Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2201

(09/2009)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Сети последующих поколений – Аспекты обслуживания: возможности услуг и архитектура услуг

Требования к СПП МСЭ-Т и возможности этих сетей

Рекомендация МСЭ-Т Y.2201

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	Y.100–Y.999
Общие положения	Y.100–Y.199
Услуги, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ	Y.1000–Y.1999
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
IPTV по СПП	
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	Y.2000–Y.2999
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности услуг и архитектура услуг	**Y.2200–Y.2249**
Аспекты обслуживания: взаимодействие услуг и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Будущие сети	Y.2600–Y.2699
Безопасность	Y.2700–Y.2799
Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т Y.2201

Требования к СПП МСЭ-Т и возможности этих сетей

Резюме

В данной Рекомендации МСЭ-Т представлены требования высокого уровня к услугам сетей последующих поколений (СПП) и возможности СПП.

Источник

Рекомендация МСЭ-Т Y.2201 была утверждена 12 сентября 2009 года 13-й Исследовательской комиссией МСЭ-Т (2009–2012 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ. Настоящее издание включает Исправление 1, которое было утверждено 29 января 2010 года 13-й Исследовательской комиссией МСЭ-Т.

Ключевые слова

Учет, адресация, аутентификация, санкционирование, возможности, требования к возможностям, начисление платы, информированность о контексте, сеть предприятия, идентификация, управление определением идентичности, функциональная совместимость, взаимодействие, IPTV, поддержка IPv6, управление, мобильность, многоадресная передача, наименование, СПП, нумерация, OAM, открытая среда услуг, политика, конфиденциальность, профиль, QoS, безопасность, средство подключения услуги.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т Y.2201

Требования к СПП МСЭ-Т и возможности этих сетей

1 Сфера применения

В данной Рекомендации определяются требования высокого уровня для разработки набора Рекомендаций МСЭ-Т, которые будут служить основой для СПП.

Требования высокого уровня и соответствующие возможности, определенные в данной Рекомендации, соответствуют основным целям и требованиям, которые зафиксированы в [ITU-T Y.2001], и основаны на требованиях к СПП версии 2 [b-ITU-T Y.Sup.7].

Эти требования в основном исходят из перспектив высокого уровня и не предназначены для формирования точных функциональных требований для различных объектов СПП.

Более подробные сведения о требованиях выходят за рамки данной Рекомендации.

Известно, что конкретная реализация СПП может быть составлена произвольным набором или расширенным набором услуг, поддерживаемых в СПП, и возможностей, как указано в данной Рекомендации.

ПРИМЕЧАНИЕ 1. – Текст, взятый из [ITU-T Y.2201], выделен синим шрифтом. Кроме того, в Дополнении I определяются основные различия между настоящей Рекомендацией и [ITU-T Y.2201] с точки зрения требований высокого уровня и функциональных возможностей.

ПРИМЕЧАНИЕ 2. – Также требуется рассмотреть вопрос о том, каким образом СПП могут способствовать экономии электроэнергии, однако исследования по данной теме ведутся в 5-й Исследовательской комиссии МСЭ-Т на основе результатов работы Оперативной группы МСЭ-Т по ИКТ и изменению климата. Таким образом, требования в отношении экономии электроэнергии подлежат дальнейшему исследованию в настоящей Рекомендации. Результаты работы указанной Оперативной группы МСЭ-Т см. в Документе [b-ITU-T Climate].

2 Справочные документы

В нижеследующих Рекомендациях МСЭ-Т и других справочных документах содержатся положения, которые, посредством ссылок в настоящем тексте, составляют положения настоящей Рекомендации. На время публикации указанные здесь издания были действительными. Все Рекомендации и другие справочные документы постоянно пересматриваются, поэтому всем пользователям данной Рекомендации настоятельно рекомендуется изучить возможность использования последних изданий, перечисленных ниже Рекомендаций и других справочных документов. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка в настоящей Рекомендации на какой-либо документ не придает этому отдельному документу статуса рекомендации.

[ITU-T E.106] Рекомендация МСЭ-Т E.106 (2003 г.), *Международная схема аварийных приоритетов (IEPS) для операций по ликвидации последствий чрезвычайных ситуаций.*

[ITU-T E.107] Рекомендация МСЭ-Т E.107 (2007 г.), *Служба электросвязи в чрезвычайных ситуациях (ETS) и основа для взаимодействия реализованных на национальном уровне ETS.*

[ITU-T E.164] Рекомендация МСЭ-Т E.164 (2005 г.), *Международный план нумерации электросвязи общего пользования*.

[ITU-T E.212] Рекомендация МСЭ-Т E.212 (2008 г.), *План международной идентификации для сетей общего пользования и абонентов.*

[ITU-T G.711] Recommendation ITU-T G.711 (1988), *Pulse code modulation (PCM) of voice frequencies*.

[ITU-T G.722] Recommendation ITU-T G.722 (1988), *7 kHz audio-coding within 64 kbit/s*.

[ITU-T G.722.2] Recommendation ITU-T G.722.2 (2003), *Wideband coding of speech at around 16 kbit/s using Adaptive Multi-Rate Wideband (AMR-WB)*.

[ITU-T G.729] Recommendation ITU-T G.729 (2007), *Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)*.

[ITU-T G.729.1] Рекомендация МСЭ-Т G.729.1 (2006 г.), *Встроенный кодер G.729 с переменной скоростью передачи: двоичный поток широкополосного масштабируемого кодера со скоростями 8-32 кбит/с, способный взаимодействовать с G.729.*

[ITU-T G.808.1] Рекомендация МСЭ-Т G.808.1 (2006 г.), *Обобщенная защитная коммутация – Линейная защита канала и подсети.*

[ITU-T H.263] Рекомендация МСЭ-Т H.263 (2005 г.), *Кодирование видеосигнала для низкоскоростной связи.*

[ITU-T H.264] Рекомендация МСЭ-Т H.264 (2005 г.), *Усовершенствованное кодирование изображений для общих аудиовизуальных услуг.*

[ITU-T I.610] Recommendation ITU-T I.610 (1999), *B-ISDN operation and maintenance principles and functions*.

[ITU-T M.3050.0] Recommendation ITU-T M.3050.0 (2007), *Enhanced Telecom Operations Map (eTOM) – Introduction*.

[ITU-T M.3050.1] Recommendation ITU-T M.3050.1 (2007), *Enhanced Telecom Operations Map (eTOM) – The business process framework*.

[ITU-T M.3060] Рекомендация МСЭ-Т M.3060/Y.2401 (2006 г.), *Принципы управления сетями последующих поколений.*

[ITU-T Q.825] Recommendation ITU-T Q.825 (1998), *Specification of TMN applications at the Q3 interface: Call detail recording*.

[ITU-T Q.1703] Recommendation ITU-T Q.1703 (2004), *Service and network capabilities framework of network aspects for systems beyond IMT-2000*.

[ITU-T Q.1706] Рекомендация МСЭ-Т Q.1706/Y.2801 (2006 г.), *Требования к управлению мобильностью для СПП.*

[ITU-T X.462] Recommendation ITU-T X.462 (1996), *Information technology – Message Handling Systems (MHS) Management: Logging information*.

[ITU-T X.805] Рекомендация МСЭ-Т X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами.*

[ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure principles and framework architecture.*

[ITU-T Y.110] Recommendation ITU-T Y.110 (1998), *Global Information Infrastructure principles and framework architecture.*

[ITU-T Y.1271] Рекомендация МСЭ-Т Y.1271 (2004 г.), *Концептуальные требования и сетевые ресурсы для обеспечения экстренной связи по сетям связи, находящимся в стадии перехода от коммутации каналов к коммутации пакетов.*

[ITU-T Y.1541] Рекомендация МСЭ-Т Y.1541 (2006 г.), *Требования к сетевым показателям качества для служб, основанных на протоколе IP.*

[ITU-T Y.1710] Recommendation ITU-T Y.1710 (2002), *Requirements for Operation & Maintenance functionality in MPLS networks*.

[ITU-T Y.1730] Recommendation ITU-T Y.1730 (2004), *Requirements for OAM functions in Ethernet-based networks and Ethernet services*.

[ITU-T Y.1901] Рекомендация МСЭ-Т Y.1901 (2009 г.), *Требования для поддержки услуг IPTV*.

[ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

[ITU-T Y.2051] Recommendation ITU-T Y.2051 (2008), *General overview of IPv6 based NGN*.

[ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Network*.

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in next generation networks*.

[ITU-T Y.2201] Рекомендация МСЭ-Т Y.2201 (2007 г.), *Требования к сетям последующих поколений версии 1*.

[ITU-T Y.2212] Recommendation ITU-T Y.2212 (2008), *Requirements of managed delivery services*.

[ITU-T Y.2213] Recommendation ITU-T Y.2213 (2008), *NGN service requirements and capabilities for network aspects of applications and services using tag-based identification*.

[ITU-T Y.2215] Recommendation ITU-T Y.2215 (2009), *Requirements and framework for the support of VPN services in NGN including mobile environment*.

[ITU-T Y.2233] Рекомендация МСЭ-Т Y.2233 (2008 г.), *Требования и структура, обеспечивающие возможности учета и начисления платы в СПП*.

[ITU-T Y.2234] Recommendation ITU-T Y.2234 (2008), *Open service environment capabilities for NGN*.

[ITU-T Y.2236] Recommendation ITU-T Y.2236 (2009), *Framework for NGN support of multicast based services*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

[ITU-T Z.100] Recommendation ITU-T Z.100 (2007), *Specification and Description Language (SDL)*.

[ETSI TS 126.071] ETSI TS 26.071 V6.0.0 (2004-12), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); AMR speech Codec; General description (3GPP TS 26.071 version 6.0.0 Release 6)*.

[TIA-127-C] TIA Standard TIA-127-C (2007), *Enhanced Variable Rate Codec, Speech Service Options 3, 68, and 70 for Wideband Spread Spectrum Digital Systems*.

3 Определения

3.1 Термины, определенные в других документах

В данной Рекомендации используются следующие термины, определенные в других документах:

3.1.1 учет (accounting) [ITU-T X.462]: Деятельность по сбору информации об операциях, осуществленных в рамках системы, и их последствиях.

3.1.2 адрес (address) [ITU-T Y.2091]: Адрес представляет собой идентификатор для конкретного пункта завершения связи и используется для маршрутизации в этот пункт завершения.

3.1.3 интерфейс приложение-сеть (application network interface) (ANI) [ITU-T Y.2012]: Интерфейс, обеспечивающий канал взаимодействия и обмена между приложениями и элементами СПП. ANI обеспечивает возможности и ресурсы, необходимые для внедрения приложений.

3.1.4 выставление счетов (billing) [ITU-T Q.1703]: Административная функция для подготовки счетов потребителям услуг, для своевременной оплаты, получения выручки и работы с рекламациями клиентов.

3.1.5 начисление платы (charging) [ITU-T Q.825]: Набор функций, необходимых для определения цены, назначаемой за пользование услугами.

3.1.6 корпоративная сеть (corporate network) [ITU-T Y.2701]: Частная сеть, которая поддерживает множество пользователей и которая может располагаться во многих местах, например на предприятии, в университетском городке.

ПРИМЕЧАНИЕ. – Владение и управление оборудованием этой частной сети осуществляются от лица предприятия. Оборудование присоединяется для предоставления услуг электросвязи к определенной группе пользователей, относящихся к данному предприятию.

3.1.7 клиент (customer) [ITU-T M.3050.1]: Клиент приобретает продукты и услуги у предприятия либо получает бесплатные предложения или услуги. Клиент может быть лицом или предприятием.

3.1.8 конечный пользователь (end user) [ITU-T M.3050.1]: Конечный пользователь является фактическим пользователем продуктов или услуг, предлагаемых предприятием. Конечный пользователь потребляет продукт или услугу. См. также определение термина "Абонент".

3.1.9 объект (entity) [ITU-T Y.2720]: Все, что существует самостоятельно и является различимым, что может быть идентифицировано уникальным образом. В контексте IdM примерами объектов являются абоненты, пользователи, сетевые элементы, сети, программные приложения, услуги и устройства. Какой-либо один объект может иметь множество идентификаторов.

3.1.10 федерация (federation) [ITU-T Y.2720]: Установление отношений между двумя или более объектами или создание ассоциации, включающей любое количество поставщиков услуг и поставщиков данных идентичности.

3.1.11 эстафетная передача вызова (handover) [ITU-T Q.1706]: Возможность предоставлять услуги, которая некоторым образом влияет на соглашения об уровне обслуживания, движущемуся объекту во время и после передвижения.

3.1.12 домашняя сеть (home network) [ITU-T Q.1706]: Сеть, с которой мобильный пользователь обычно соединен, или поставщик услуг, с которым связан мобильный пользователь, где осуществляется управление информацией о контракте пользователя.

3.1.13 идентификатор (identifier) [ITU-T Y.2091]: Идентификатор представляет собой серию цифр, букв и символов или данных в любой другой форме, используемую для идентификации абонента(ов), пользователя(ей), элемента(ов) сети, функции(й), объекта(ов) сети, предоставляющего(их) услуги/приложения, или других объектов (например, физические или логические объекты). Идентификаторы могут использоваться для регистрации или авторизации. Они могут быть либо открытыми для всех сетей и используемыми совместно ограниченным количеством сетей, либо частными для конкретной сети (частные ID, как правило, не раскрываются третьим сторонам).

3.1.14 идентичность (identity) [ITU-T Y.2720]: Информация об объекте, которая является достаточной для идентификации этого объекта в том или ином конкретном контексте.

3.1.15 управление определением идентичности (identity management) [ITU-T Y.2720]: Набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, сопоставление и увязка, обеспечение реализации политики, аутентификация и утверждения), используемых для:

– гарантирования информации, подтверждающей идентичность (например, идентификаторов, регистрационных данных, атрибутов);

– гарантирования идентичности объекта (например, пользователей/абонентов, групп, устройств пользователей, организаций, поставщиков доступа к сети и поставщиков услуг, сетевых элементов и объектов, а также виртуальных объектов); и

– обеспечения коммерческих приложений и приложений безопасности.

3.1.16 поставщик данных идентичности (identity provider) [ITU-T Y.2720]: Объект, который создает и поддерживает надежную информацию, подтверждающую идентичность других объектов (например, пользователей/абонентов, организаций и устройств), и управляет такой информацией, а также предоставляет основанные на идентичности услуги на основе доверия, деловых отношений и других типов отношений.

3.1.17 интернет (internet) [ITU-T Y.101]: Совокупность присоединяемых сетей, использующих протокол Интернет, который позволяет им функционировать как единой, крупной виртуальной сети.

3.1.18 СПП на базе IPv6 (IPv6-based NGN) [ITU-T Y.2051]: Обозначает СПП, поддерживающую адресацию, протоколы маршрутизации и услуги, относящиеся к IPv6. СПП на базе IPv6 распознают и обрабатывают заголовки и варианты IPv6, работая поверх различных транспортных технологий, которые лежат ниже в страте транспортирования.

3.1.19 мобильность (mobility) [ITU-T Y.2001]: Возможность для пользователя или других подвижных объектов осуществлять связь и иметь доступ к услугам вне зависимости от изменений местоположения или технических условий. Степень доступности услуги может зависеть от нескольких факторов, включая возможности сети доступа, соглашения об уровне обслуживания между домашней сетью пользователя и визитной сетью (если это применимо) и т. д. Мобильность включает возможность обеспечения электросвязи с непрерывным предоставлением услуг или без непрерывного предоставления услуг.

ПРИМЕЧАНИЕ. – В Рекомендации [ITU-T Y.2001] это понятие называется универсальной мобильностью.

3.1.20 управление мобильностью (mobility management) [ITU-T Q.1706]: Набор функций, используемых для обеспечения мобильности.

3.1.21 кочевничество (nomadism) [ITU-T Q.1706]: Возможность для пользователя изменять при передвижении свой пункт доступа к сети; при изменении пункта доступа к сети сеанс обслуживания пользователя полностью останавливается и затем вновь начинается, т. е. непрерывный сеанс или передача абонента невозможны. Считается, что обычный способ использования следующий: пользователь завершает своей сеанс обслуживания до перемещения в другой пункт доступа.

3.1.22 информация, позволяющая установить личность (personally identifiable information) [ITU-T Y.2720]: Информация, относящаяся к любому живущему лицу, которая дает возможность идентифицировать такое лицо (включая информацию, которая может идентифицировать лицо в сочетании с другой информацией, даже если такая информация не точно идентифицирует данное лицо).

3.1.23 персональная мобильность (personal mobility) [ITU-T Q.1706]: Означает мобильность для тех сценариев, при которых пользователь изменяет оконечное оборудование, используемое для доступа к сети в различных пунктах. Возможность пользователя получить доступ к услугам электросвязи с любого оконечного оборудования на основе персонального идентификационного номера, а также возможность сети предоставлять эти услуги определяется в профиле услуги пользователя.

3.1.24 присутствие (presence) [ITU-T Y.2720]: Набор атрибутов, характеризующий объект по отношению к его текущему статусу.

3.1.25 сеть общего пользования (public network) [b-ITU-T I.570]: Любая сеть, предоставляющая услуги населению.

ПРИМЕЧАНИЕ. – Настоящее определение не включает правовые или регуляторные аспекты и не указывает на какие бы то ни было аспекты собственности.

3.1.26 роуминг (roaming) [ITU-T Q.1706]: Означает возможность пользователей получать доступ к услугам в соответствии со своим профилем пользователя, находясь при этом вне своей домашней абонентской сети, т. е. используя пункт доступа визитной сети. Для этого необходима возможность доступа к визитной сети, наличие интерфейса между домашней сетью и визитной сетью, а также соглашение о роуминге между соответствующими сетевыми операторами.

3.1.27 плавная эстафетная передача вызова (seamless handover) [ITU-T Q.1706]: Особый случай мобильности с непрерывностью обслуживания, так как он сохраняет способность предоставлять услуги движущимся объектам во время и после движения без какого-либо влияния на соглашения об уровне обслуживания.

3.1.28 услуга (service): Набор функций и средств, предлагаемых поставщиком услуг пользователю.

3.1.29 непрерывность обслуживания (service continuity) [ITU-T Q.1706]: Возможность для подвижного объекта сохранять предоставляемое обслуживание, включая текущее состояние, такое как сетевая среда пользователя и сеанс для предоставления услуги.

3.1.30 абонент (subscriber) [ITU-T M.3050.1]: Абонент отвечает за заключение контрактов на абонируемые услуги и за оплату этих услуг.

3.1.31 мобильность оконечного оборудования (terminal mobility) [ITU-T Q.1706]: Означает мобильность для тех сценариев, при которых одно и то же оконечное оборудование перемещается или используется в разных пунктах. Возможность оконечного оборудования получить доступ к услугам электросвязи из различных пунктов и во время движения, а также возможность сети определять и устанавливать местоположение этого оконечного оборудования.

3.1.32 сеть пользователя (user network) [ITU-T Y.2701]: Частная сеть, состоящая из оконечного оборудования, которая может иметь множество пользователей.

3.1.33 визитная сеть (visited network) [ITU-T Q.1706]: Сеть за пределами домашней сети, предоставляющая услуги обслуживание мобильному пользователю. Данный термин имеет большее значение в деловом смысле, чем в географическом.

3.2 Термины, определенные в данной Рекомендации

В данной Рекомендации определяются следующие термины:

3.2.1 "впуск" трафика (break-in): Передача информации от пользователей сети общего пользования пользователям сети предприятия.

3.2.2 "выпуск" трафика (break-out): Передача информации от пользователей сети предприятия пользователям сети общего пользования.

3.2.3 транкинг для коммерческой деятельности (business trunking) (BT): Соединение корпоративной сети последующего поколения (КСПП) с СПП.

