitoring NGN protocols

Q.3911: Parameters for monitoring voice services in NGN

Q.3925: The types of traffic flows which should be generated for voice, data and video on the Model network for testing QoS parameters

Q.3931.1: Performance benchmark for the PSTN/ISDN emulation subsystem of an IP multimedia system - Part 1: Core concepts

Q.3931.2: Performance benchmark for the PSTN/ISDN emulation subsystem of an IP multimedia system - Part 2: Subsystem configurations and benchmarks

Q.3941.1: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 1: Test suite structure and test purposes for SIP-ISDN

Q.3941.2: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 2: Abstract test suite and partial protocol implementation extra information for testing proforma specification for SIP-ISDN

Q.3941.3: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 3: Test suite structure and test purposes for SIP-SIP

Q.3941.4: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 4: Abstract test suite and partial protocol implementation extra information for testing proforma specification for SIP-SIP

Q.3945: Test specifications for next generation network services on model networks - Test set 1

Q.3948: Service testing framework for VoIP at the user-to-network interface of next generation networks

Q.3950: Testing and model network architecture for tag-based identification systems and functions

8 Supplements and Handbooks

Q Suppl. 51: Signalling requirements for IP-QoS

Q Suppl. 52: NNI mobility management requirements for systems beyond IMT-2000

Q Suppl. 53: Signalling requirements to support the International Emergency Preference Scheme (IEPS)

Q Suppl. 54: Signalling requirements at the interface between SUP-FE and I/S-CSC-FE

Q Suppl. 55: Signalling requirements at the interface between AS-FE and S-CSC-FE

Q Suppl. 56: Organization of NGN service user data

Q Suppl. 57: Signalling requirements to support the emergency telecommunications service (ETS) in IP networks

Q Suppl. 58: Organization of NGN transport user data

Q Suppl. 59: Signalling flows and parameter mapping for resource control

Q Suppl. 60: Supplement to Recommendations ITU-T Q.3610 and ITU-T Q.3611 - Service flows for customized multimedia ring-back tone (CRBT) and customized multimedia ringing tone (CRT) services

Q Suppl. 61: Evaluation of signalling protocols to support ITU-T Y.2171 admission control priority levels

Q Suppl. 62: Overview of the work of standards development organizations and other organizations on emergency telecommunications service

Handbook on deployment of packet based networks (2009)

Handbook on Testing (2011)

IMT related Recommendations

Q.1711: Network functional model for IMT

Q.1721: Information flows for IMT capability set 1

Q.1731: Radio-technology independent requirements for IMT layer 2 radio interface

Q.1741.1: IMT references to release 1999 of GSM evolved UMTS core network with UTRAN access network

Q.1741.2: IMT references to release 4 of GSM evolved UMTS core network with UTRAN access network

Q.1741.3: IMT references to release 5 of GSM evolved UMTS core network

Q.1741.4: IMT references to release 6 of GSM evolved UMTS core network

Q.1741.5: IMT references to Release 7 of GSM-evolved UMTS core network

Q.1741.6: IMT references to Release 8 of GSM-evolved UMTS core network

Q.1741.7: IMT references to Release 9 of GSM-evolved UMTS core network

Q.1742.1: IMT references to ANSI-41 evolved core network with cdma2000 access network

Q.1742.2: IMT references (approved as of 11 July 2002) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.3: IMT references (approved as of 30 June 2003) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.4: IMT references (approved as of 30 June 2004) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.5: IMT references (approved as of 31 December 2005) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.6: IMT references (approved as of 31 December 2006) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.7: IMT references (approved as of 30 June 2008) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.8: IMT references (approved as of 31 January 2010) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.9: IMT references (approved as of 31 December 2010) to ANSI-41 evolved core network with cdma2000 access network

Q.1751: Internetwork signalling requirements for IMT capability set 1

Q.1761: Principles and requirements for convergence of fixed and existing IMT systems