3.2.4 приложение транкинга для коммерческой деятельности (business trunking application): Приложение СПП, которое либо предоставляет возможность транзита между несколькими корпоративными сетями последующих поколений (КСПП), или возможность "впуска" трафика из СПП в КСПП и/или возможность "выпуска" трафика из КСПП в СПП.

ПРИМЕЧАНИЕ. – С помощью приложения транкинга для коммерческой деятельности могут также предоставляться дополнительные услуги, помимо возможностей "впуска" трафика, "выпуска" трафика и транзита между КСПП.

3.2.5 информированность о контексте (context awareness): Информированность о контексте – это возможность определять любую последующую операцию в процессе электросвязи или ином процессе, а также влиять на эту операцию путем обращения к статусу соответствующих объектов, которые формируют согласованную среду, составляющую контекст.

3.2.6 идентификатор пользователя корпоративной сети (corporate network user identifier): Определяет находящегося на связи пользователя корпоративной сети, и либо представляет вызывающего пользователя корпоративной сети, либо выступает в качестве идентичности адресата с возможностью глобальной маршрутизации, при вхождении в сеть СПП, ее оставлении или транзите через СПП.

3.2.7 связь на предприятии (enterprise communication): Любая связь, которая либо:

1) инициируется какой-либо корпоративной сетью последующего поколения (КСПП); либо

2) завершается на какой-либо КСПП; либо

3) инициируется СПП от имени предприятия; либо

4) завершается на СПП от имени предприятия;

и которая регулируется специальными соглашениями между оператором СПП и предприятием.

3.2.8 возможности связи на предприятии (enterprise communication capabilities): Любая возможность, размещаемая либо в корпоративной сети последующего поколения (КСПП), либо в СПП, с помощью которой обеспечивается и/или улучшается связь на предприятии.

ПРИМЕЧАНИЕ. – Приложение транкинга для коммерческой деятельности, размещаемые услуги предприятия и виртуальные арендованные линии являются примерами возможностей связи на предприятии, размещаемых в СПП.

3.2.9 размещаемые услуги предприятия (Hosted Enterprise Services (HES)): Приложение СПП, при помощи которого в СПП размещаются все возможности инициирования/завершения коммерческой связи для пользователей предприятия, которые непосредственно подключены к СПП и являются абонентами данного приложения в СПП.

ПРИМЕЧАНИЕ. – Эти услуги обычно называются услугами центральной АТС на базе IP (IP-Centrex).

3.2.10 корпоративная сеть последующего поколения (КСПП) (Next Generation CN (NGCN)): Обособленная корпоративная сеть, которая рассчитана на использование преимуществ появляющихся решений в области связи на базе IP и которая может иметь свои собственные приложения и предоставлять свои собственные услуги.

ПРИМЕЧАНИЕ. – Для целей данной Рекомендации корпоративная сеть является сетью, которая обеспечивает интерфейс с СПП на базе IP.

3.2.11 сайт КСПП (NGCN site): Отдельная часть корпоративной сети последующего поколения (КСПП).

ПРИМЕЧАНИЕ. – Какая-либо КСПП может являться частью другой КСПП, привязанной к конкретному географическому объекту. Если сайт КСПП обслуживает несколько географических объектов, то все объекты, обслуживаемые данным сайтом КСПП, будут иметь доступ к соответствующей СПП по соглашению о подключении сайта КСПП к данной СПП. Связь между различными сайтами КСПП, принадлежащими к одной и той же КСПП, может осуществляться через их соответствующую(ие) СПП, но это не является обязательным. Например, такие передаваемые данные могут маршрутизироваться СПП только во время интенсивного обмена трафиком или в случае отказа оборудования в КСПП. Любой сайт КСПП может иметь доступ к своей СПП либо непосредственно, либо через другую СПП, предоставляющую возможность транзита. КСПП может иметь сайты в разных странах.

3.2.12 классификация приоритетов (priority classification): Классификация классов трафика в соответствии с различными уровнями приоритетов.

3.2.13 механизм поддержки приоритета (priority enabling mechanisms): Механизмы, с помощью которых может обеспечиваться режим передачи трафика в сети, соответствующий приоритету.

3.2.14 трафик частной сети (private network traffic): Трафик, отправляемый или принимаемый СПП для обработки в соответствии с согласованным набором правил, характерных для какого-либо предприятия или сообщества тесно связанных предприятий.

3.2.15 трафик сети общего пользования (public network trafic): Трафик, отправляемый или принимаемый от СПП для обработки в соответствии с обычными правилами СПП.

3.2.16 однократная регистрация входа (single sign-on): Возможность использовать утверждение аутентификации от одного оператора сети/поставщика услуг в сети другого оператора/поставщика услуг для пользователя, запрашивающего доступ к услуге или возможность роуминга в визитной сети.

3.2.17 идентификатор оконечного оборудования (terminal equipment identifier): Уникальный идентификатор оконечного оборудования.

3.2.18 пользователь (user): Понятие "пользователь" включает в себя конечного пользователя [ITU-T Y.2091], физическое лицо, абонента, систему, оборудование, терминал, например факс, персональный компьютер, (функциональный) блок, процесс, приложение, поставщика или корпоративную сеть.

3.2.19 атрибут пользователя (user attribute): Характеристика, которая описывает пользователя, например время жизни идентификатора пользователя, статус пользователя в значении "доступен", "не беспокоить" и т. д.

3.2.20 идентификатор пользователя (user identifier): Тип пароля, образа или псевдонима, связанного с пользователем, который назначается и передается между операторами и поставщиками услуг для идентификации пользователя, аутентификации ее/его личности и/или для авторизации пользования услугой. Примерами могут служить SIP (протокол инициации сеанса связи), URI (унифицированный идентификатор ресурса) и т. д.

4 Сокращения и акронимы

В данной Рекомендации используются следующие сокращения и акронимы:

AMR	Adaptive Multi Rate	Адаптивное кодирование со многими скоростями
ANI	Application Network Interface	Интерфейс приложение-сеть
API	Application Programming Interface	Программный интерфейс приложения
ATM	Asynchronous Transfer Mode	Режим асинхронной передачи
B2B	Business-to-Business	Взаимодействие бизнес-бизнес
CC	Content of Communication	Содержимое передаваемой информации (контент)
CD	Compact Disk	Компакт диск
cPVR	Client Personal Video Recorder	Персональный видеомагнитофон клиента
DECT NG	Digital Enhanced Cordless Telecommunications New Generation	Новое поколение усовершенствованной цифровой беспроводной связи
DNS	Domain Name System	Система доменных имен
DTMF	Dual Tone Multi Frequency	Двухтональный многочастотный набор
EAN	Emergency Alert Notification	Оповещение о чрезвычайной ситуации
ENUM	tElephone NUmber Mapping	Отображение телефонного номера в IP-сети
ETS	Emergency Telecommunications Service	Служба электросвязи в чрезвычайных ситуациях
EVRC	Enhanced Variable Rate Codec	Усовершенствованный кодек с переменной скоростью
HES	Hosted Enterprise Services	Размещаемые услуги предприятия
HTML	Hyper Text Markup Laungage	Язык гипертекстовой разметки
IdM	Identity Management	Управление определением идентичности
IEPS	International Emergency Preference Scheme	Международная приоритетная схема для оказания помощи в чрезвычайных ситуациях
IM	Instant Messaging	Мгновенная передача сообщений
IMS	IP Multimedia Subsystem	Мультимедийная подсистема IP
IN	Intelligent Network	Интеллектуальная сеть
IP	Internet Protocol	Протокол Интернет
IPv4	Internet Protocol version 4	Протокол Интернет версии 4
IPv6	Internet Protocol version 6	Протокол Интернет версии 6
IPTV	Internet Protocol Television	Телевидение на основе протокола Интернет
IRI	Intercept Related Information	Сведения, полученные в результате перехвата данных
ISDN	Integrated Services Digital Network	Цифровая сеть с интеграцией служб (ЦСИС)
LDAP	Lightweight Directory Access Protocol	Облегченный протокол доступа к сетевому каталогу
LEA	Law Enforcement Agencies	Правоохранительные органы
MMS	Multimedia Messaging Service	Услуга передачи мультимедийных сообщений
MPLS	Multi-Protocol Label Switching	Многопротокольная коммутация на основе признаков
NAI	Network Access Identifier	Сетевой идентификатор доступа
NAPT	Network Address Port Translation	Трансляция сетевых адресов и портов
NAT	Network Address Translation	Трансляция сетевых адресов

NB	Narrow Band	Узкая полоса
NGCN	Next Generation Corporate Network	Корпоративная сеть последующего поколения (КСПП)
NGN	Next Generation Network	Сети последующих поколений
NNA	Numbering, Naming and Adressing	Нумерация, наименование и адресация
NNI	Network-Network Interface	Межсетевой интерфейс
nPVR	network Personal Video Recorder	Сетевой персональный видеомагнитофон
OAM	Operations, Administration and Maintenance	Эксплуатация, администрирование и техническое обслуживание
OIP	Originating Identity Presentation	Представление идентичности исходящего пункта
OMA	Open Mobile Alliance	Открытый альянс мобильной связи
OS	Operating System	Операционная система
OSA	Open Service Access	Открытый доступ к услугам
OTN	Optical Transport Network	Оптическая транспортная сеть
PBX	Private Branch Exchange	Телефонная система для частного пользования
PC	Personal Computer	Персональный компьютер
PDA	Personal Digital Assistant	Персональный цифровой секретарь
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PNP	Private Numbering Plan	Частный план нумерации
POTS	Plain Old Telephone Service	Обычная аналоговая телефонная служба
PSAP	Public Safety Answering Point	Пункт сообщений общественной безопасности
PSTN	Public Switched Telephone Network	Коммутируемая телефонная сеть общего пользования (КТСОП)
QoE	Quality of Experience	Оценка пользователем качества услуги
QoS	Quality of Service	Качество обслуживания
QoSM	Quality of Service Measurement	
RACF	Resource and Admission Control Functions	Функции управления ресурсами и допуском
SIP	Session Initiation Protocol	Протокол инициации сеанса связи
SLA	Service Level Agreement	Соглашение об уровне обслуживания
SMS	Short Message Service	Услуга передачи коротких сообщений
SR	Service Resiliency	
TDR	Telecommunications for Disaster Relief	Электросвязь для оказания помощи при бедствиях
TE	Terminal Equipment	Оконечное оборудование
TIP	Termination Identity Presentation	Представление идентичности пункта завершения
UC	Unsolicited Communication	Незапрашиваемое сообщение
UDDI	Universal Discovery, Description and Integration	Универсальное обнаружение, описание и интеграция
UMTS	Universal Mobile Telecommunications System	Универсальная система подвижной электросвязи
UNI	User to Network Interface	Интерфейс пользователь-сеть
URI	Uniform Resource Identifier	Унифицированный идентификатор ресурса
USN	Ubiquitous Sensor Network	Повсеместная сенсорная сеть

VoD	Video on Demand	Видеопрограмма по заказу
VoIP	Voice over Internet Protocol	
VPN	Virtual Private Network	Виртуальная частная сеть
WB	Wide Band	Широкая полоса
Wi-Fi	Wireless Fidelity	Высокая точность беспроводной передачи
xDSL	Various types of Digital Subscriber Lines	Различные типы цифровых абонентских линий

5 Соглашения по терминологии

В настоящей Рекомендации:

Ключевые слова "требуется, чтобы" означают требование, которое необходимо неукоснительно соблюдать и отклонение от которого не допускается, если будет сделано заявление о соответствии этому документу.

Ключевые слова "запрещается" означают требование, которое необходимо неукоснительно соблюдать и отклонение от которого не допускается, если будет сделано заявление о соответствии этому документу.

Ключевые слова "рекомендуется" означают требование, которое рекомендуется соблюдать, но это не является абсолютно необходимым. Таким образом, соблюдение этого требования не является обязательным для заявления о соответствии.

Ключевые слова "не рекомендуется" означают требование в отношении того, что конкретно не запрещено, но рекомендуется избегать. Следовательно, даже если этого избежать не удалось, заявление о соответствии этим техническим требованиям все равно может быть сделано.

Ключевые слова "может быть дополнительно" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Это выражение не означает, что вариант реализации поставщика должен обеспечивать выполнение этой функции и функция может быть дополнительно активирована оператором сети/поставщиком услуг. Это означает лишь, что поставщик может дополнительно предоставить эту функцию и по-прежнему заявлять о соответствии спецификации.

Для целей настоящего документа выражения "сеть предприятия" и "корпоративная сеть" могут взаимно заменять друг друга.

6 Транспортировка

6.1 Возможности подключений для транспортировки

Для страты транспортирования СПП [ITU-T Y.2012] должен использоваться IP-протокол с целью обеспечения общих возможностей подключения повсеместно и на глобальном уровне. IP-протокол может дополнительно передаваться с помощью различных базовых технологий транспортирования на участках доступа и в центральной части страты транспортирования (например, xDSL, ATM, MPLS, ретрансляция кадров, OTN) в соответствии со средой передачи, используемой оператором.

ПРИМЕЧАНИЕ. – Это не мешает операторам предоставлять услуги непосредственно пользователю с применением конкретных технологий (например, ATM, MPLS, ретрансляция кадров, OTN).

Возможности подключения должны предусматривать:

1) использование протоколов IPv4 и IPv6;
2) обеспечение связи в режиме реального времени и не в режиме реального времени;
3) возможность подключения по сценарию "один к одному";
4) возможность подключения по сценарию "один ко многим".

6.2 Режимы связи

Требуется, чтобы сеть СПП поддерживала следующие режимы связи:

– один с одним;

– один со многими;

– многие со многими;

– многие с одним.

6.3 Компоненты транспортной сети

Целью СПП является поддержка услуг и приложений независимо от технологий сети доступа и базовой сети. Таким образом:

1) Требуется, чтобы сеть СПП поддерживала различные технологии, обеспечивающие функции транспортировки доступа и функции базовой транспортировки.

2) Требуется, чтобы страта транспортирования поддерживала возможности установления IP-соединения между функциями конечного пользователя и функциями базовой транспортировки.

3) Требуется, чтобы сеть СПП не препятствовала тому, чтобы сети пользователя имели любой уровень сложности конфигурации.

6.4 Подключение к сети

Применяются следующие требования, касающиеся присоединения к сети:

1) Требуется, чтобы сеть СПП поддерживала регистрацию на уровне сети доступа, инициализацию функций конечного пользователя для доступа к услугам СПП и управление пространством IP-адресов сети доступа, включая функцию NAT.

2) Требуется, чтобы в профиле пользователя содержались данные аутентификации доступа пользователя и сведения, относящиеся к конфигурации доступа к сети.

3) Требуется, чтобы сеть СПП поддерживала перенастройку услуг доступных пользователю в том случае, если пользователь является кочующим и обращается к услугам из места, не являющегося местом подписки. Работа услуг может дополнительно зависеть от одного или от всех далее приведенных факторов: устройства пользователя, сети доступа и соглашений (например, соглашений о роуминге) между поставщиком услуг и поставщиком сети доступа. Требуется, чтобы в сети доступа ресурсы были распределены в соответствии с предоставляемыми услугами.

4) Если сети с многостанционным доступом имеют соединение с одной базовой сетью СПП, требуется, чтобы сеть доступа поддерживала аутентификацию/авторизацию доступа пользователем, посещающим данную сеть доступа в процессе роуминга из другой сети доступа.

5) Для обеспечения гарантированной доступности услуг роуминга требуется, чтобы процедуры подключения к сети доступа СПП поддерживали аутентификацию сети доступа, основанную на стандартизованном методе для идентифицирующего пользователя на уровне сети доступа (например, механизм идентификатора присоединения к сети (NAI), определенный в [b-IETF RFC 2486]).

6.5 Поддержка IPv6

Использование IPv6 обеспечивает не только расширение пространства IP-адресов, но и также различные усовершенствованные характеристики, которые оказываются влияние на функции СПП и соответствующие функциональные объекты. То есть IPv6 обеспечивает также большую гибкость при внедрении новых приложений/услуг за счет использования расширенных заголовков в сочетании с дополнительными возможностями.

Таким образом, в настоящем пункте определяются общие требования к СПП на базе IPv6, на которые оказывают влияние характеристики IPv6. Признано, что СПП на базе IPv6 должна удовлетворять следующим требованиям:

– Требуется, чтобы СПП на базе IPv6 поддерживала расширенные заголовки и дополнительные возможности IPv6.

– Требуется, чтобы СПП на базе IPv6 обеспечивала возможность использования схемы адресации формата IPv6.

6.5.1 Множественная адресация в СПП на базе IPv6

– Требуется, чтобы СПП на базе IPv6 поддерживала возможность множественного доступа для пользователя, включая возможности доступа к сетям доступа с использованием различных технологий (например, сетей подвижной связи, Wi-Fi).

– Требуется, чтобы оконечное оборудование пользователя имело много соединений со многими сетевыми интерфейсами и/или многими адресами IPv6.
– Рекомендуется, чтобы оконечное оборудование пользователя, использующее множественную адресацию на базе IPv6, динамически приобретало (или освобождало) дополнительные адреса IPv6.
– Рекомендуется, чтобы оконечное оборудование пользователя, использующее множественную адресацию на базе IPv6, динамически приобретало (или освобождало) дополнительный(ые) сетевой(ые) интерфейс(ы).
– Требуется, чтобы СПП на базе IPv6 динамически приобретала (или освобождала) дополнительные префиксы IPv6.

6.5.2 Сигнализация в сетях СПП на базе IPv6

1) Требуется, чтобы СПП на базе IPv6 обеспечивала взаимодействие на уровне сигнализации с другими сетями (например, с СПП на базе IPv4).
2) Требуется, чтобы СПП на IPv6 поддерживала сигнализацию, которая бы сводила к минимуму необходимость изменений в протоколы сигнализации, используемые в СПП на базе IPv4.

6.5.3 Переход СПП к СПП на базе IPv6

Требуется, чтобы СПП поддерживала функцию перехода к использованию IPv6 в функциях транспортировки доступа или в функциях базовой транспортировки.

6.6 Поддержка многоадресной передачи

Благодаря этим возможностям приложения могут одновременно доставлять контент многим пользователям.

Помимо возможности одноадресной передачи требуется, чтобы обеспечивалась возможность многоадресной передачи для эффективного использования ресурсов сети и доставки данных с возможностью расширения.

К СПП предъявляются следующие требования:

1) Требуется, чтобы в одном домене СПП обеспечивалась возможность многоадресной передачи.
2) Рекомендуется, чтобы в совокупности доменов СПП обеспечивалась возможность многоадресной передачи.
3) Требуется, чтобы СПП обеспечивала возможность многоадресной доставки данных.
4) Требуется, чтобы СПП обеспечивала возможность управления обслуживанием при многоадресной передаче.
5) Требуется, чтобы СПП обеспечивала возможность управления группой при многоадресной передаче.
6) Требуется, чтобы СПП обеспечивала механизмы обеспечения безопасности для многоадресной передачи.
7) Требуется, чтобы СПП обеспечивала возможность кочевничества при многоадресной передаче сообщений.
8) Рекомендуется, чтобы СПП обеспечивала предварительно установленное качество обслуживания по всей группе при многоадресной передаче и при этом не требовалась поддержка согласования QoS.
9) Рекомендуется, чтобы СПП обеспечивала непрерывную мобильность в режиме многоадресной передачи.
10) СПП может дополнительно обеспечивать надежность групповой передачи.

ПРИМЕЧАНИЕ. – Более подробная информация представлена в [ITU-T Y.2236].

7 Поддержка услуг и приложений

7.1 Открытая среда услуг

7.1.1 Общие требования к открытой среде услуг

Возможности открытой среды услуг проистекают из общих характеристик СПП в части поддержки и формирования среды для создания расширенной, гибкой и открытой услуги и ее предоставления в рамках страты обслуживания.

Реализация новых функциональных возможностей в существующих сетях может быть дополнительно ограничена или невозможна из-за возможностей установленного оборудования. Предоставление программного обеспечения для реализации новых функций в оборудовании определенных поставщиков также ограничено, так как программный интерфейс приложения (API) обычно является чьей-то собственностью (т. е. не открыт).

Требуется, чтобы сети СПП применяли новые возможности и поддерживали широкий спектр новых услуг, включая услуги с улучшенными и комплексными функциональными возможностями. Благодаря усилиям таких третьих лиц, как поставщики приложений и поставщики услуг, направленным на разработку новых приложений и возможностей, доступных через открытые и стандартные интерфейсы, существует все возрастающая потребность объединения усилий поставщиков сетей и поставщиков услуг для разработки стандартных интерфейсов приложение-сеть (ANI). Более того, рекомендуется, чтобы поддерживалась возможность многократного использования программного обеспечения и его переносимость, а также использования коммерческого программного обеспечения для содействия экономически эффективной разработке.

Далее перечислены некоторые общие преимущества открытой среды услуг.

– Приложения и возможности могут легко создаваться поставщиками сетей, а также третьими лицами.
– Возможности можно сделать переносимыми и/или многократно используемыми в различных сетях.
– Открытые и стандартные интерфейсы ANI будут обеспечивать возможность взаимодействия между объектами и приложениями СПП, например для создания услуг.

Требуется, чтобы внутри открытой среды услуг каждая возможность функционировала отдельно или совместно с другими возможностями для реализации приложений. Каждая возможность выполняет для нужного объекта (например, третьего лица) все соответствующие функции услуги. Приложения могут дополнительно предоставляться в разных сетях, поэтому возможности должны быть способны работать независимо от технологий базовых сетей.

Требуется, чтобы СПП удовлетворяли следующим общим требованиям открытой среды услуг:

1) Независимость от поставщиков транспортных сетей. Требуется, чтобы функциональные возможности приложений и услуг, работа с ними эксплуатация и управление ими были независимыми от лежащей в основе инфраструктуры поставщиков транспортных сетей и от технологии сетей.
2) Независимость от производителей. Требуется, чтобы поддерживалась открытая среда услуг, предоставляющая пользователям широкий спектр услуг и приложений в конкурентной среде.
3) Прозрачность местоположения. Требуется, чтобы в распределенной среде поставщики услуг имели доступ к возможностям отовсюду, независимо от реального физического местоположения таких возможностей.
4) Прозрачность сети. Требуется, чтобы среда открытых услуг позволяла приложениям и услугам быть независимыми от технологии или оконечного оборудования.
5) Прозрачность протокола. Требуется, чтобы достигалась прозрачность протокола, с помощью предоставления открытых стандартизованных интерфейсных средств для программирования протокола с целью реализации независимого процесса управления услугами и сокрытия сложных технических деталей сети от открытой среды услуг.
6) Требуется, чтобы безопасный доступ к возможностям открытой среды услуг удовлетворял общим требованиям безопасности СПП, как это определено в пункте 10.

ПРИМЕЧАНИЕ. – Дополнительные требования к поддержке открытой среды услуг представлены в [ITU-T Y.2234].

7.2 Средства подключения услуг

В категории "средства подключения услуг" сгруппированы возможности для обеспечения характеристик конкретных или улучшенных услуг или приложений, и/или возможности для доступа к конкретной информации, предоставленной этими же возможностями, и/или для обработки этой информации.

ПРИМЕЧАНИЕ. – В Дополнении II представлено примерное распределение выбранных услуг по выбранным средствам подключения услуг.

7.2.1 Управление группой

С помощью этой возможности предоставляются функциональные возможности, связанные с надежным и эффективным управлением группами сетевых объектов (оконечным оборудованием, пользователями, сетевыми узлами и т. п.). Она может дополнительно использоваться приложениями и другими услугами в разных целях, включая приложения VPN, распределение видеоконтента, управление устройствами, предоставление и управление услугами и сетью, службы чрезвычайных ситуаций (оповещение общественности) и т. п.

Типичный случай, в котором требуется управление группой, – это услуга VPN, предоставляемая оператором сети. В случае VPN закрытая группа лиц должна быть определена с помощью списка участников – пользователей услугой, и рекомендуется, чтобы связь в пределах этой группы была надежно защищена от других пользователей. Рекомендуется, чтобы сети СПП управляли такими группами и обеспечивали надежную связь в группе.

Другим примером является одновременное распределение видеоконтента с помощью многоадресной передачи от источника ко многим пользователям в группе. Для этого приложения возможность управления группой также важна. К управлению группой предъявляются следующие требования.

1) Требуется, чтобы СПП предоставляла возможность, которая активирует создание групп в страте транспортирования.
2) Требуется, чтобы СПП предоставляла возможность, которая активирует создание группы и/или групп для конкретной услуги (в страте обслуживания).
3) Требуется, чтобы сеть СПП управляла группами и обеспечивала надежную связь в группе.

7.2.2 Управление персональной информацией

Данная возможность обеспечивает управление статической и динамической информацией (конкретного приложения, связанного с пользователем, и с особенностями соединения). Примерами информации конкретного приложения являются контактная информация пользователя, членство в приложении (пароли и т. п.), загрузочные параметры приложения, полоса пропускания/предпочтения QoS (например, в соответствии с имеющимися сетями доступа), предпочтительные среды передачи, конкретные данные пользователя и т. п. Эта информация, доставленная с помощью приложений (например, услуги по уведомлению и информированию) в соответствии с предварительно определенными предпочтениями пользователя и стратегическими атрибутами (например, посредством разных мобильных устройств и типов сетей доступа), может дополнительно накапливаться и управляться от лица пользователей с помощью возможности управления персональной информацией. Возможность управления персональной информацией, выступающая в качестве посредника пользователя по отношению к приложениям, может также дополнительно извлекать эту информацию из приложений от лица пользователей.

Далее следуют требования к возможности управления персональной информацией:

1) Возможность управления персональной информации может предоставляться дополнительно. С помощью возможности управления персональной информацией можно дополнительно собирать статическую и динамическую информацию конкретного приложения от лица пользователей и управлять этой информацией; можно также дополнительно извлекать эту информацию из приложения от лица пользователей.
2) Требуется, чтобы информация, которая управляется возможностью управления персональной информацией, была защищена от несанкционированного доступа/извлечения или действий с ней и пр.
3) Рекомендуется, чтобы с помощью возможности управления персональной информацией поддерживались разные контексты режимов связи.

7.2.3 Обработка сообщений

В современных сетях некоторые услуги поддерживаются в среде как проводной, так и беспроводной передачи, а другие могут быть найдены только в одной из них. Например, услуга передачи коротких сообщений (SMS) была разработана для беспроводных сетей, хотя сейчас ее можно найти в некоторых выделенных сетях, в то время как услуги мгновенной передачи сообщений (IM) были разработаны для проводных сетей, хотя в некоторых мобильных сетях реализованы услуги IM. Результаты, ожидаемые от разных услуг, также отличаются, в том смысле, что некоторые услуги разработаны для использования, как предполагается, в "реальном времени", а другие разработаны, как услуга "почтового ящика", где сообщения накапливаются и готовятся к доставке позднее.

Возможность обработки сообщений обеспечивает функциональные возможности для предоставления услуг, основанных на сообщениях. Такими функциональными возможностями являются управление услугой передачи сообщений в реальном времени и не в реальном времени. Примерами передачи сообщений в реальном времени являются IM и чат, а примерами передачи сообщений не в реальном времени являются электронная почта, SMS и услуга передачи мультимедийных сообщений (MMS).

Далее следуют общие требования.

1) Требуется, чтобы возможность обработки сообщений СПП поддерживала услуги сообщений, доступные как в выделенном оконечном оборудовании, так и в мобильном оконечном оборудовании, предназначенные для использования как в доступе проводного транспорта, так и в доступе беспроводного транспорта.

2) Требуется, чтобы возможность обработки сообщений СПП поддерживала услуги передачи сообщений как в реальном времени, так и не в реальном времени.

ПРИМЕЧАНИЕ. – Возможность управления группой также может быть дополнительно необходима для поддержки услуг передачи сообщений.

Кроме того, существуют требования пользователей, чтобы возможности обработки сообщений обеспечивали характеристики конфигурации применительно к услугам передачи сообщений, таким как выбор, фильтрация, форматирование, управление группой и обработка (например, изолирование массовых незапрашиваемых сообщений электросвязи).

7.2.4 Присутствие

С помощью возможности (услуги) присутствия обеспечивается доступ пользователей и услуг к информации о присутствии, а также доступность этой информации для пользователей и услуг. Присутствие – это набор атрибутов, характеризующих текущие свойства объекта, например состояние, местоположение и т. п.

Объектом в данном случае является любое устройство, услуга, приложение и т. п., способное предоставить информацию о присутствии. Доступность, с другой стороны, обозначает способность и намерение объекта передавать сообщения в соответствии с различными свойствами правилами, связанными с этим объектом – например, времени суток, возможностей устройства, предпочтений и возможностей в отношении среды и т. п. Термины "присутствие" и "доступность" почти всегда используются вместе для предоставления полного набора информации о присутствии.

Требуется, чтобы СПП поддерживала два типа пользователей: тех, кто предоставляет информацию о присутствии (иногда их называют "объектами присутствия" [b-ETSI TR 121.905]), и тех, кто запрашивает информацию о присутствии ("наблюдателей").

Услуга присутствия обеспечивается с помощью трех групп возможностей. Требования для каждой группы возможностей описаны ниже.

Сбор информации о присутствии

1) Требуется, чтобы СПП обеспечивала с разрешения пользователя возможность сбора информации, описывающей состояние соединения объектов присутствия, например устройств(а), используемых(ого) пользователем.

2) Требуется, чтобы СПП обеспечивала возможность сбора информации относительно местоположения объекта присутствия в соответствии с национальными регуляторными положениями и законами.

3) Требуется, чтобы СПП обеспечивала возможность сбора информации относительно мультимедийного контента объекта присутствия.

4) Требуется, чтобы СПП обеспечивала возможность сведения воедино информации о присутствии, поставляемой многими объектами присутствия.

Распространение информации о присутствии

5) Требуется, чтобы СПП обеспечивала для объекта, например пользователя, возможность получения информации о текущем статусе присутствия, которым обладает объект присутствия. Другим примером является использование этой возможности для включения другой услуги, чтобы получить доступ к информации о присутствии пользователей при наличии разрешения со стороны пользователя.

6) Требуется, чтобы СПП обеспечивала возможность распространения информации относительно мультимедийного контента объекта присутствия.

7) Требуется, чтобы СПП обеспечивала возможность отправления массовых уведомлений многим объектам присутствия.

8) Требуется, чтобы СПП распространяла информацию о присутствии в соответствии со временем истечения срока (продолжительности), которое может быть разовым событием или периодом действия.

Управление информацией о присутствии

9) Требуется, чтобы СПП обеспечивала управление информацией о присутствии, то есть набор возможностей для управления собранной информацией о присутствии.

10) Требуется, чтобы управление контролем доступа к информации о присутствии (с использованием возможности распространения информации о присутствии) осуществлялось в соответствии с конфиденциальностью объекта присутствия и требованиями правил доступа.

11) Требуется, чтобы возможности управления информацией о присутствии включали возможность распределения, чтобы при необходимости предоставлялась только часть информации о присутствии.

12) Требуется, чтобы возможности управления информацией о присутствии включали сбор запросов от определенных объектов для получения информации о присутствии в отношении других объектов. Возможности управления присутствием также предоставляют объекту присутствия возможность регулировать распространение его информации о присутствии, например принимать или отклонять запросы в отношении информации о присутствии в зависимости от конкретного наблюдателя.

7.2.5 Управление местоположением

Управление местоположением – это возможность для подключения приложений и услуг, основанных на местоположении, в которых используется информация, касающаяся местоположения пользователей и устройств внутри сетей. Местоположение пользователей и приборов внутри сетей может быть дополнительно связано с их физическим позиционированием и, следовательно, с расширением приложений с учетом местного контекста и соответствия.

Механизмы определения и сообщения информации о местоположении часто зависят от технологии сети доступа. Это значит, что в рамках каждой технологии сети доступа рекомендуется осуществлять поддержку приложений и услуг, основанных на местоположении.

Далее приведены требования для управления определением местоположения.

1) Требуется, чтобы в сетях СПП предоставлялась возможность управления определением местоположения для определения и сообщения информации, относящейся к местоположению пользователей и устройств внутри СПП в соответствии с национальными регуляторными положениями и законами.

2) Требуется, чтобы в СПП должны предоставлялись дополнительные функциональные возможности для подтверждения правильности и аутентичности информации о местоположении, используемой приложениями и услугами, с целью уменьшения любых негативных воздействий, обусловленных искаженной или фальсифицированной информацией о местоположении.

3) Требуется, чтобы при предоставлении услуг и приложений, основанных на местоположении, решались вопросы конфиденциальности.

4) Требуется, чтобы возможность управления определением местоположения предоставляла средство для передачи информации о местоположении, в соответствии с информацией, содержащейся в профилях пользователя/устройства.

7.2.6 Принудительная доставка

Принудительная доставка – это средство подключения услуги, обеспечивающее возможность передачи данных от отправителя к получателю, без предварительного запроса со стороны получателя, например посредством механизма принудительной доставки на основе протокола SIP.

В то время как у пользователя обычно есть возможность конфигурировать услуги принудительной доставки из диапазона услуг, предоставленных поставщиками услуг, получателю нет необходимости делать конкретный запрос на отправку требуемых данных. Вместо этого делается общий запрос. Данные могут отправляться или в результате единичного, связанного с конкретным приложением инициированного вызова или периодически.

В качестве примера можно привести принудительную доставку, которая может дополнительно использоваться для предоставления уведомления о доступности сообщения MMS.

К принудительной доставке предъявляются следующее требование:

1) Требуется, чтобы в СПП поддерживалась возможность принудительной доставки в соответствии с национальными регуляторными положениями и законами.

ПРИМЕЧАНИЕ. – Для вызова услуг принудительной доставки может дополнительно потребоваться согласие пользователя.

7.2.7 Управление устройствами

Управление устройствами – это средство подключения, которое предоставляет сетевые возможности для управления устройствами и их контроля. Возможности управления устройствами могут дополнительно использоваться для:

– управления конфигурацией аппаратного/программного обеспечения, например информацией об аппаратном обеспечении устройств, возможностями среды, версией программного обеспечения;

– дистанционного обновления программного обеспечения как с участием, так и без участия пользователя, например исправления ошибок, функциональных возможностей, операционных систем, встроенных программ, клиентских приложений;

– дистанционной диагностики сбоев.

К управлению устройствами предъявляются следующие общие требования:

1) Требуется, чтобы в СПП поддерживалась модернизация устройств.

2) Требуется, чтобы в СПП поддерживалась автоконфигурация устройств.

3) Требуется, чтобы в СПП поддерживался сбор информации о подсоединении устройств, в соответствии с национальными регуляторными положениями и законами, например адресов IP и местоположения.

4) Управление устройствами может дополнительно предоставлять функции для регистрации, управления и обновления информации об устройствах.

5) Управление устройствами может дополнительно предоставлять функции для удаленной проверки состояния устройств, включая состояние изменений и обновлений, и создание отчетов о диагностике.

6) Требуется, чтобы управление устройствами было безопасным и всегда выполнялось доверенным объектом в соответствии с национальными регуляторными положениями и законами.

ПРИМЕЧАНИЕ 1. – Рекомендуется, чтобы управление устройствами позволяло осуществлять установку предпочтений и приложений пользователя.

ПРИМЕЧАНИЕ 2. – Для вызова услуг управления устройствами, как правило, требуется согласие пользователя.

7.2.8 Обработка сеанса

Требуется, чтобы в СПП предоставлялись возможности установки, управления и завершения сквозной услуги сеансов, которые включают в себя, например, множество участников, группу конечных точек, связанную с этими участниками, и описание мультимедийных соединений между этими конечными точками. Такие возможности обработки сеанса должны предоставляться как в фиксированной, так и в подвижной среде, для того чтобы учесть требования различных услуг, а также использовать для работы услуг соответствующие серверы приложений.

В функции обработки сеанса входит следующее:

– создание сеанса;

– представление идентификатора исходящей стороны и подключающейся стороны сеанса;

– подавление идентификатора исходящей стороны и подключающейся стороны сеанса;

– доставка и подавление дополнительной информации, предоставленной пользователем, например изображения, видеоданных или текста во время создания сеанса;

– обработка входящего сеанса связи завершающей стороной;

– согласование возможностей входящего сеанса;

– принятие, игнорирование, перенаправление или отклонение входящего сеанса;

– согласование среды передачи и компонентов среды передачи во время создания сеанса;

– обработка текущего сеанса;

– изменение среды передачи и компонентов среды передачи в текущем сеансе;

– приостановка и возобновление текущего сеанса;

– окончание сеанса;

– завершение сеанса под управлением сети.

К обработке сеанса предъявляются следующие общие требования:

1) Требуется, чтобы при обработке сеанса существовала возможность использования для работы услуги соответствующих серверов приложений.

2) Требуется, чтобы сеть СПП обеспечивала пользователю возможность создавать один или несколько сеансов и активировать сопутствующие мультимедийные приложения в каждом сеансе.

3) Требуется, чтобы в процессе обработки сеанса поддерживались сеансы с различными типами среды передачи (голос, видео, текст).

4) Требуется, чтобы поддерживался контроль допуска сеанса, основанный на определенных уровнях QoS и безопасности.

5) Требуется, чтобы механизмы контроля допуска сеанса охватывали много видов услуг, (например, передачу голоса, текста, видео).

6) Если в сеансе заняты один или два участника, то требуется, чтобы сеть оканчивала сеанс в любое время в течение сеанса по запросу любого из пользователей сеанса. Сеть может дополнительно окончить сеанс в любое время в течение сеанса связи (например, при сбое).

7) Если в сеансе занято более двух участников, сеть может дополнительно окончить сеанс в любое время в течение сеанса по запросу любого из пользователей сеанса. Сеть может дополнительно окончить сеанс в любое время в течение сеанса (например, при сбое).

7.2.9 Поддержка приложений на базе веб-сети

Средство подключения поддержки приложений на базе веб-сети дает возможность улучшенного использования возможностей устройств и характеристик сетей для приложений на базе веб-сети.

Возможности поддержки приложений на базе веб-сети предоставляют пользователям согласованную веб-среду, которая объединяет множество сетевых сред и множество устройств (ПК, портативный компьютер, PDA, сотовый телефон и т. п.).

Поддержка приложений на базе веб-сети включает следующие виды взаимодействия:

– от сервера (приложений) к серверу;

– от сервера к оконечному оборудованию;

– от оконечного оборудования к серверу;

– от оконечного оборудования к оконечному оборудованию (или одноранговое взаимодействие).

Требуется, чтобы СПП поддерживала приложения на базе веб-сети, соблюдая следующие требования:

1) функциональная совместимость в проводных и беспроводных сетевых средах;

2) безопасный доступ к приложениям;

3) кочевничество;

4) небольшое время запаздывания и эффективное использование пропускной способности.

Рекомендуется, чтобы сеть СПП поддерживала приложения на базе веб-сети, соблюдая следующие требования:

5) многократное использование существующих технологий и компонентов СПП (например, аутентификации) для предоставления приложений на базе веб-сети;

6) многократное использование средств разработки и интеграции;

7) согласованный опыт пользователя по сетям;

8) поддержка методов построения услуг;

9) масштабируемость приложений на базе веб-сети;

10) неснижаемая надежность СПП.