Operation & Tariff related Recommendations

D.271: Charging and accounting principles for NGN

E.370: Service principles when public circuit-switched international telecommunication networks interwork with IP-based networks

E.4110: Framework for operations requirements of next generation networks and services

NGN Management related Recommendations

M.3210.1: TMN management services for IMT-2000 security management

M.3340: Framework for NGN service fulfilment and assurance management across the business to business and customer to business interfaces

M.3341: Requirements for QoS/SLA management over the TMN X-interface for IP-based services

M.3342: Guidelines for the definition of SLA representation templates

M.3343: Requirements and analysis for NGN trouble administration across B2B and C2B interfaces

M.3344: Requirements and analysis for NGN appointment management across the business-to-business and customer-to-business interfaces

M.3345: Principles for self-service management

M.3347: Requirements for the NGN service activation of NMS-EMS interface

M.3348: Requirements of the NMS-EMS management interface for NGN service platforms

M.3350: TMN service management requirements for information interchange across the TMN X-interface to support provisioning of Emergency Telecommunication Service (ETS)

M.3361: Requirements for business-to-government management interfaces - B2G interfaces – Introduction

M.3400: TMN management functions

M.3410: Guidelines and requirements for security management systems to support telecommunications management

NGN Related ITU-R Recommendations

Recommendation S.1806: Availability objectives for hypothetical reference digital paths in the fixed-satellite service operating below 15 GHz

Report ITU-R M.2176-1: Vision and requirements for the satellite radio interface(s) of IMT-Advanced

Preliminary draft new Recommendation ITU-R S.1897: Cross-layer based QoS provisioning in IP-based hybrid satellite-terrestrial networks

Recommendation F.1094-2: Maximum allowable error performance and availability degradations to digital fixed wireless systems arising from radio interference from emissions and radiations from other sources

Recommendation F.1704: Characteristics of multipoint-to-multipoint fixed wireless systems with mesh network topology operating in frequency bands above about 17 GHz

Recommendation F.1763: Radio interface standards for broadband wireless access systems in the fixed service operating below 66 GHz

Recommendation M.819: International Mobile Telecommunications-2000 (IMT-2000) for developing countries

Recommendation M.1457: Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2000 (IMT-2000)

Recommendation M.2012: Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications Advanced (IMT-Advanced)

_____

Международный союз электросвязи (МСЭ)
Бюро развития электросвязи (БРЭ)
Канцелярия Директора
Place des Nations
CH-1211 Geneva 20 - Switzerland
Эл. почта: **bdtdirector@itu.int**
Тел.: +41 22 730 5035/5435
Факс: +41 22 730 5484

Заместитель Директора и руководитель Департамента администрирования и координации основной деятельности (DDR)
Эл. почта: **bdtdeputydir@itu.int**
Тел.: +41 22 730 5784
Факс: +41 22 730 5484

Департамент инфраструктуры, благоприятной среды и электронных приложений (IEE)
Эл. почта: **bdtiee@itu.int**
Тел.: +41 22 730 5421
Факс: +41 22 730 5484

Департамент инноваций и партнерских отношений (IP)
Эл. почта: **bdtip@itu.int**
Тел.: +41 22 730 5900
Факс: +41 22 730 5484

Департамент поддержки проектов и управления знаниями (PKM)
Эл. почта: **bdtpkm@itu.int**
Тел.: +41 22 730 5447
Факс: +41 22 730 5484

Африка

Эфиопия
Региональное отделение МСЭ
P.O. Box 60 005
Gambia Rd., Leghar ETC Bldg 3rd Floor
Addis Ababa – Ethiopia
Эл. почта: **itu-addis@itu.int**
Тел.: (+251 11) 551 49 77
Тел.: (+251 11) 551 48 55
Тел.: (+251 11) 551 83 28
Факс: (+251 11) 551 72 99

Камерун
Зональное отделение МСЭ
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun
Эл. почта: **itu-yaounde@itu.int**
Тел.: (+ 237) 22 22 92 92
Тел.: (+ 237) 22 22 92 91
Факс: (+ 237) 22 22 92 97