ПРИМЕЧАНИЕ. – СПП могут дополнительно ограничиваться в отношении возможностей поддержки приложений на базе веб-сети.

7.2.10 Синхронизация данных

Синхронизация данных определяется как процесс установления эквивалентности двух наборов данных. Средство подключения услуги по синхронизации данных синхронизирует передаваемые по сети данные от разного оконечного оборудования, включая портативные компьютеры, мобильные телефоны, портативные и настольные компьютеры. Приложения, в которых может дополнительно использоваться средство подключения услуги по синхронизации данных, включают в себя календарь, управление контактной информацией, управление данными предприятия, накопленными в базах данных, и управление веб-документами.

Рекомендуется, чтобы в СПП обеспечивалось средство подключения услуги по синхронизации данных со следующими характеристиками:

1) синхронизация передаваемых по сети данных с оконечным оборудованием, поддерживающим эту возможность;
2) синхронизация оконечного оборудования с соответствующими передаваемыми по сети данными;
3) синхронизация передаваемых по сети данных среди оконечного оборудования.

Если обеспечивается средство подключение услуги по синхронизации данных, то применяются следующие требования:

1) Требуется, чтобы средство подключения услуги по синхронизации не зависело от транспортных протоколов.
2) Требуется, чтобы поддерживались произвольные данные, передаваемые по сети.
3) Рекомендуется, чтобы при синхронизации обеспечивалось наличие информации об ограниченности ресурсов оконечного оборудования.

7.3 Информированность о контексте

Информированность о контексте представляет собой возможность определять любую последующую операцию в процессе электросвязи или ином процессе, а также влиять на эту операцию путем обращения к статусу соответствующих объектов, которые формируют согласованную среду, составляющую контекст. Статусы отдельных объектов и их агрегированный статус считаются информацией о контексте. Примерами информации о контексте являются соединение абонента, местоположение отмеченных товаров в системе распространения и статус трафика в сети.

Предусматриваются следующие ключевые роли:

- **Генератор информации о контексте**: Создает информацию о контексте и разрешает доступ к ней. Генератор контекста может находиться в самой СПП или за ее пределами.
- **Запросчик информации о контексте**: Запрашивает информацию о контексте и обращается к ней. Он может находиться в самой СПП или за ее пределами.
- **Распространитель информации о контексте**: Осуществляет сбор, распространение, обработку и дополнительное хранение информации о контексте, выступая в качестве посредника между генератором и запросчиком информации о контексте.

Если указанные выше роли выполняются СПП, то рекомендуется, чтобы СПП обеспечивала выполнение следующих требований:

1) Безопасность информации о контексте с точки зрения генератора информации о контексте:
   - Требуется, чтобы информация о контексте могла быть доступна запросчику(ам) информации о контексте только тогда, когда это разрешает генератор. Требуется, чтобы выполнение данного правила обеспечивалось до тех пор, пока информация о контексте сохраняется в СПП.
   - Требуется, чтобы запрещалось ненамеренное отслеживание в отношении генератора информации о контексте.

     ПРИМЕЧАНИЕ. – Настоящим требованием предусматривается ситуация, когда информация о контексте, создаваемая генератором, открыта различным запросчикам информации о контексте для разных целей. Сюда следует отнести только намеренное использование. Например, несмотря на то что генератор информации о контексте допускает открытие его/ее истории покупок книг (для получения информации о возможных новых выпусках), требуется запретить, чтобы данная информация была доступной другим приложениям, например для распространения рекламы, касающейся билетов в кино, музыкальных дисков или спортивной одежды.
   - Требуется, чтобы в СПП обеспечивалось отсутствие утечки или неправильного использования информации о контексте в процессе распространения информации о контексте.
   - Требуется, чтобы в СПП обеспечивалось отсутствие утечки или неправильного использования информации о контексте, которая хранится в базе данных.

2) Надежность информации о контексте с точки зрения запросчика информации о контексте:
   - Рекомендуется, чтобы информация о контексте прозрачно передавалась запросчику, не подвергаясь изменению.
   - Рекомендуется, чтобы запросчику информации о контексте передавалась самая последняя информация о контексте.
   - Желательно, чтобы старая информация о контексте автоматически прекращала использоваться.
   - Требуется, чтобы ложная информация о контексте не была ни создана, ни открыта.
3) Простое использование информации, которая должна храниться, с точки зрения запросчика информации о контексте/поставщика приложения:
   - Рекомендуется, чтобы формат и семантика данных, составляющих информацию о контексте, были стандартизованы, с тем чтобы их могли использовать различные запросчики информации о контексте/поставщики приложений.
   - Рекомендуется, чтобы запросчик информации о контексте мог легко находить ее, если это разрешено.
   - Рекомендуется, чтобы запросчик информации о контексте мог использовать ее в любое время, если это разрешено.
   - Первичная информация о контексте может дополнительно быть преобразована в нужную информацию о контексте, с тем чтобы любой поставщик приложений мог свободно разрабатывать любое приложение путем использования преобразованной информации о контексте.
   - Распространитель информации о контексте может дополнительно иметь возможность автоматического выбора элементов услуги и данных из многих возможных вариантов, с тем чтобы внешние разработчики приложений могли свободно разрабатывать любые приложения путем использования информации о контексте.
4) Информация о контексте должна передаваться в реальном времени и на основании запроса, если того пожелает запросчик информации о контексте.
5) Масштабируемость распространителя информации о контексте:
   - Рекомендуется, чтобы обрабатывалось большое количество информации о контексте, с тем чтобы не допускалось получения ложных выводов в связи с ограниченностью информации о контексте.
   - Рекомендуется, чтобы распространитель информации о контексте обладал гибкостью, с тем чтобы обрабатывать различные виды информации о контексте и поддерживать различные приложения.
6) Эффективное распространение информации о контексте.

8 Маршрутизация

Требуется, чтобы в сети СПП представлялись возможности выбора нужного пути маршрутизации между конечной точкой, формирующей исходящий трафик, и конечной точкой, получающей трафик.

Требуется, чтобы в СПП поддерживались схемы маршрутизации, наиболее подходящие для поставщиков услуг СПП. В частности, требуется, чтобы сеть СПП поддерживала:

1) как статические, так и динамические схемы маршрутизации;
2) схемы маршрутизации, которые могут эффективно работать в пределах домена сети СПП;
3) схемы маршрутизации, которые могут эффективно работать между доменами сети СПП, обеспечивая, таким образом, взаимодействие;
4) маршрутизацию на основе диапазона номеров, указанного в ITU-T E.164.

Рекомендуется, чтобы СПП поддерживала:

5) маршрутизацию на основе информации о контексте (например, маршрутизацию на основе присутствия, местоположения и персональной информации).

ПРИМЕЧАНИЕ. – В пункте 7.3 представлена дополнительная информация, касающаяся информированности о контексте.

9 Качество обслуживания

Для того чтобы обеспечить пользователям или приложениям требуемый уровень обслуживания, требуется, чтобы в сети СПП поддерживалось сквозное QoS при передаче через различные сети с различными технологиями инфраструктуры, которые предоставляются множеством операторов. Требуется, чтобы в СПП поддерживалось много уровней QoS, которые могут дополнительно согласовываться между пользователем и поставщиком услуг, либо между поставщиками услуг. В поддержку уровня обслуживания QoS входит использование механизмов управления ресурсами и допуском, разграничение классов трафика, управление установлением приоритетов, механизмы сигнализации QoS, измерение и управление рабочими характеристиками для обеспечения гарантии качества и управление перегрузками/избыточной нагрузкой.

9.1 Общие требования к QoS

Требуется, чтобы сеть СПП удовлетворяла следующим требованиям к QoS:

1) Допускала использование различных технологий и бизнес-моделей.
2) Поддерживала различные процессы, относящиеся к жизненному циклу услуги, например абонентскую подписку/предоставление услуг, вызов функций, мониторинг.
3) Поддерживала различные функциональные возможности оконечного оборудования, например некоторые виды оконечного оборудования могут поддерживать сигнализацию QoS в страте транспортирования, а другие – нет.
4) Управляла транспортными ресурсами, относящимися к QoS, в пределах сетей с пакетной коммутацией и на границах сети в соответствии с их функциональными возможностями, см. [ITU-T Y.2111].
5) Поддерживала управление ресурсами и допуском в пределах отдельного домена СПП и между доменами СПП.
6) Поддерживала как относительное, так и абсолютное управление QoS, см. [ITU-T Y.2111].
7) Поддерживала управляемые приложениями требования к QoS.
8) Проверяла наличие транспортных ресурсов на основе сквозного соединения, см. [ITUT Y.2111].
9) Обеспечивала установление различий в QoS для разных категорий пакетного трафика, включая пакетные потоки и пользовательские обозначения, см. [ITU-T Y.2111].
10) Осуществляла авторизацию запросов в отношении QoS и работала только с авторизованными запросами в отношении QoS, см. [ITU-T Y.2111].
11) Поддерживала динамическое управление NAPT на ближнем конце и выбор режима работы брандмауэра, см. [ITU-T Y.2111].
12) Поддерживала (дистанционный) обход NAT на дальнем конце, см. [ITU-T Y.2111].
13) Обеспечивала управление ресурсами и допуском при многоадресной передаче для поддержки, например IPTV, см. [ITU-T Y.2111].
14) Обеспечивала управление ресурсами и допуском для поддержки кочевничества, см. [ITU-T Y.2111].

9.2 Классы QoS в сети

1) Рекомендуется, чтобы сеть СПП учитывала рабочие характеристики сети в страте транспортирования.
2) Рекомендуется, чтобы сеть СПП поддерживала классы QoS сети СПП, основанные на [ITU-T Y.1541].

9.3 Приоритет услуг/приложений

Рекомендуется, чтобы сеть СПП обеспечивала следующие приоритеты услуг/приложений:

1) схемы классификации приоритетов для управления допуском и восстановления;
2) расширения сигнализации, указывающие уровни приоритетов на интерфейсах UNI, NNI и ANI;
3) механизмы поддержки приоритета, которые выполняют действие с желаемым уровнем приоритета.

9.4 Управление QoS

Рекомендуется, чтобы сеть СПП поддерживала:

1) степень детализации управления QoS на уровне потока, сеанса, класса обслуживания;
2) динамические характеристики QoS (то есть, рекомендуется, чтобы была возможность изменения атрибутов QoS во время активного сеанса связи);
3) управление ресурсами QoS, основанное на распределенном, централизованном или смешанном подходе;
4) механизмы управления допуском и перегрузками;
5) механизмы, обеспечивающие гарантированную своевременную и надежную доставку пакетов сигнализации и управляющих пакетов;
6) механизмы для назначения приоритетов доставки для электросвязи в чрезвычайных ситуациях и приоритетной электросвязи;
7) методы управления допуском на основе ресурсов, например, с использованием информации об измеренных качественных показателях.

9.5 Сигнализация QoS

Рекомендуется, чтобы сеть СПП использовала механизмы сигнализации для поддержки QoS.

Более подробные требования к сигнализации QoS выходят за рамки данной Рекомендации и содержатся в других особых Рекомендациях.

9.6 Качественные показатели

Для обеспечения гарантированного QoS требуется, чтобы в СПП поддерживалось измерение качественных показателей и управление ими.

Рекомендуется, чтобы при измерении качественных показателей и управление ими обеспечивалось следующее:

1) гарантированное обеспечение поставщиком услуг качественных показателей (для сравнения с SLA);
2) предоставление информации о качественных показателях поставщиками услуг предполагаемым пользователям;
3) устранение поставщиками услуг неисправностей в сетях в пределах определенных маршрутов;
4) предоставление поставщиками услуг сообщений о влиянии на качественные показатели изменений, произошедших в пределах их сетей;
5) взаимное наблюдение поставщиками за рабочими характеристиками сетей друг друга;
6) предоставление информации для других функций СПП, например RACF.

Более подробные требования для измерения качественных показателей и управления находятся вне области применения данной Рекомендации и содержатся в других конкретных Рекомендациях.

9.7 Обработка и управление трафиком

Во избежание обработки и перегрузки трафика и для удержания времени отклика достаточно низким при таких перегрузках, с целью предотвращения отказа пользователей от сделанных ими запросов на обслуживание рекомендуется, чтобы в СПП представлялись механизмы для обнаружения перегрузок и управления ими (включая такие расширенные элементы управления, как балансировка нагрузки и репликация ресурса) как в страте обслуживания, так и в страте транспортирования.

Рекомендуется, чтобы в СПП существовали механизмы управления перегрузкой, которые:

1) передают в другие сети данные об условиях перегрузки и степени перегрузки;
2) оптимизируют эффективную пропускную способность перегруженного ресурса (например, допустимое количество запросов на услугу/сек или пакетов/сек) с учетом приоритета обслуживания;
3) обеспечивают наличие такой пропускной способности на протяжении всего события перегрузки вне зависимости от пропускной способности перегруженного ресурса или количества источников перегрузки;
4) позволяют сети, которая получает сообщение о перегрузке, управлять своим трафиком.

10 Идентификация и безопасность

ПРИМЕЧАНИЕ. – Использование в настоящем пункте термина "идентичность" не указывает на его абсолютное значение. В частности, использование термина не означает какой-либо положительной валидации того или иного лица.

10.1 Общие требования к идентификации, аутентификации и авторизации

Требования, представленные в данном пункте, не привязаны к какому либо определенному набору услуг или приложений сети СПП.

ПРИМЕЧАНИЕ 1. – Конкретные механизмы аутентификации и авторизации выходят за рамки данной Рекомендации.

Существуют требования для возможностей двусторонней идентификации, аутентификации и авторизации как в страте транспортирования, так и в страте обслуживания. В страте транспортирования существуют требования по использованию транспортных ресурсов сети СПП. Требования для страты обслуживания касаются взаимосвязи между пользователем и услугой или между пользователем и другим пользователем, включая случай, когда эти два пользователя находятся в разных сетях СПП.

ПРИМЕЧАНИЕ 2. – Иногда фраза "поставщик услуг" используется для ссылки на поставщика услуг страты транспортирования. В данном подпункте, поставщик сетевых услуг обычно сокращается до "СПП", а "поставщик услуг" называется именно так "поставщиком услуг"; поставщик услуг может находиться в любом месте, и он не обязательно является поставщиком сетевых услуг.

Далее приведены общие требования для возможностей идентификации, аутентификации и авторизации.

1) Требуется, чтобы в СПП поддерживались функции двусторонней аутентификации и авторизации, как в страте транспортирования, так и в страте обслуживания. Для аутентификации в страте транспортирования требуется, чтобы пользователь был идентифицирован сетью для получения доступа к сети и привилегированному использованию. Функция аутентификации может являться важным фактором защиты от несанкционированного использования сетей, например для предотвращения массовых незапрашиваемых сообщений электросвязи. С помощью функции авторизации можно установить доступ к сетевым ресурсам и предотвратить нарушение прав доступа.

2) Требуется, чтобы сеть СПП однозначно идентифицировала пользователя с помощью одного или двух из следующих типов идентификатора пользователя:
   - открытый идентификатор пользователя: Информация, которая обычно используется одним пользователем СПП для соединения или общения с другим пользователем СПП;
   - секретный идентификатор пользователя: Секретный идентификатор пользователя СПП может использоваться для идентификации пользователя СПП в его/ее сети СПП или у поставщика услуг. Секретный идентификатор пользователя является единственным компонентом, используемым для аутентификации.

3) Требуется, чтобы в СПП поддерживалась раздельная идентификация, аутентификация и санкционирование пользователей и оконечного оборудования.

4) Требуется, чтобы в СПП для некоторых определенных услуг поддерживалась верификация взаимосвязи между пользователем и оконечным оборудованием пользователя.

5) Рекомендуется, чтобы аутентификация, санкционирование и учет, выполняемые поставщиком услуг СПП и поставщиком услуг, осуществлялись в защищенном режиме.

6) Требуется, чтобы поставщик услуг предоставлял механизмы, которые обеспечивают отображение открытого идентификатора инициатора связи там, где это необходимо и где разрешено.

7) Требуется, чтобы поставщиком услуг должны быть представлены механизмы, которые обеспечивают скрытие открытого идентификатора инициатора связи, если отображение данных сведений ограничено инициатором связи или сетью.

8) Требуется, чтобы поставщик услуг, выполняющий аутентификацию, предоставлял механизмы для определения достоверности представленного открытого идентификатора пользователя для входящей связи.

9) Требуется, чтобы поставщик услуг, выполняющий аутентификацию, поддерживал механизмы, обеспечивающие предоставление открытого идентификатора пользователя

подключенной стороны инициатору сеанса связи, если это необходимо и не наложено ограничений подключенной стороной или сетью.

10) Требуется, чтобы СПП поддерживалась возможность проверки секретных идентификаторов пользователей и оконечного оборудования (при необходимости). Дополнительно должна поддерживаться возможность проверки аутентификации и авторизации пользователей и оконечного оборудования для использования ресурсов СПП.

11) Требуется, чтобы поставщик услуг имел возможность проверки секретных идентификаторов тех пользователей, которым предоставляются услуги. Дополнительно требуется, чтобы поставщик услуг поддерживал возможность проверки аутентификации и авторизации пользователей для использования ресурсов, которыми он управляет.

12) Требуется, чтобы соответствующий поставщик услуг сети управлял секретными и открытыми идентификаторами (идентификаторы, которые используются для аутентификации и авторизации) пользователей СПП, использующих ресурсы страты транспортирования.

13) Требуется, чтобы соответствующий поставщик услуг управлял секретными и открытыми идентификаторами (идентификаторы, которые используются для аутентификации, авторизации и маршрутизации) пользователей услуг, использующих ресурсы страты обслуживания, и требуется, чтобы такое управление предотвращало возможность несанкционированного изменения пользователями открытых и секретных идентификаторов.

14) Требуется, чтобы секретные идентификаторы пользователя СПП, предоставляемые для аутентификации/авторизации, не были видны другим пользователям.

15) Открытые идентификаторы пользователя услуг СПП могут быть дополнительно видны другим пользователям, если в процесс взаимодействия не включены промежуточные услуги и имеется разрешение пользователя.

16) Поставщик услуг может дополнительно разрешить пользователю использовать для доступа к услуге один и тот же открытый или секретный идентификатор пользователя параллельно с несколькими видами оконечного оборудования.

17) Так как одному пользователю может быть дополнительно разрешено использовать несколько секретных идентификаторов пользователя, введенных в процессе одной процедуры подписки, требуется, чтобы сеть СПП поддерживала использование множества секретных идентификаторов пользователя в одной процедуре подписки.

18) СПП может дополнительно позволить аутентификацию и авторизацию отдельного пользователя для ее использования в работе с множеством услуг ("однократная регистрация входа").

ПРИМЕЧАНИЕ 3. – Даже в тех случаях, когда требуется выполнение только однократной аутентификации, может дополнительно оставаться потребность в выполнении многократных авторизаций. Кроме того, выполнение однократного входа может быть реализовано на стороне клиента, чтобы даже если требуется многократное выполнение аутентификации, пользователю необходимо всего лишь один раз установить взаимоотношение аутентификации. Сеть СПП не должна поддерживать возможности однократной регистрации. Однако там, где такая поддержка осуществляется существующими технологиями, ожидается, что она также будет использоваться для СПП.

Аутентификация идентификатора абонента или пользователя не предназначена для указания на положительную валидацию того или иного лица.

10.2 Требования к идентификации

Сети СПП представляют возможности для идентификации пользователей, позволяющие операторам сети и поставщикам услуг идентифицировать пользователей определенных услуг СПП и при необходимости использовать данные сведения (например, для процедур аутентификации и авторизации). Требуется, чтобы сети СПП обеспечивали возможности пользователям для идентификации поставщика (на каждой страте), где существует взаимосвязь.

К возможности идентификации предъявляются следующие требования:

1) Использование нескольких идентификаторов пользователя.

Так как пользователь СПП может дополнительно иметь несколько открытых и секретных идентификаторов, требуется, чтобы сеть СПП отличала один идентификатор от другого (например, для личного использования и для использования в бизнесе).

2) Переносимость идентификатора.

Требуется, чтобы сеть СПП предоставляла возможности, эквивалентные переносимости номера в средах КТСОП.

3) Независимость идентификатора.

Рекомендуется, чтобы открытый идентификатор пользователя присваивался пользователю независимо от места хранения, оконечного оборудования пользователя и базовых сетевых технологий. Однако обратная совместимость (например, для телефонных трубок КТСОП) может быть дополнительно достигнута с помощью соответствующих функций взаимодействия.

4) Поддержка атрибутов идентификатора.

Такие атрибуты секретного идентификатора, как время жизни данного идентификатора для пользователя, абонента, используемой сети и т. п., могут быть дополнительно связаны с идентификатором пользователя.

5) Поддержка условий атрибута.

Условия для атрибута того или иного пользователя (например, установка таймера в качестве условий достоверности) могут быть дополнительно связаны с идентификатором пользователя у поставщика атрибута (например, сети, главного пользователя, участником, конечным пользователем).

6) Выборочная санкционирование атрибута.

Требуется, чтобы сеть СПП поддерживала выборочную авторизацию сведений атрибута секретного идентификатора пользователя поставщиком атрибута (например, время жизни идентификатора).

7) Поддержка программирования со стороны абонента.

Рекомендуется, чтобы сеть СПП поддерживала программирование абонентом различных разрешений для различных данных атрибута, например использование и доступ к сведениям атрибута секретного идентификатора для каждого атрибута.

8) Привязка пользователя к оконечному оборудованию.

Требуется, чтобы в СПП для определенных услуг поддерживалась динамическая привязка открытого идентификатора пользователя к идентификатору оконечного оборудования.

9) Взаимосвязи с несколькими видами оконечного оборудования.

Требуется, чтобы сеть СПП допускала взаимосвязь открытого или секретного идентификатора пользователя с несколькими (подвижными или фиксированными) идентификаторами оконечного оборудования для определенных услуг. Пользователю может дополнительно быть разрешено использование нескольких видов оконечного оборудования в любое время.

10) Передача сведений идентификатора.

Требуется, чтобы сеть СПП поддерживала передачу сведений идентификатора пользователя пользователями СПП, если было получено разрешение от устройства ввода, поддерживающего пользователя, или на своем оконечном оборудовании или на принимающем данные оконечном оборудовании для определенных услуг (например, оконечного оборудования пункта продажи).

11) Администрирование открытого идентификатора пользователя.

Требуется, чтобы оператор сети осуществлял администрирование открытого идентификатора пользователя. Требуется, чтобы открытый идентификатор пользователя не мог изменяться его пользователем.

12) Аутентичность открытого идентификатора пользователя.

Требуется, чтобы оператор сети обеспечивал гарантированную аутентичность открытого идентификатора пользователя, представляемого пользователю на входящем сеансе, в случае если связь полностью осуществляется в доверенной сети.

10.3 Требования к аутентификации

Аутентификация является процессом установления доверия к идентификаторам пользователя и оконечного оборудования, а так же к предложениям по присоединению сети и предоставлению услуг. С точки зрения поставщиков, в СПП могут дополнительно быть отличия между аутентификацией транспортной сети и аутентификацией услуги. С точки зрения абонентов, в СПП могут дополнительно быть отличия между аутентификацией пользователя и аутентификацией оконечного оборудования. Сетевая аутентификация является процессом проверки идентификаторов пользователя/оконечного оборудования для доступа к сети, который выполняется только поставщиками сетевых услуг. Аутентификация услуги отвечает за проверку идентификаторов пользователя/оконечного оборудования для использования услуги. С точки зрения абонентов

требуется, чтобы сеть предоставляла пользователям возможность аутентификации и идентификации поставщика транспортной сети.

С точки зрения абонентов требуется, чтобы сеть также предоставляла пользователям возможность аутентификации и идентификации поставщика услуг.

Требуется, чтобы сеть СПП обеспечивала независимость данных возможностей.

Эти различные концепции аутентификации могут дополнительно быть объединены в единую концепцию или применяться раздельно, в зависимости от технологии транспортирования или модели бизнеса. Например, если поставщик сети также является поставщиком услуг, то может дополнительно обрабатываться один поток аутентификации.

К возможностям аутентификации предъявляются следующие требования:

1) Требуется, чтобы в СПП поддерживались различные механизмы сетевой аутентификации в соответствии с базовыми технологиями сети доступа.

2) Рекомендуется, чтобы аутентификация услуги по мере возможности была не зависимой от технологий сетей доступа к СПП и поддерживался совместимый механизм аутентификации услуги.

3) Требуется, чтобы в СПП была возможность выполнения запроса к пользователю/оконечному оборудованию на ввод данных аутентификации, либо в явной или неявной форме.

4) Рекомендуется, чтобы в СПП поддерживались как программные, так и аппаратные механизмы аутентификации.

5) Требуется, чтобы поддерживалась аутентификация оконечного оборудования, в которой используются данные профиля устройства.

6) Рекомендуется, чтобы в СПП были представлены возможности взаимной аутентификации между поставщиком услуг и пользователем.

7) Рекомендуется, чтобы в СПП были представлены возможности взаимной аутентификации между поставщиком транспортной сети и пользователем.

10.4 Требования к авторизации

К возможностям авторизации предъявляются следующие требования:

1) Требуется, чтобы доступ к услуге в СПП предоставлялся аутентифицированным пользователям и/или устройствам, на основе предоставленных им прав доступа, профилей пользователей и сетевой политики.

2) Рекомендуется, чтобы санкционирование услуги по мере возможности была независимой от технологий сетей доступа к СПП.

3) Рекомендуется, чтобы там, где это применимо, санкционирование поддерживала сценарии мобильности СПП.

10.5 Управление определением идентичности

1) Требуется, чтобы в сети СПП обеспечивался структурированный подход к управлению определением идентичности (IdM) в отношении идентичности (идентичностей) объектов (включая соответствующую информацию, например идентификаторы, атрибуты, утверждения и политику), таких как:

   a) пользователи/группы;

   b) организации/федерации/предприятия/поставщики услуг;

   c) устройства/сетевые элементы/системы;

   d) объекты (прикладные процессы, контент, данные).

2) Требуется, чтобы в сети СПП поддерживались возможности IdM, которые позволяют:

   a) безопасное управление жизненным циклом (например, регистрацией, валидацией, отменой) идентичности (идентичностей) того или иного объекта;

b) безопасное обнаружение и обмен информацией об идентичности, связанной с идентичностью (идентичностями) того или иного объекта. Сюда относится обнаружение и обмен информацией, которая может дополнительно быть размещена внутри домена СПП и в пределах различных доменов СПП.

3) Требуется, чтобы в сети СПП поддерживалась возможность по обеспечению выполнения применимой политики, связанной с идентичностью того или иного объекта, либо с информацией об идентичности.

4) Требуется, чтобы в сети СПП поддерживались возможности общего управления определением идентичности, которые должны использоваться многими услугами и приложениями, включая:

a) услуги связи в реальном времени (например, VoIP, линейное телевидение и услуги по передаче сообщений в реальном времени);

b) другие услуги связи (например, транзакции на базе веб).

5) Требуется, чтобы в сети СПП поддерживались возможности IdM, позволяющие анонимно утверждать информацию об идентичности, при условии соблюдения применимой политики.

6) Требуется, чтобы в сети СПП поддерживались возможности IdM, позволяющие взаимодействовать сетевым элементам внутри домена СПП (т. е. в интрасети) и в пределах совокупности различных доменов СПП или федераций. Для этого требуется, чтобы:

a) использовались стандартные интерфейсы для обмена информацией для IdM;

b) использовались стандартные механизмы (например, протоколы, структуры и схемы данных) обмена данными для IdM.

7) Требуется, чтобы в сети СПП поддерживались возможности IdM, обеспечивающие конечным пользователям удобные свойства, например:

a) единый вход/выход для пользования многими услугами и приложениями;

b) конвергенция фиксированной и подвижной связи;

c) управление информацией, позволяющей установить личность (PII), и защита этой информации.

8) Требуется, чтобы в сети СПП поддерживались возможности, обеспечивающие защиту услуг и приложений.

9) Требуется, чтобы в сети СПП обеспечивалась безопасность возможностей, функций, данных и связи для IdM.

10.6 Требования к безопасности

Требуется, чтобы в СПП содержались функции безопасности, используемые в существующих сетях и позволяющие выполнять защищенное присоединение к другим сетям СПП или не СПП. Эти требования основаны на применении для СПП [ITU-T X.805] и поэтому сводятся к следующим аспектам безопасности СПП: управлению доступом, аутентификации, сохранности данных, конфиденциальности данных, безопасности связи, целостности данных, готовности к работе и защите персональной информации.

Требуется, чтобы сеть СПП обеспечивала следующее:

1) защиту от несанкционированного использования сетевых ресурсов и несанкционированного доступа к информационным потокам и приложениям;

2) аутентификацию подлинности объектов связи, если это требуется политикой;

3) механизмы, обеспечивающие конфиденциальность данных;

4) механизмы, обеспечивающие целостность данных;

5) средства для ведения отчетности, в соответствии с которыми лицо признается ответственным за любые выполненные им действия;

6) готовность к работе и доступность сети при обращении авторизованного объекта;

7) механизмы сохранности данных для предотвращения ложного отказа одним из объектов или сторон, участвующих в передаче информации, от принятия полного или частичного участия в процессе передачи информации;

8) конфиденциальность данных пользователя, например настроек, профилей, сведений о присутствии пользователя в сети, данных о доступности и расположении. Эти сведения должны быть защищены так, чтобы информация была доступной, только когда обеспечена правильная санкционирование;

9) защиту для сведения к минимуму влияния(й) сетевых атак изнутри сети или снаружи.

10.7 Защита важнейшей инфраструктуры

Рекомендуется, чтобы поставщики услуг имели возможность защитить свои инфраструктуры СПП от злонамеренных атак, таких как отказ в обслуживании, перехват, получение доступа обманным путем, тайные действия с сообщениями (модификация, задержка, удаление, вмешательство, воспроизведение, изменение маршрута, неправильный маршрут или неправильный порядок сообщений), отказ от факта получения или отправления сообщения или подлог. В защиту может дополнительно входить предупреждение, обнаружение и восстановление после атаки, а также меры по предотвращению перерывов в обслуживании.

Требования к безопасности предоставлены в пункте 10.6.

11 Управление

Возможности управления СПП поддерживают области управления, которые охватывают планирование, установку, эксплуатацию, администрирование, техническое обслуживание и предоставление сетей и услуг. Целью высокого уровня является предоставление живучих и рентабельных сетей.

Возможностями управления СПП также поддерживаются услуги мониторинга и управления услугами СПП и транспортными компонентами, за счет передачи управляющей информации через интерфейсы между компонентами СПП и системами управления, между вспомогательными системами управления СПП, а также между компонентами СПП и персоналом поставщиков сетевых услуг и поставщиков услуг.

Возможности управления СПП выполняют задачи СПП с помощью:

1) предоставления возможности управления на протяжении всего жизненного цикла компонентов СПП, как физических, так и логических. Сюда входят ресурсы в страте транспортирования и в страте обслуживания, функции доступа к транспортировке, взаимосвязанные компоненты, сети пользователей и оконечное оборудование;

2) предоставления возможности управления компонентами услуг СПП независимо от основополагающих транспортных компонентов СПП, и позволяя организациям, предоставляющим услуги СПП, создавать для клиентов различные услуги (возможно, из услуг от различных поставщиков);

3) предоставления возможностей управления, которые позволяют организациям, предоставляющим услуги СПП, дать своим пользователям возможность персонализации услуг и создания новых услуг из различных возможностей СПП (от различных поставщиков услуг);

4) предоставления возможностей управления, которые позволяют организациям, предлагающим услуги СПП, добавить к ним улучшения, включая самообслуживание со стороны пользователя, например предоставление услуги, сообщения о сбоях, онлайновые отчеты о выставлении счетов);

5) разработки архитектуры управления и услуг управления, которые позволят поставщикам услуг уменьшить время, необходимое для разработки, создания и доставки новых услуг;

6) поддержки безопасности информации управления, включая информацию о клиенте и информацию пользователя;

7) поддержки доступности услуг управления в любом месте, в любое время и для любой зарегистрированной организации или физического лица;

8) поддержания сетей электронного бизнеса, основанных на концепции ролей в бизнесе (клиент, поставщик услуг, исполнитель, посредник, поставщик (например, поставщик оборудования)) [ITU-T Y.110], [ITU-T M.3050.0];

9) разрешения предприятию и/или физическому лицу исполнять множество ролей в разных сетях, а также множество ролей в пределах определенной сети (например, одна роль – это розничный поставщик услуг, а другая роль – это оптовый поставщик услуг) [ITU-T M.3050.0];

10) поддержания процессов B2B между организациями, предоставляющими услуги и возможности СПП;

11) разрешения управления гибридными сетями, состоящими из СПП и не-СПП ресурсов;

12) объединения абстрактных точек зрения на ресурсы (сеть, вычисление и приложение), в которых кроются сложность и многообразие технологий и доменов.

Подробные требования к управлению СПП выходят за рамки данной Рекомендации и описаны в конкретных рекомендациях по управлению, таких как [ITU-T M.3060].

ПРИМЕЧАНИЕ. – См. также требования в пункте 16.2 "Учет и начисление платы".

12 Обслуживание, связанное с мобильностью

Управление мобильностью включает возможность перемещения между различными сетями (СПП или не поддерживающими СПП) мобильных объектов таких как пользователи, оконечное оборудование и сети. В СПП рассматриваются два различных типа мобильности: персональная мобильность и мобильность оконечного оборудования [ITU-T Q.1706].

Для СПП персональная мобильность имеет место в том случае, если пользователи могут использовать механизмы регистрации для установления привязки к самим себе того или иного оконечного оборудования, которое может быть привязано сетью к пользователю. Там где имеются интерфейсы между пользователями и оконечным оборудованием, и между пользователями и сетями, предполагается, что данные интерфейсы будут использоваться для СПП.

Для СПП мобильность оконечного оборудования имеет место в том случае, когда для привязки оконечного оборудования к сети используются механизмы регистрации. Там где имеется поддержка оконечного оборудования с непрерывностью предоставления услуги, ожидается, что такая поддержка также будет использоваться для СПП.

Далее представлены общие требования для управления мобильностью, акцентированные на поддержке потребностей пользователя.

Требуется, чтобы для услуг, которым свойственна мобильность, в сети СПП обеспечивалось:

1) кочевничество для персональной мобильности и мобильности оконечного оборудования;

2) поддержка мобильности для существующих технологий доступа, возможностей QoS и средств защиты;

3) поддержка управления местоположением для регистрации, обновления сведений о местоположении и трансляции адреса с целью обеспечения мобильности при пересечении границ сетей поставщиков услуг;

4) поддержка управления подпиской о роуминге, идентификацией и аутентификацией при роуминге;

5) обеспечение безопасности для предотвращения несанкционированного доступа и гарантии конфиденциальности пользователя, с учетом непрерывности обслуживания и эстафетной передачи вызова, где это применимо;

6) обеспечение конфиденциальности данных о местоположении для скрытия этих данных от объектов, не являющихся доверенными;

7) поддержка персонального вызова для установления входящих вызовов с целью сохранения энергии в мобильном оконечном оборудовании и уменьшения потоков сигнализации в сети.

8) поддержка управления мобильностью на базе IP-технологии, либо, по меньшей мере, достижение достаточной степени гармонизации с IP-технологией для обеспечения эффективного функционирования и интегральности этих услуг.

Рекомендуется, чтобы для услуг, которым свойственна мобильность, в сети СПП обеспечивалась:

– поддержка непрерывности обслуживания для сценариев связи внутри сети доступа и между сетями доступа. Непрерывность обслуживания предусматривает следующие случаи:
  a) непрерывность обслуживания для мобильности оконечного оборудования;
  b) непрерывность обслуживания для персональной мобильности.

ПРИМЕЧАНИЕ 1. – Уровни реализации непрерывности обслуживания могут быть различными для каждого сценария в зависимости от условий, например ограничений в отношении технологии доступа и уровня обслуживания, обеспечиваемого поставщиком услуг/поставщиком сетевых услуг.

ПРИМЕЧАНИЕ 2. – Непрерывность обслуживания для сценариев связи между базовыми сетями подлежит дальнейшему исследованию.

В случае услуг по передаче голоса требуется, чтобы сеть СПП поддерживала непрерывность обслуживания для мобильности оконечного оборудования.

Требуется, чтобы СПП обеспечивала возможности поддержки непрерывности обслуживания, учитывая сетевые условия (например, количество сеансов пользователя, события, связанные с мобильностью и использование ширины полосы), а также требования пользователей.

Рекомендуется, чтобы СПП позволяла осуществлять адаптацию, для того чтобы поддерживать непрерывность обслуживания, когда требования пользователей и сетевые условия не совпадают. Адаптация может включать согласование/повторное согласование QoS сети и/или параметров оконечного оборудования (например, изменение/адаптацию кодека).

ПРИМЕЧАНИЕ 3. – Подробная информация о требованиях к управлению мобильностью для СПП представлена в [ITU-T Q.1706].

13 Управление профилем

13.1 Управление профилем пользователя

Профиль пользователя – это накопленная информация, связанная с пользователем (или абонентом). В среде СПП управление атрибутами профиля пользователя особенно важно, так как для реализации некоторых возможностей, включая аутентификацию, авторизацию, мобильность, определение местоположения, начисление платы и т. п., требуется информация пользователя. В профиль пользователя входит информация, связанная с транспортом, и информация, связанная с услугой. Профиль пользователя может храниться в отдельных базах данных страты обслуживания и страты транспортирования и может дополнительно иметь функции обмена между ними.

Основными требованиями к профилю пользователя являются следующие:

1) Требуется, чтобы для каждого пользователя существовал свой профиль, необходимый поставщику, который может дополнительно состоять из нескольких "компонентов".

2) Эти компоненты могут быть дополнительно распределены в домашней сети и в среде поставщика услуг; должны удовлетворяться критерии конфиденциальности и защиты данных.

3) Внутри домашней сети эти компоненты могут быть дополнительно распределены по разным объектам.

4) Внутри домашней сети требуется функциональная возможность, позволяющая определить местоположение компонентов профиля пользователя. Данная возможность позволяет услугам/приложениям не знать об истинном местоположении компонентов, и необходима для управления домашней сетью.

5) Требуется, чтобы услуги, приложения и другие объекты СПП были способны получать полный профиль пользователя или избранные его части (по требованию) в одной транзакции; должны удовлетворяться критерии конфиденциальности и защиты данных.

6) Требуется, чтобы присутствовали эффективные средства поиска компонентов профиля отдельного пользователя с приемлемой задержкой для услуг, работающих в реальном времени.

   ПРИМЕЧАНИЕ. – Хотя при управлении профилем пользователя не предпринимается попытка классификации данных, которые может дополнительно содержать этот профиль, но может дополнительно применяться распределение по категориям, например основной информации пользователя или конкретной информации об услуге.

Ожидается, что подробные требования, связанные с профилем пользователя, его использованием и управлением будут содержаться в следующей(их) Рекомендации(ях) МСЭ-Т.