Сенегал
Зональное отделение МСЭ
Immeuble Fayçal, 4e étage
19, Rue Parchappe x Amadou Assane Ndoye
Boîte postale 50202 Dakar RP
Dakar - Sénégal
Эл. почта: **itu-dakar@itu.int**
Тел.: (+221) 33 849 77 20
Факс: (+221) 33 822 80 13

Зимбабве
Зональное отделение МСЭ
TelOne Centre for Learning
Corner Samora Machel
and Hampton Road
P.O. Box BE 792
Belvédère Hararé - Zimbabwe
Эл. почта: **itu-harare@itu.int**
Тел.: (+263 4) 77 59 41
Тел.: (+263 4) 77 59 39
Факс: (+263 4) 77 12 57

Северная и Южная Америка

Бразилия
Региональное отделение МСЭ
SAUS Quadra 06 Bloco "E"
11º andar – Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
CEP 70070-940 Brasilia, DF – Brésil
Эл. почта: **itubrasilia@itu.int**
Тел.: (+55 61) 2312 2730-1
Тел.: (+55 61) 2312 2733-5
Факс: (+55 61) 2312 2738

Барбадос
Зональное отделение МСЭ
United Nations House
Marine Gardens
Hastings - Christ Church
P.O. Box 1047
Bridgetown - Barbados
Эл. почта: **itubridgetown@itu.int**
Тел.: (+1 246) 431 0343/4
Факс: (+1 246) 437 7403

Чили
Зональное отделение МСЭ
Merced 753, Piso 4
Casilla 50484 - Plaza de Armas
Santiago de Chile - Chile
Эл. почта: **itusantiago@itu.int**
Тел.: (+56 2) 632 6134/6147
Факс: (+56 2) 632 6154

Гондурас
Зональное отделение МСЭ
Colonia Palmira, Avenida Brasil
Edificio COMTELCA/UIT 4.º Piso
P.O. Box 976
Tegucigalpa - Honduras
Эл. почта: **ituteguciglapa@itu.int**
Тел.: (+504) 22 201 074
Факс: (+504) 22 201 075

Арабские государства

Египет
Региональное отделение МСЭ
Smart Village, Building B 147, 3rd floor
Km 28 Cairo - Alexandria Desert Road
Giza Governorate
Cairo - Egypt
Эл. почта: **itucairo@itu.int**
Тел.: (+202) 3537 1777
Факс: (+202) 3537 1888

Азиатско-Тихоокеанский регион

Таиланд
Региональное отделение МСЭ
Thailand Post Training Center,
5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 - Thailand
Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand
Эл. почта: **itubangkok@itu.int**
Тел.: (+66 2) 575 0055
Факс: (+66 2) 575 3507

Индонезия
Зональное отделение МСЭ
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 - Indonesia
Mailing address:
c/o UNDP - P.O. Box 2338
Jakarta 10001 - Indonesia
Эл. почта: **itujakarta@itu.int**
Тел.: (+62 21) 381 35 72
Тел.: (+62 21) 380 23 22
Тел.: (+62 21) 380 23 24
Факс: (+62 21) 389 05 521

СНГ

Российская Федерация
Зональное отделение МСЭ
4, building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Mailing address:
P.O. Box 25 - Moscow 105120
Russian Federation
Эл. почта: **itumoskow@itu.int**
Тел.: (+7 495) 926 60 70
Факс: (+7 495) 926 60 73

Европа

Швейцария
Международный союз электросвязи (МСЭ)
Бюро развития электросвязи (БРЭ)
Европейское подразделение (EBP)
Place des Nations
CH-1211 Geneva 20 - Switzerland
Эл. почта: **eurregion@itu.int**
Тел.: +41 22 730 5111

Международный союз электросвязи
Бюро развития электросвязи
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

Отпечатано в Швейцарии
Женева, 2014 г.

01/2014 г.