13.2 Управление профилем устройства

Профиль устройства – это набор накопленной информации, связанной с оборудованием пользователя. В среде СПП управление атрибутами профиля устройства также важно, так как информация об устройстве вместе с информацией о "профиле пользователя" часто требуется для ряда возможностей, включая аутентификацию, авторизацию, мобильность, определение местоположения, начисление платы и т. п. Профили устройств могут дополнительно включать информацию,

связанную с транспортированием, и информацию, связанная с услугой. Профили устройств могут храниться в отдельных базах данных страты обслуживания и страты транспортирования и могут дополнительно иметь функции обмена данными между ними.

ПРИМЕЧАНИЕ 1. – Данная информация может дополнительно включать атрибуты идентификации оконечного оборудования, например адрес, имя, статические атрибуты, такие как поддерживаемая среда и протоколы передачи, данные об экране (размер в пикселях, цвета, разрешающая способность, время отклика и т. п.), скорость передачи данных, полоса пропускания, рабочая мощность; динамические атрибуты, такие как пользователь оконечного оборудования, географическое положение, приложения, выполняющиеся на этом оконечном оборудовании.

Профили устройств могут дополнительно использоваться в следующих целях:

– для отслеживания похищенных или незаконно присвоенных устройств;

– для определения типа и уровня обслуживания, который может быть дополнительно предоставлен пользователю, на основании возможностей устройства;

– для определения требуемого качества обслуживания для соединения между оконечным оборудованием, на основании возможностей устройства.

К профилям устройств предъявляются следующие требования:

1) Для каждого оборудования пользователя может дополнительно существовать один профиль устройства, который может дополнительно состоять из нескольких "компонентов".

2) Эти компоненты могут быть дополнительно распределены в домашней сети и/или в среде поставщика услуг стороннего лица.

3) Внутри домашней сети эти компоненты могут быть дополнительно распределены по разным объектам.

4) Внутри домашней сети требуется функциональная возможность, позволяющая определить местоположение компонентов профиля устройства. Данная возможность позволяет службам/приложениям не знать об истинном местоположении компонентов; требуется, чтобы домашняя сеть управляла этой возможностью.

5) При одобрении пользователем, услуги, приложения и другие объекты СПП могут быть дополнительно способны находить целый профиль устройства или избранные его части (по требованию) в одной транзакции; требуется, чтобы удовлетворялись критерии конфиденциальности и защиты данных.

6) Требуется, чтобы присутствовали эффективные средства поиска компонентов профиля индивидуального устройства с приемлемой задержкой для услуг, работающих в реальном времени.

   ПРИМЕЧАНИЕ 2. – Хотя при управлении профилем устройства не предпринимается попыткаклассификации данных, которые может дополнительно содержать этот профиль, но может дополнительно применяться распределение по категориям, например основной информации устройства или конкретной информации об услуге.

Ожидается, что подробные требования, связанные с профилем устройства, его использованием и управлением будут содержаться в следующей(их) Рекомендации(ях) МСЭ-Т.

14 Обработка медиаданных

14.1 Управление медиаресурсами

Механизмы управления медиаресурсами обычно используются в сочетании с традиционными услугами обработки речи и взаимодействия пользователей посредством речевого общения и DTMF. В СПП они должны быть расширены за счет новых услуг передачи данных, видео услуг и услуг передачи контента.

Требуется, чтобы сеть СПП поддерживала различные медиаресурсы и возможности управления медиаресурсами с целью реализации широкого диапазона приложений.

Возможности медиаресурсов в сети СПП включают:

– запись медиаданных (например, для предоставления услуг голосовой почты);

– воспроизведение записанных медиаданных (например, прослушивание голосовой почты, сигналов, объявлений);

– распознавание сигналов DTMF (например, для предоставления услуг интерактивного голосового ответа);

– улучшенное распознавание речи (например, для предоставления услуг интерактивного голосового ответа);

– преобразование медиаданных (например, преобразование текста в речь, речи в текст, факсимильных сообщений в электронную почту);
– перекодировку;
– параллельную передачу видео/текста/звука/данных (например, для конференц-связи);
– дублирование медиаданных (например, для реализации сценариев законного перехвата данных);
– вставку медиаданных.

Дополнительные возможности медиаресурсов для сети СПП включают:
– загрузку медиаданных (например, видео-/аудиоклипов, рисунков);
– передачу медиапотока (например, видеопрограммы по заказу);
– прозрачная передача;
– распределенные хранение и доставку медиаданных (несколько копий медиаданных, несколько сегментов медиаданных);
– динамическую адресацию медиаданных (определение местоположения существующих медиаданных на соответствующем устройстве хранения для обеспечения доступа пользователя к медиаданным в реальном времени).

14.2 Требования к кодеку

14.2.1 Общие требования

Общие требования к кодекам, используемым в СПП, включают следующее:

1) Требуется по мере возможности избегать перекодировки.
2) Требуется, чтобы сеть СПП поддерживала сквозное согласование любого кодека между объектами СПП (оконечным оборудованием, элементами сети). За согласование и выбор общего кодека для каждого сквозного сеанса передачи данных отвечают объекты, расположенные на границах СПП (например, оконечное оборудование СПП и оборудование пользователя) и сетевое оборудование, инициирующее и завершающее передачу IP-потоков медиаданных СПП. СПП должна поддерживать сквозное согласование текстовых кодеков, например кодеков, указанных в Рекомендациях МСЭ-Т.

Рекомендуется, чтобы кодеки для СПП обладали следующими характеристиками:

1) адаптивная работа в различных условиях QoS;
2) решение вопроса, связанного с влиянием изменения уровня обслуживания на работу кодека;
3) совместимость с кодеками КТСОП/ЦСИС;
4) обнаружение/запрос параметров кодека;
5) выбор/согласование параметров кодека и повторное согласование этих параметров в середине сеанса.

14.2.2 Аудиокодеки

Предусматриваются следующие классы аудиокодеков:

a) "узкополосные аудиокодеки" – для диапазона звуковых частот от 300 Гц до 3400 Гц;
b) "широкополосные аудиокодеки" – для диапазона звуковых частот от 50 Гц до 7000 Гц;
c) "сверхширокополосные аудиокодеки" – для диапазона звуковых частот от 50 Гц до 14 000 Гц;
d) "аудиокодеки с полной полосой" – для диапазона звуковых частот от 20 Гц до приблизительно 20 000 Гц и соответствующие им возможности многоканальной передачи (моно, стерео и т. д.).

Для обеспечения взаимодействия между СПП и другими сетями, включая КТСОП /ЦСИС, PLMN и другие СПП, сеть СПП должна иметь возможность приема и воспроизведения речи, закодированной согласно [ITU-T G.711], при взаимодействии с другой сетью. Если размер пакета не был выбран во время согласования кодека между оконечными устройствами и/или сетевыми элементами, или он не установлен двусторонним соглашением, то для речи, закодированной согласно Рекомендации МСЭ-Т G.711, рекомендуется использовать размер пакета с отсчетами 10 мс; это

значение рекомендуется как оптимальное для уравнивания сквозной задержки с загрузкой сети. Известно, что в сети могут дополнительно существовать ограничения, для которых требуется, чтобы двусторонним соглашением было согласовано более высокое значение; в таких случаях рекомендуется значение 20 мс.

ПРИМЕЧАНИЕ 1. – Если размер пакета выбирается путем согласования кодека между оконечными устройствами и/или элементами сети, данная Рекомендация не налагает никаких требований к выбираемому значению.

ПРИМЕЧАНИЕ 2. – Указанное выше не налагает требований в отношении того, чтобы оконечные устройства поддерживали любой кодек или чтобы СПП поддерживали перекодирование между любым произвольным звуковым кодеком и [ITU-T G.711].

Кроме того, рекомендуется, чтобы поддерживались следующие аудиокодеки:

– AMR [ETSI TS 126.071]: для поддержки оконечного оборудования 3GPP и облегчения взаимодействия с сетями 3GPP.
– G.729A [ITU-T G.729]: для облегчения взаимодействия с существующими сетями VoIP и поддержки существующего оконечного оборудования VoIP.
– EVRC/EVRC-B [TIA-127-C]: для поддержки оконечного оборудования 3GPP2 и облегчения взаимодействия с сетями 3GPP2.

14.2.3 Широкополосные аудиокодеки

14.2.3.1 Общие требования

Требуется, чтобы пункт 14.2.1 пользовался преимуществом перед этим пунктом, с тем чтобы уменьшить необходимость перекодировки, а также улучшить функциональную совместимость в широкой полосе и сквозное качество.

Возможность широкополосного звука является дополнительной и может дополнительно обеспечиваться за счет:

– объектов на границе СПП (например, оконечного оборудования СПП), которые способны работать с широкополосным звуком;
– сетевого оборудования, инициирующего и завершающего передачу IP-потоков медиаданных в СПП, содержащих широкополосный звуковой контент.

Требуется, чтобы оконечное оборудование, обеспечивающее возможности широкополосного звука, также имело возможности узкополосного звука и соответствовало требованиям пункта 14.2.2.

Требуется, чтобы сетевое оборудование, обеспечивающее возможности широкополосного звука, также имело возможности узкополосного звука и соответствовало требованиям пункта 14.2.2.

Перекодирование звука может дополнительно осуществляться для обеспечения сквозной функциональной совместимости услуги, однако, по возможности, рекомендуется его избегать.

14.2.3.2 Широкополосные аудиокодеки в оконечном оборудовании

Рекомендуется, чтобы оконечное оборудование, инициирующее и завершающее передачу сквозных IP-потоков медиаданных в СПП, поддерживающее широкополосный звук, обеспечивало один или несколько следующих широкополосных аудиокодеков:

– G.722 [ITU-T G.722].

  ПРИМЕЧАНИЕ 1. – Требуется для оборудования пользователя стандарта DECT NG, которое используется в некоторых видах оборудования пользователя VoIP и/или в старом оборудовании.

– AMR-WB/G.722.2 [ITU-T G.722.2].

  ПРИМЕЧАНИЕ 2. – Требуется для оборудования пользователя 3GPP или оборудования пользователя с функцией мобильного доступа по стандарту 3GPP.

– G.729.1 [ITU-T G.729.1].

  ПРИМЕЧАНИЕ 3. – Используется в некоторых видах оборудования пользователя стандарта DECT NG, оборудования VoIP и/или старом оборудовании пользователя.

– EVRC-WB [TIA-127-C].

  ПРИМЕЧАНИЕ 4. – Требуется для оборудования пользователя 3GPP2 и/или оборудования пользователя с функцией мобильного доступа по стандарту 3GPP2.

  ПРИМЕЧАНИЕ 5. – Оконечное оборудование может дополнительно предоставлять любые иные кодеки, помимо перечисленных выше.

ПРИМЕЧАНИЕ 6. – В исключительных случаях рекомендуется разрешать использование в СПП оконечного оборудования, предоставляющего один или более аудиокодеков, ни один из которых не относится к перечисленным выше (например, существующее/старое оконечное оборудование). Такое оконечное оборудование может дополнительно обладать ограниченной функциональной совместимостью в отношении широкополосного звука.

14.2.3.3 Широкополосные аудиокодеки в сетях

Рекомендуется, чтобы сетевое оборудование, инициирующее или завершающее передачу сквозных IP-потоков медиаданных в СПП, поддерживающее широкополосный звук, обеспечивало следующие широкополосные аудиокодеки:

– G.722 [ITU-T G.722].

ПРИМЕЧАНИЕ 1. – Для поддержки оборудования пользователя стандарта DECT NG, некоторых видов оборудования VoIP и/или старого оборудования пользователя, и/или для взаимодействия с другими сетями.

– AMR-WB/G.722.2 [ITU-T G.722.2].

ПРИМЕЧАНИЕ 2. – Для поддержки оборудования пользователя стандарта 3GPP, оборудования пользователя с функцией мобильного доступа по стандарту 3GPP и/или для взаимодействия с сетями 3GPP.

– G.729.1[ITU-T G.729.1].

ПРИМЕЧАНИЕ 3. – Если требуется поддержка оборудования пользователя стандарта DECT NG, оборудования VoIP и/или старого оборудования пользователя и/или для взаимодействия с некоторыми сетями VoIP и старыми сетями.

– EVRC-WB [TIA-127-C].

ПРИМЕЧАНИЕ 4. – Если требуется поддержка оборудования пользователя стандарта 3GPP2, оборудования пользователя с функцией мобильного доступа по стандарту 3GPP2 и/или для взаимодействия с сетями 3GPP2.

14.2.4 Видеокодеки

Чтобы предоставить возможность взаимодействия между СПП и другими сетями для предоставления услуг видеосвязи, рекомендуется обеспечить поддержку кодеков с нулевым профилем согласно Рекомендации МСЭ-Т H.263 [ITU-T H.263] и базовым профилем согласно Рекомендации H.264 [ITU-T H.264].

ПРИМЕЧАНИЕ. – Указанное выше не налагает требований в отношении видеокодеков, которые должны поддерживаться оконечным оборудованием, и не делает обязательным, чтобы от СПП требовалась поддержка перекодировки видеосигнала между любым произвольным кодеком и кодеками на базе [ITU-T H.263] или H.264 [b-ITU-T H.264].

15 Управление контентом

Рекомендуется, чтобы СПП обеспечивала возможности управления контентом, с тем чтобы управлять различными ресурсами контента, имеющими большие объемы.

ПРИМЕЧАНИЕ 1. – Объекты управления контентом, как правило, делятся на следующие классы: контент предприятия (например, коммерческие документы); контент веб-услуг (например, файлы HTML, изображения); контент услуг IPTV (например, потоки данных относительно больших объемов). Управление контентом в СПП предоставляет возможность управления жизненным циклом контента (например, от создания, через редактирование, утверждение, публикацию и сопровождение до архивирования). Кроме того, управление контентом предоставляет возможность поддержки процессов B2B между организациями в соответствии с происходящими в них процессами.

ПРИМЕЧАНИЕ 2. – Что касается услуг IPTV, подробные требования к управлению контентом содержатся в пункте 14.1.

ПРИМЕЧАНИЕ 3. – Возможности управления контентом включают в себя, в том числе:

– приобретение контента, накопление и импорт контента/метаданных из различных внешних источников;

– валидацию и верификацию формата контента/метаданных, а также определение взаимосвязи между контентом и его метаданными;

– классификацию контента на основе различных классификационных стандартов;

– обращение с контентом и метаданными (например, добавление, изменение, поиск, обработка в соответствии с требованиями авторского права, адаптация).

ПРИМЕЧАНИЕ 4. – Адаптация контента включает возможность преобразования контента, с тем чтобы приспособить его к возможностям устройства и/или ограничениям, накладываемым сетью.

– Распространение контента в пределах сети СПП в соответствии с присвоенными ресурсами доставки контента, ограничениями на публикацию контента и т. д.;

– Мониторинг и проверку контента (например, мониторинг состояния контента и/или результатов обращения с контентом, анализ контента и статистические данные).

16 Эксплуатация и предоставление услуг

16.1 Требования к нумерации, наименованию и адресации

Сеть СПП предназначена для обеспечения эффективной, безопасной и доверенной среды нумерации, наименования и адресации для пользователей, операторов сетей и поставщиков услуг. Там где это необходимо, будут учтены требования по регулированию, а так же взаимодействие с КТСОП/ЦСИС.

Требуется, чтобы эволюция по направлению к СПП гарантировала, что независимость Государств – Членов МСЭ по отношению к планам нумерации, наименования и адресации будет полностью сохранена, как описано в [ITU-T E.164] и других относящихся к данной тематике Рекомендациях и Спецификациях других организаций по стандартизации.

Далее приведены требования для поддержки возможностей нумерации, наименования и адресации. Они применяются как в страте транспортирования, так и в страте обслуживания, если не отмечено иное.

1) Требуется, чтобы поддерживался как динамический, так и статический режим присвоения адресов.
2) Возможности нумерации, наименования и адресации могут быть дополнительно реализованы с помощью отдельной схемы соответствия для каждой услуги, или через общую для различных услуг схему соответствия.
3) Требуется, чтобы поддерживалось динамическое обновление базы данных наименования (например, в случае использования подвижного оконечного устройства, адреса на одном или нескольких уровнях могут дополнительно динамически изменяться в зависимости от местоположения оконечного устройства).

ПРИМЕЧАНИЕ. – Этими хранилищами могли бы стать справочники МСЭ-Т X.500, доступ к которым определен в [b-ITU-T X.511].

16.1.1 Нумерация

Далее приведены требования к нумерации, применимые к СПП.

1) Требуется, чтобы в механизмах адресации поддерживалась возможность различать планы набора номера, нумерации и адресации.
2) Требуется, чтобы в механизмах адресации поддерживалась возможность преобразования последовательности набора номера в нумерацию и схему адресации.
3) Требуется, чтобы в СПП поддерживалась нумерация по Рекомендации МСЭ-Т E.164 (глобальные номера).
4) Рекомендуется, чтобы в СПП была разрешена нумерация, не соответствующая Рекомендации МСЭ-Т E.164 (локальные номера).
5) Рекомендуется, чтобы в СПП были разрешены короткие номера в национальных планах набора номера.
6) Рекомендуется, чтобы сеть СПП не препятствовала существованию систем частной и корпоративной нумерации (см. пункт 17).
7) Требуется, чтобы при использовании нумерации или последовательностей набора номера, не соответствующих Рекомендации МСЭ-Т E.164 (локальных номеров), адресация в СПП определяла область, в пределах которой будет допустимо использование локальных номеров.
8) Требуется, чтобы в СПП поддерживалась международная нумерация по Рекомендации МСЭ-Т E.164.
9) Требуется, чтобы в СПП поддерживалась национальная нумерация по Рекомендации МСЭ-Т E.164.
10) Требуется, чтобы в СПП поддерживались короткие коды в национальных планах набора номера (для номеров, не соответствующих Рекомендации МСЭ-Т E.164).
11) Требуется, чтобы в СПП поддерживалась система частной нумерации (например, зависящая от услуги и корпоративной нумерации) (см. пункты 17.1 и 17.2).
12) Требуется, чтобы при использовании номеров, соответствующих Рекомендации МСЭ-Т E.164, коротких кодов или частных номеров, адресация в СПП определяла область, в пределах которой будет допустимо использование этих номеров.
13) Требуется, чтобы в СПП поддерживалась возможность различия алфавитно-цифровых идентификаторов, в которых могут содержаться только цифры, от идентификаторов, являющихся телефонными номерами, и рекомендуется, чтобы они соответственно обрабатывались в процедурах маршрутизации.

16.1.2 Схемы нумерации, наименования и адресации

1) Требуется, чтобы в страте транспортирования сети СПП поддерживались схемы IP-адресации, основанные на версии протокола IPv4 или IPv6, или на обеих версиях.

   ПРИМЕЧАНИЕ 1. – Рекомендуется принимать во внимание, что комбинация IPv4 и IPv6 в пределах одного домена оператора может дополнительно вызвать проблемы с оказанием услуг.

2) Домены сети СПП могут дополнительно поддерживать оборудование пользователя в интерфейсе "пользователь-сеть" при помощи только IPv4, только IPv6, или обеих версий.

   ПРИМЕЧАНИЕ 2. – Подразумевается, что протокол IPv6, основанный на оборудовании пользователя, также может поддерживать протокол IPv4 в интерфейсе "пользователь-сеть".

3) Требуется, чтобы сеть СПП поддерживала установление мультимедийной связи по протоколу IP (как в случае исходящего вызова, так и при завершении вызова), используя как минимум, телефонный унифицированный идентификатор ресурса по Рекомендации МСЭ-Т E.164 (URI телефона), например тел.: +4412345678, и унифицированный идентификатор ресурса SIP (SIP URI), например как минимум sip:my.name@company.org. Для телефонных URI:

   – Требуется, чтобы поддерживались международные номера, соответствующие Рекомендации МСЭ-Т E.164.

   – Требуется, чтобы поддерживался национальный формат номера, соответствующий Рекомендации МСЭ-Т E.164, и короткий код.

4) В некоторых сценариях услуг, например взаимодействия с КТСОП/ЦСИС, требуется, чтобы сеть СПП поддерживала установление мультимедийной связи по IP-протоколу (как в случае исходящего вызова, так и при завершении вызова), используя нумерацию по Рекомендации МСЭ-Т E.164 с поддержкой там, где это необходимо, нумерации подобной ENUM.

5) Требуется, чтобы в схемах адресации поддерживались одноадресные и многоадресные типы услуг.

6) Рекомендуется, чтобы в схемах адресации поддерживались радиовещательные типы услуг.

7) Могут дополнительно поддерживаться другие схемы нумерации, наименования и адресации.

   ПРИМЕЧАНИЕ 3. – Другие схемы нумерации, наименования и адресации, например различение имен, как указано в [b-ITU-T X.501], подлежат дальнейшему исследованию.

16.1.3 Разрешение имен/номеров/адресов

В [ITU-T Y.2001] представлены основные принципы и требования для разрешения имен, адресов и присвоения номеров. В соответствии с ними представлены следующие требования.

1) Масштабируемость: рекомендуется, чтобы сети СПП были масштабируемыми, для обработки увеличивающихся запросов на разрешение имени/номера/адреса.

2) Надежность: требуется, чтобы возможности разрешения имен/номеров/адресов не были затронуты сбоем в каком-либо одном месте, путем использования, например, механизмов распределенного разрешения.

3) Безопасность: требуется, чтобы для возможностей разрешения имен/номеров/адресов были реализованы меры безопасности.

   ПРИМЕЧАНИЕ. – Данные возможности могут дополнительно использовать базы данных, являющиеся внутренними или внешними по отношению к СПП, например базу данных DNS интернета, LDAP [b-ITU-T X.511]. Примеры мер безопасности включают аутентификацию доступа пользователя, защиту данных, синхронизацию данных и восстановление при сбоях.

16.1.4 Нумерация, наименование и адресация при взаимодействии сетей

При необходимости, функции взаимодействия выполняют преобразование номеров, имен и адресов в сценариях взаимодействия сетей.

1) Требуется, чтобы сеть СПП поддерживала множество сценариев межсетевого взаимодействия адресов в страте транспортирования, сводя к минимуму влияние на услугу, предоставляемую пользователям (то есть, сценарии взаимодействия между доменами с различной адресацией, например доменами, основанными на схемах адресации по протоколу IPv4 или IPv6, и доменами, основанными на общих или частных схемах адресации).

2) Там где необходимо, требуется, чтобы возможности преобразования адреса использовались для поддержки различий в формате адреса, как в страте транспортирования, так и в страте обслуживания, сводя к минимуму влияние на услугу, предоставляемую пользователям.

16.2 Учет и начисление платы

В сетях СПП поддерживаются возможности по ведению учета и начислению платы с целью предоставления оператору сети данных об учете и начислении платы, связанных с использованием ресурсов сети.

Ниже приведены требования к СПП для ведения учета и начисления платы:

1) Требуется, чтобы функциональные возможности ведения учета и начисления платы обеспечивали сбор данных для последующей обработки (начисление оплаты в автономном режиме), а также близкое к реальному времени взаимодействие с такими приложениями, как приложения для внесения предоплаты за обслуживание (начисление оплаты в интерактивном режиме).

2) Требуется, чтобы для управления начислением оплаты были доступны открытые механизмы.

3) Требуется, чтобы выполнялись различные правила начисления оплаты (например, начисление оплаты по фиксированной ставке и начисление оплаты за сеансы связи).

4) Требуется, чтобы возможности ведения учета и начисления платы поддерживали услуги с функциями многоадресной передачи.

5) Требуется, чтобы сети СПП поддерживали все возможные типы соглашений о ведении учета, включая передачу сведений учета/начисления оплаты между поставщиками услуг. Данное требование также включает соглашения об электронной коммерции.

   Например, в сценариях услуг доставки контента с функциями многоадресной передачи, услуги могут быть дополнительно предоставлены в результате совместной деятельности нескольких компаний (например, несколько поставщиков контента и поставщик сетевых услуг): в дополнение к возможностям начисления платы пользователям необходимо иметь возможности начисления платы между компаниями.

6) Требуется, чтобы сети СПП поддерживали интерфейсы и протоколы между элементами сети и элементами учета, а также между элементами учета и начисления платы для сбора и передачи данных об использовании ресурсов (например, показатели учета и учетные записи для начисления платы (CIR)). Указанные интерфейсы и протоколы требуются для выполнения положений [ITU-T Y.2233].

7) Требуется, чтобы сети СПП поддерживали функции управления в целях обеспечения плавной работы функциональных элементов учета и начисления платы [ITU-T Y.2233].

8) Рекомендуется, чтобы сети СПП поддерживали функциональную возможность учета и начисления платы, базирующиеся на потоках, для различных услуг СПП (например, использования ресурсов в рамках однонаправленного потока, использования ресурсов в рамках двунаправленного потока, использования ресурсов в рамках сеанса).

ПРИМЕЧАНИЕ. – Использование сведений о начислении платы, собранных СПП для выписки счетов, выходит за рамки данной Рекомендации.

16.3 Требования к эксплуатации, администрированию и техническому обслуживанию (OAM)

Известно, что возможности OAM весьма важны для сетей общего пользования, позволяя упростить эксплуатацию сети, проверку рабочих характеристик сети и уменьшить эксплуатационные расходы за счет сведения к минимуму перерывов в обслуживании, вероятностей ухудшения обслуживания и простоев. Возможности OAM особенно важны для сетей, в которых необходима доставка (и, следовательно, измерение) параметров рабочих характеристик сети и работоспособности [ITU-T Y.1710], [ITU-T Y.1730].

Требуется, чтобы в СПП были представлены функции OAM как для страты обслуживания, так и для страты транспортирования.

Для того чтобы предложить надежные услуги СПП, которые могут поддерживать требования SLA, требуется, чтобы услуги СПП имели собственные возможности OAM.

ПРИМЕЧАНИЕ 1. – Возможности OAM, приведенные в данном пункте, являются дополнением к возможностям управления, описанным в пункте 11.

Далее приведены требования OAM к сетям СПП.

1) Требуется, чтобы поддерживалась возможность выбора поставщиком услуг или поставщиком сетевых услуг нужных функций OAM.

2) Требуется, чтобы поддерживалась возможность применения функций OAM в приложениях для связи пункта с пунктом, пункта со многими пунктами и многих пунктов со многими пунктами.

3) Требуется, чтобы функции OAM обеспечивали возможность эффективного расширения сети до больших размеров.

4) Требуется, чтобы поддерживалась возможность обнаружения ошибок, дефектов и сбоев.

5) Требуется, чтобы поддерживались возможности диагностики, локализации и уведомления объектов управления сетью, а также выполнение соответствующих действий по исправлению.

6) Требуется, чтобы поддерживалась возможность, позволяющая СПП предотвращать запуск пользователем каких либо функций OAM, относящихся к поставщику услуг/поставщику сетевых услуг.

7) Требуется, чтобы поддерживалась возможность, позволяющая СПП не допускать обнаружения или локализации пользователем неисправностей в сети (так как это является частью ответственности поставщика услуг или поставщика сетевых услуг).

8) Требуется, чтобы трафик OAM передавался по тому же пути, что и трафик пользователя.

9) Требуется, чтобы автоматически обнаруживались следующие ошибки:
   - потеря данных;
   - потеря соединения;
   - ошибочные данные;
   - непреднамеренно самопроизвольно скопированные данные;
   - неправильно введенные данные [ITU-T Y.1730].

10) Требуется, чтобы функциями OAM поддерживалась обратная совместимость. Требуется, чтобы в СПП была возможность задействовать функции OAM незаметно для пользователя, не затрагивая трафик пользователя и без выполнения излишних действий.

11) Требуется, чтобы функции OAM надежно выполнялись даже в условиях плохой передачи данных, например при возникновении ошибок.

12) Требуется, чтобы оценка статуса возможности подключения не зависела от динамического характера трафика пользователя [ITU-T Y.1710], [ITU-T Y.1730].

13) Требуется, чтобы поддерживались взаимоотношения уровня сервер-клиент OAM между нижними уровнями и верхними уровнями (например, сигнал сбоя/сигнал ухудшения работы) в случае использования многоуровневой сети.

14) Требуется, чтобы в случае использования многоуровневой сети, событие неисправности в заданном серверном уровне сети не приводило к появлению множества аварийных событий, и требуется избегать выполнения излишних действий по исправлению в любом более высоком клиентском уровне сети. Рекомендуется, чтобы на клиентском уровне сетей поддерживалась блокировка аварийного предупреждения для серверного уровня, инициирующего дефекты, присутствие которых было передано средствами упреждающего отображения дефекта. Требуется, чтобы на клиентском уровне сетей поддерживалась возможность упреждающего отображения дефекта [ITU-T Y.1710], [ITU-T Y.1730].

15) Требуется, чтобы в случае использования многоуровневой сети, функции OAM в заданном уровне сети не зависели от каких-либо конкретных более низких или более высоких уровней сети. Для архитектуры является критически важной гарантия того, что уровни сети могут развертываться, добавляться и удаляться без влияния на другие уровни сети.

16) Требуется, чтобы в случае использования многоуровневой сети, функции OAM в заданном уровне сети были в достаточной степени независимы от любой конкретной плоскости управления таким образом, чтобы изменения в плоскости управления не вносило изменений в плоскость пользователя OAM. Для архитектуры является критически важным гарантия того, что плоскость пользователя и плоскость управления могут развиваться, не влияя друг на друга.

17) Требуется, чтобы функции OAM поддерживались при различных условиях поставщиков услуг/поставщиков сетевых услуг.

18) Если услуги СПП предоставляются в различных условиях поставщиков услуг/поставщиков сетевых услуг, то требуется обнаружить и отметить, кто из поставщиков услуг/поставщиков сетевых услуг несет ответственность за дефект, для того чтобы можно было быстро среагировать. Кроме того, требуется, чтобы поставщик услуг/поставщик сетевых услуг, который предлагает эту услугу клиенту, был поставлен в известность о сбое в обслуживании, даже если этот сбой и место обнаружения расположены в сети другого поставщика услуг/поставщика сетевых услуг.

19) Требуется, чтобы у СПП были механизмы, для того чтобы удостовериться в том, что потоки поставщиков услуги/сети OAM, которые предназначены для внутреннего использования, находятся внутри их сетей и не существует утечки данных к клиентам или к другим поставщикам услуг/сети.

20) Для реализации функций OAM в гибридных сетях таким образом, чтобы услуги могли предоставляться по сквозному тракту, состоящему из комбинации сетей СПП и сетей, не являющихся СПП, требуется, чтобы функции OAM поддерживались в сценариях взаимодействия (пункт 18.3).

21) Для того чтобы сделать возможным раздельное управление частью сети, ответственность за которую несет поставщик, а также гибко определять объекты технического обслуживания, требуется, чтобы поддерживались как "сегментная" функция OAM, так и "сквозная" функция OAM.

ПРИМЕЧАНИЕ 2. – Сегмент – это часть сквозного соединения, которая определяется для задач эксплуатации и технического обслуживания.

22) Требуется, чтобы поддерживалась регистрация времени простоя услуги для оценки качества и надежности.

23) Требуется, чтобы информация, полученная с помощью функций OAM, была организована таким образом, чтобы предоставить надлежащие сигналы индикации техническому персоналу для поддержания качества уровня обслуживания, предложенного клиентам [ITU-T I.610].

24) Требуется, чтобы поддерживались возможности мониторинга качественных показателей.

16.4 Управление на основе политики

Управление на основе политики может дополнительно использоваться в СПП чтобы:

1) Убедиться в согласованности услуги во всем диапазоне технологий доступа и базовой сети. Оно также может применяться во многих сетях, предоставляющих услуги.

ПРИМЕЧАНИЕ 1. – Такое управление, применяемое в каждой сети, зависит от технологии сети и может дополнительно конкретизироваться под каждую сетевую технологию.

2) Обеспечить контроль доступа с учетом использования возможностей и ресурсов сети услугами и приложениями.

3) Обеспечить регистрацию использования ресурсов сети.

ПРИМЕЧАНИЕ 2. – Это можно рассматривать как функцию, предоставляющую информацию, которая может быть дополнительно использована другими возможностями сети, такими как учет и назначение цены.

4) Скрыть услуги и приложения от сложных деталей реализации транспортной сети.

ПРИМЕЧАНИЕ 3. – Управление на основе политики может быть использовано для нужд приложений, пока они остаются независимыми от развернутых сетевых технологий.

Вместе с основными областями применения, указанными выше, и применяемой с возможностью соединения, QoS и безопасностью, может быть предпринято еще много действий в сфере управления, которые принесут пользу службам СПП. Например, управление на основе политики может быть дополнительно применено к:

– предоставлению услуги;

– конфигурации услуги;

– авторизации (например, названия);

– доставке услуги;

– учету и начислению платы.

Управление на основе политики может вводить правила для предоставления надежных, согласованных, однозначных результатов, называемых стратегическими решениями. Сложность этих правил зависит от их предполагаемого использования.

ПРИМЕЧАНИЕ 4. – Возможности управления QoS, такие как ресурс и контроль доступа (пункт 9) могут дополнительно рассматриваться как часть общего управления набором возможностей на основе политики.

Следующие общие требования предъявляются к управлению СПП на основе политики:

1) Требуется, чтобы поддерживались возможности управления на основе политики, для того чтобы гарантировать доступ к услуге, ее предоставление и управление ею.

2) Требуется, чтобы возможности управления на основе политики действовали в пределах конкретных услуг и в пределах конкретных доменов поставщиков или во всем множестве доменов поставщиков.

3) Требуется, чтобы возможности управления на основе политики отвечали отказом или не отвечали на несанкционированные запросы и отвечали на санкционированные запросы.

16.5 Требования к живучести

Функции живучести необходимы для реализации сетей с высокой надежностью.

16.5.1 Защитная коммутация

Требуется, чтобы в СПП поддерживались возможности защитной коммутации для реализации быстрых и детерминированных функций живучести для всех трактов трафика.

Следующие общие требования предъявляются к защитной коммутации транспорта СПП:

1) Требуется, чтобы поддерживались возможности для предотвращения запуска защитной коммутации более низкого уровня из-за дефекта в более высоком уровне.

2) Если в защитной коммутации участвует более одного уровня, то требуется, чтобы более низкие уровни пользовались приоритетом перед более высокими уровнями (это также известно, как стратегия межуровневого распространения).

3) Рекомендуется, чтобы предоставлялась как защитная коммутация по схеме 1 + 1, так и по схеме 1: n.

4) Неиспользованные ресурсы защиты транспорта могут дополнительно использоваться для передачи трафика с наибольшей эффективностью.

5) Рекомендуется, чтобы влияние на производительность сети (например, дополнительная задержка, изменение задержки, ошибки в битах, потери пакетов и т. п.) из-за защитной коммутации было сведено к минимуму.

6) Требуется, чтобы поддерживались функции ручного управления, такие как блокировка защиты, принудительное подключение и подключение команд вручную.

Подробные требования для конкретных технологий предоставлены в разных Рекомендациях, например [ITU-T G.808.1].

16.5.2 Повторная маршрутизация

Если случаются серьезные аварии или происходят особые события, то может дополнительно произойти ухудшение качества или, в самом худшем случае, сбой в сети. В этих случаях требуются такие возможности как повторная маршрутизация, с возможным понижением производительности или качества услуги и механизмы контроля трафика.

ПРИМЕЧАНИЕ. – Эти возможности могут также рассматриваться как часть функций целостности сети.

Следующие общие требования предъявляются к повторной маршрутизации СПП:

1) Если в повторной маршрутизации участвует более одного уровня, то более низкие уровни могут дополнительно пользоваться приоритетом перед более высокими уровнями (стратегия межуровневого распространения.

2) Требуется, чтобы механизм повторной маршрутизации был способен найти альтернативный маршрут за приемлемый период времени.

3) Рекомендуется, чтоб влияние на производительность сети (например, дополнительная задержка, изменение задержки, ошибки в битах, потери пакетов и т. п.) из-за защитной коммутации было сведено к минимуму.

4) Требуется, чтобы сеть СПП не исключала управление оператором.

5) Требуется, чтобы при необходимости была возможна повторная оптимизация сети после восстановления поврежденного трафика.

6) Требуется, чтобы при возвращении в исходное состояние после сбоя или условий ухудшенного качества, была восстановлена производительность уровня обслуживания, предшествовавшая сбою или условиям ухудшенного качества.

16.5.3 Способность услуги к восстановлению

Условия способности услуги к восстановлению зависят от конкретной услуги, следовательно, требуется, чтобы они были определены для каждой услуги.

Следующие общие требования предъявляются к способности услуги к восстановлению (SR):

1) Требуется, чтобы сеть СПП имела возможность для независимого присвоения разных уровней SR разным услугам.

2) Требуется, чтобы сеть СПП имела возможность для независимого присвоения разных уровней SR разным услугам в различных потоках.

3) Требуется, чтобы в зависимости от присвоенного уровня SR услуги, охваченные SR, имели возможность представлять тот же уровень качества обслуживания, который был до сбоя.

4) Оконечное оборудование может дополнительно передавать уровни SR сети СПП.

5) Требуется, чтобы сеть СПП имела возможность присвоения и поддержки SR от точки входа до точки выхода в сети поставщика услуги.

6) Требуется, чтобы сеть СПП имела возможность разделения панели пользователя и панели управления в потоках с задействованными SR.

7) Требуется, чтобы сеть СПП поддерживала возможность уведомления приложения/пользователя, если требуемый уровень SR не отвечает требованиям сетей СПП.

17 Сети пользователей, включая сети предприятий

17.1 Общие требования к сети СПП, касающиеся доступа через сети пользователей

Далее приведены общие требования к сети СПП, касающиеся доступа через сети пользователей:

1) Требуется, чтобы сеть СПП не запрещала решения по предоставлению доступа через сеть пользователя к СПП с использованием NAT/NAPT и брандмауэров в среде пользователя, где назначение IP-адресов оборудованию пользователя может быть дополнительно выполнено сетью пользователя. Для таких адресов может отсутствовать возможность маршрутизации в СПП.

2) Требуется, чтобы решения по предоставлению доступа к СПП через сеть пользователя оказывали минимальное влияние на существующие модели развертывания сети пользователя.

3) Требуется, чтобы решения по предоставлению доступа к СПП через сеть пользователя поддерживали следующие конфигурации:

   – прямое соединение и взаимодействие отдельных оконечных устройств и СПП;

   – опосредованное соединение и взаимодействие отдельных оконечных устройств и СПП (через домашние сети и сети предприятий).

Рекомендуется, чтобы сети СПП поддерживали одновременное использование одним оконечным устройством нескольких типов функций транспорта доступа, однако требования по согласованию связи отсутствуют. Поэтому с точки зрения сети такие оконечные устройства могут дополнительно отображаться как два или несколько отдельных оконечных устройств.

ПРИМЕЧАНИЕ. – Не подразумевается запрет присоединения оконечного оборудования, которое может позволять адаптацию интерфейса под различные нужды пользователей, включая людей с ограниченными возможностями, при помощи наиболее распространенных устройств интерфейса пользователя.

17.2 Общие требования к сетям пользователей

Далее приведены требования высокого уровня к сетям пользователей, соединенным с СПП:

– Рекомендуется, чтобы сети пользователей, соединенные с СПП, обеспечивали пользователю доступ:

  1) к услугам, предоставляемым СПП;

  2) к услугам, предоставляемым в самих сетях пользователей (локально и через присоединенную сеть СПП);

  3) в качестве корпоративного и домашнего пользователей.

– Рекомендуется, чтобы сети пользователей, соединенные с СПП, обеспечивали:

  1) безопасность домашних сетей, управление ими и качество обслуживания в них;

  2) инициализацию устройства и конфигурацию услуги (оконечное оборудование пользователей, шлюза для сетей пользователей), включая удаленный доступ.

17.3 Сети предприятий

17.3.1 Введение

В настоящем пункте определяются требования высокого уровня к связи на предприятии, направленные на:

1) обеспечение соединения и взаимодействия возможностей связи на предприятии (размещаемых либо в корпоративной сети последующего поколения (КСПП), либо в СПП) с возможностями СПП;

2) обеспечение соединения и взаимодействия возможностей связи на предприятии с другими возможностями связи на предприятии (размещаемыми либо в КСПП, либо в СПП);

3) обеспечение соединения и взаимодействие возможностей связи на предприятии с другими возможностями связи на предприятии, расположенными в ЦСИС и КТСОП или соединенными с ними;

4) поддержку размещаемых услуг предприятия в той или иной СПП.

ПРИМЕЧАНИЕ 1. – В настоящей Рекомендации определяются сетевые требования по обеспечению непосредственного соединения КСПП с СПП, а также сетевые требования по обмену информацией между возможностями КСПП (включая оборудование пользователя) и другими возможностями КСПП того же самого предприятия, осуществляемому с помощью СПП (например, в случае географического разноса).

ПРИМЕЧАНИЕ 2. – Предполагается, что в случае присоединения старой РВХ к СПП применяются требования к существующим старым услугам.

17.3.2 Виды трафика предприятия

Трафик, создаваемый или принимаемый от имени КСПП, может являться:

– либо трафиком, передаваемым в СПП для обработки в соответствии с обычными правилами СПП. Данный вид трафика называется трафиком сети общего пользования;

– либо трафиком, передаваемым в СПП для обработки по согласованному набору правил, характерных для того или иного предприятия. Такой вид трафика называется трафиком частной сети. Как правило, трафик частной сети передается в пределах одного предприятия, однако такой вид трафика может также передаваться между двумя различными предприятиями, если это не запрещено по соображениям регуляторного характера.

  ПРИМЕЧАНИЕ. – Сеть предприятия может дополнительно по отдельности различать передачу информации по частной сети, которая инициируется в СПП, от передачи информации по частной сети, которая инициируется на предприятии. Данный вопрос выходит за рамки данной Рекомендации.

Требуется, чтобы сеть СПП отличала трафик сети общего пользования от трафика частной сети.

Требуется, чтобы сеть СПП отличала трафик частной сети, принадлежащий одному предприятию, от трафика частной сети, принадлежащего другому предприятию.

Для трафика частной сети может дополнительно требоваться обработка в СПП, отличающаяся от обработки трафика сети общего пользования.

Требуется, чтобы за исключением случаев, когда это не допускается национальными регуляторными положениями и законами, СПП обрабатывала трафик между предприятиями таким же образом, как трафик сети общего пользования. При этом в рамках предоставляемых предприятию возможностей СПП может дополнительно обеспечить возможности впуска и выпуска трафика от имени каждого предприятия.

Требуется, чтобы для трафика частной сети СПП являлась прозрачной к механизмам сигнализации, за исключением случаев, когда имеет место особая потребность в том, чтобы СПП осуществляла вмешательство для доставки услуг по запросу корпоративных клиентов.

17.3.3 Возможности связи на предприятии

Требуется, чтобы СПП позволяла использовать любую среду передачи на базе IP при осуществлении связи на предприятии, при условии наличия ресурсов и договорных соглашений.

Требуется, чтобы за исключением случаев, разрешенных на основании явного соглашения с КСПП (путем сигнализации или договора), либо предусматривающих удовлетворение формальных юридических требований, СПП не вмешивалась в передачу медиаданных в СПП.

ПРИМЕЧАНИЕ 1. – Примерами оснований для согласованного вмешательства является перекодирование, трансляция и параллельная передачи. Правило невмешательства нарушается для предотвращения ненадлежащего ухудшения качества работы (в частности, для данных телеметрии в реальном времени, двунаправленной передачи аудио- и видеосигналов) и также для защиты воспринимаемой конфиденциальности среды передачи.

Рекомендуется, чтобы СПП позволяла транспортировку самой сигнализации, в то время как транспортировка медиаданных осуществляется по другим сетям.

ПРИМЕЧАНИЕ 2. – Например, для обеспечения связи между двумя предприятиями СПП может участвовать в передаче сигнализации (в целях содействия маршрутизации от первого предприятия ко второму предприятию), однако трафик медиаданных может направляться непосредственно по другим сетям на базе IP.

СПП может дополнительно предоставлять предприятию следующие возможности:

a) Виртуальные арендованные линии, когда сайты КСПП присоединяются с помощью СПП. СПП не предоставляет никаких дополнительных возможностей.

b) Приложение транкинга для коммерческой деятельности, когда в СПП размещаются возможности транзита трафика между КСПП, возможности впуска трафика из СПП в КСПП и возможности выпуска трафика из КСПП в СПП. Приложение транкинга для коммерческой деятельности может также дополнительно размещать возможности, помимо базовых возможностей впуска трафика, выпуска трафика и транзита трафика в КСПП. Как правило, отсутствует оконечное оборудование корпоративной сети, подключенное непосредственно к СПП.

c) Размещаемые услуги предприятия (HES), когда в СПП размещаются возможности инициирования/завершения коммерческой связи для пользователей связи на предприятии, которые непосредственно подключены к СПП и являются абонентами этих услуг в данной СПП.

17.3.4 Управление местоположением

Требуется, чтобы СПП предоставляла КСПП информацию о географическом местоположении пользователя. Эта информация может зависеть от требований к конфиденциальности.

ПРИМЕЧАНИЕ 1. – КСПП может использовать информацию о географическом местоположении, например для предоставления пользователю услуг, основанных на местоположении.

ПРИМЕЧАНИЕ 2. – Источником информации о географическом местоположении может дополнительно выступать пользователь СПП или КСПП.

17.3.5 Сигнализация

Требуется, чтобы сеть СПП предлагала один из стандартных видов сигнализации для сопряжения с КСПП.

17.3.6 Маршрутизация

17.3.6.1 Маршрутизация в направлении пользователя КСПП

Требуется, чтобы СПП поддерживала маршрутизацию в направлении пользователей КСПП, которые не являются абонентами СПП и с которыми, однако, возможна связь через сайт КСПП, имеющий соглашение с СПП относительно транкинга для коммерческой деятельности.

ПРИМЕЧАНИЕ. – В этом случае сайт КСПП является абонентом услуг СПП, и пользователям корпоративной сети, относящимся к КСПП, не требуется самим являться абонентами СПП, поскольку они принадлежат КСПП и управляются ей. Благодаря этому требованию с этими пользователями корпоративной сети может быть установлена связь открытой части СПП путем непосредственного указания их адреса с использованием открытого адреса.

17.3.6.2 Маршрутизация на базе диапазона номеров

Для обеспечения возможности маршрутизации в направлении пользователей корпоративной сети в КСПП рекомендуется, чтобы СПП поддерживала маршрутизацию только для конкретного диапазона номеров согласно [ITU-T E.164], присвоенных этой КСПП.

17.3.7 Управление QoS

Требуется, чтобы СПП поддерживала протокол управления допуском при передаче сообщений для каждого конкретного сайта КСПП.

ПРИМЕЧАНИЕ 1. – Поставщик сетевых услуг СПП определяет набор правил или политик, в соответствии с которым рекомендуется передавать сообщения, а также рекомендуется, чтобы поставщик сетевых услуг КСПП мог управлять конфигурацией возможности в рамках этих правил и политик.

Требуется обеспечивать возможность установки следующих пороговых значений для каждого конкретного направления (например, передача исходящих и входящих сообщений):

1) максимальное количество одновременных передач, осуществляемых на основе сеансов;

2) максимальное количество одновременно передаваемых потоков, используемых при передаче.

Передачи, превышающие допустимое пороговое значение, могут разрешаться или отклоняться.

ПРИМЕЧАНИЕ 2. – Предприятие может выбирать значения, устанавливаемые для управления допуском при передаче сообщений, которые соответствуют соглашению об уровне обслуживания (SLA) между этим предприятием и поставщиком сетевых услуг СПП. Если такое значение выбрано, то к превышающим допустимое пороговое значение передачам, которые принимаются, могут применяться особые правила в отношении начисления платы.

17.3.8 Идентификация

17.3.8.1 Идентификация сайта КСПП

Требуется, чтобы СПП поддерживала идентификацию сайта КСПП в целях аутентификации и авторизации.

ПРИМЕЧАНИЕ 1. – Идентификация сайта КСПП необходима, чтобы позволить СПП определить, с какого сайта КСПП инициирована связь.

ПРИМЕЧАНИЕ 2. – КСПП может дополнительно располагать несколькими сайтами КСПП и, следовательно, несколькими относящимися к ним идентификаторами сайта КСПП.

17.3.8.2 Идентификация пользователя сети предприятия

В дополнение к требованиям к наименованию, нумерации и адресации, перечисленным в пункте 16, требуется, чтобы СПП предоставляла возможность однозначной идентификации пользователей КСПП. Идентификаторы пользователя КСПП присваиваются КСПП.

ПРИМЕЧАНИЕ 1. – Данное требование не исключает сценариев, когда одна организации, действующая как поставщик сетевых услуг СПП, выполняет еще одну роль и осуществляет администрирование этой КСПП предприятия от имени данного предприятия.

ПРИМЕЧАНИЕ 2. – Приведенное выше требование гарантирует, что при связи между пользователем КСПП и пользователем СПП, услуга предоставления пользователю СПП идентичности исходящего пункта (OIP) может представить правильный идентификатор пользователя КСПП, осуществляющего вызов.

ПРИМЕЧАНИЕ 3. – Приведенное выше требование гарантирует, что для связи между пользователями СПП и пользователями КСПП услуга предоставления пользователю СПП (идентификатора пункта завершения (TIP)) может представить правильный идентификатор вызываемого пользователя КСПП.

ПРИМЕЧАНИЕ 4. – Приведенное выше требование гарантирует, что пользователи СПП могут вызывать пользователей КСПП, идентификаторы которых находятся в наборе идентификаторов, доступных данной КСПП в соответствии с соглашением о транкинге для коммерческой деятельности, относящимся к данной КСПП.

Не рекомендуется, чтобы СПП препятствовала присвоению КСПП новых идентификаторов пользователей в пределах своего домена, без предварительного соглашения с СПП.

Рекомендуется, чтобы СПП поддерживала идентификаторы пользователей КСПП, которые преобразуются номера МСЭ-Т E.164.

Не рекомендуется, чтобы СПП препятствовала изменению КСПП преобразований идентификаторов пользователей в пределах своего домена в номера МСЭ-Т E.164 без предварительного соглашения с СПП.

ПРИМЕЧАНИЕ 5. – Данное правило подразумевает, что для связи, осуществляемой из КТСОП/ЦСИС в направлении КСПП, СПП должна быть в состоянии определить, что вызываемый номер МСЭ-Т E.164 находится в пределах домена КСПП и, таким образом, направить сообщение в КСПП, указав в качестве номера адресата либо вызываемый номер МСЭ-Т E.164, либо обнаруженный идентификатор КСПП, который получен из информации, опубликованной КСПП (например, DNS).

Рекомендуется, чтобы СПП поддерживала идентификаторы пользователей КСПП, которые не преобразуются в номера МСЭ-Т E.164.

ПРИМЕЧАНИЕ 6. – Несмотря на то что идентификаторы пользователя КСПП, которые не преобразуются в номера МСЭ-Т E.164, будут недоступны со стороны КТСОП/ЦСИС, они должны быть доступны со стороны других пользователей КСПП или СПП.

Не рекомендуется, чтобы СПП препятствовала доставке до КСПП идентификаторов вызывающих и соединенных пользователей, при условии готовности и отсутствия требований к конфиденциальности или регуляторных требований, запрещающих такую доставку.

Не рекомендуется, чтобы СПП препятствовала применению конфиденциальности к идентификаторам вызывающих и соединенных пользователей на постоянной основе или при каждом сеансе связи, таким образом, чтобы идентификаторы не оказывались скрытыми от других пользователей.

ПРИМЕЧАНИЕ 7. – Это требование означает, чтоб СПП не должна доставлять другим сторонам при таких условиях ни каких бы то ни было идентификаторов, предоставляемых КСПП (и обозначенных, как частные), ни какого бы то ни было стандартного идентификатора, который СПП присваивает КСПП.

17.3.9 Аутентификация

Требуется, чтобы аутентификация в отношении соединения КСПП и СПП удовлетворяла требованиям, указанным в настоящем пункте, и в пункте 10.3.

17.3.10 Безопасность

Требуется, чтобы безопасность, связанная с соединением той или иной КСПП с СПП, удовлетворяла требованиям, указанным в пункте 10.

17.3.11 Управление мобильностью

В настоящем пункте определяются требования к роумингу в контексте связи на предприятии.

Рекомендуется, чтобы для роуминга в контексте связи на предприятии обеспечивалось кочевничество применительно к мобильности терминала и персональной мобильности.

В частности, рекомендуется, чтобы пользователь КСПП мог зарегистрироваться и получать услугу от своей КСПП, находясь в режиме роуминга по отношению к:

a) другому сайту КСПП той же самой КСПП, присоединенному с помощью СПП;

b) СПП, с которой непосредственно соединена КСПП;

c) СПП, с которой КСПП опосредованно соединена с помощью другой СПП.

Помимо возможностей роуминга для пользователей СПП, описанных в настоящем пункте, рекомендуется, чтобы при условии соглашения с КСПП, пользователь СПП мог зарегистрироваться и получать услугу от своей СПП, находясь в режиме роуминга по отношению к:

a) КСПП, с которой непосредственно соединена СПП;

b) КСПП, которая опосредованно соединена с СПП.

17.3.12 Учет

Предприятие может осуществлять учет трафика с помощью своих возможностей связи на предприятии, которые размещаются либо на КСПП, либо на СПП.

Для трафика сетей общего пользования применяются требования, изложенные в [ITU-T Y.2201] и [ITU-T Y.2233].

Для трафика сетей общего пользования требуется, чтобы предприятие и поставщик сетевых услуг СПП имели возможность идентифицировать друг друга на любых интерфейсах присоединения, включая интерфейсы внутри СПП к размещаемым возможностям связи на предприятии.

Для трафика частных сетей требуется, чтобы любые участвующие предприятия имели возможность идентифицировать друг друга на любых интерфейсах присоединения, расположенных между возможностями связи на этих предприятиях.

Требуется, чтобы любая возможность связи на предприятии, размещенная в СПП, была в состоянии вести учет трафика частной сети, передаваемого на предприятие, таким же образом, как поставщик сетевых услуг СПП учитывает свой собственный трафик.

Кроме того, для трафика частных сетей требуется, чтобы предприятие и поставщик сетевых услуг имели возможность идентифицировать друг друга на любых интерфейсах присоединения.

18 Присоединение и взаимодействие сетей

Функциональная совместимость и взаимодействие – это две отдельные функции, они определены соответственно в [ITU-T Y.101] и в Рекомендациях МСЭ-Т серии Y.1400.

18.1 Требования к присоединению

Различаются два типа присоединений между сетями СПП:

– "присоединение, ориентированное на обеспечение соединения": Основывается на простом установлении IP-соединений, независимо от уровней функциональной совместимости сетей.

ПРИМЕЧАНИЕ 1. – Присоединение данного типа не содержит сведений о конкретной услуге, предоставляемой в сквозном режиме, и как следствие, рабочие характеристики сети, требования к QoS и безопасности не могут быть гарантированы в обязательном порядке.

– "присоединение, ориентированное на услугу": Дает возможность операторам и поставщикам услуг предлагать услуги с определенными уровнями функциональной совместимости.

ПРИМЕЧАНИЕ 2. – Примером являются услуги по Рекомендации МСЭ-Т G.711, предоставляемые через IP-присоединение. Определенные уровни функциональной совместимости сетей зависят от услуги или QoS, или безопасности и т. д.

ПРИМЕЧАНИЕ 3. – Только присоединение, ориентированное на услугу, полностью удовлетворяет требованиям к функциональной совместимости СПП.

Требования к присоединению являются следующими:

1) Требуется, чтобы между сетями СПП поддерживался тип присоединения, ориентированный на обеспечение соединения.

   Требуется, чтобы данный тип присоединения между сетями СПП поддерживался с использованием различных версий IP.

2) Требуется, чтобы между сетями СПП поддерживался тип присоединения, ориентированный на услугу.

   Требуется, чтобы данный тип присоединения между сетями СПП поддерживался с использованием различных версий IP.

3) Требуется, чтобы между СПП и КСПП поддерживалось присоединение, ориентированное на услугу, если СПП предоставляет размещаемые услуги предприятия.

   Требуется, чтобы данный тип присоединения между СПП и КСПП поддерживался с использованием различных версий IP.

18.1.1 Присоединение, ориентированное на услугу, между сетями СПП на базе IMS

Требования к присоединению, ориентированному на услугу, между сетями СПП на базе IMS являются следующими:

1) Требуется, чтобы логический канал присоединения между поставщиками сетевых услуг СПП имел информацию о конкретных услугах СПП. Это может быть физический или логический канал, по которому передаются и данные, и носители сигналов. Требуется, чтобы СПП предоставлял один стандартизованный интерфейс для присоединения к другой СПП.

2) Требуется управлять ресурсами в канале присоединения, с тем чтобы воспринимать характеристики данных и носителей сигналов, относящиеся к различным услугам.

3) Требуется, чтобы принимались во внимание характеристики безопасности и учета.

Другие подробные требования к присоединению, ориентированному на услугу, подлежат дальнейшему исследованию (например, требования из областей передачи сигнала, кодека, маршрутизации, безопасности, начисления платы и ведения учета, ресурсов, QoS и SLA).

18.2 Требования к функциональной совместимости

Для обеспечения предоставления определенных услуг по сквозному маршруту, состоящему из одного или нескольких доменов СПП, требуется чтобы:

1) в пределах домена одной СПП взаимодействовали необходимые компоненты услуг;

2) не исключалась функциональная совместимость присоединенных сетей СПП, в которых развернуты одинаковые наборы возможностей услуг.

18.3 Требования к взаимодействию сетей

Требуется, чтобы для предоставления определенных услуг СПП поддерживала взаимодействие с различными видами сетей. Требуется, чтобы услуги, определенные для взаимодействия, беспрепятственно предоставлялись по всей инфраструктуре, представляемой одним или несколькими поставщиками сетевых услуг. Сети СПП предоставляют возможности, включающие, наряду с другими, безопасность, OAM, устойчивость к внешним воздействиям, качество обслуживания и, там где необходимо, перекодирование медиаданных для поддержки сценариев присоединения с другими сетями, не относящимися к СПП, с целью обеспечения беспрепятственной сквозной работы.

Для того чтобы дать возможность предоставления определенных услуг на маршруте, состоящем из сочетания сетей СПП и сетей, не относящихся к СПП:

– Требуется, чтобы, сеть СПП могла взаимодействовать с другими сетями, не относящимися к сетям СПП.

– Рекомендуется, чтобы сеть СПП по мере возможности поддерживала следующие возможности взаимодействия:

  - маршрутизация;
  - взаимодействие на уровне сигнализации;
  - взаимодействие по нумерации, наименованию и/или адресации;
  - обмен данными, относящимися к ведению учета и начислению платы;
  - взаимодействие в области безопасности;
  - взаимодействие в области QoS;
  - обмен информацией о профиле пользователя и оконечного устройства;
  - взаимодействие на уровне сред передачи;
  - взаимодействие в области управления;
  - управление политикой (например, в соответствии с междоменными правилами, может дополнительно возникнуть необходимость в том, чтобы внутренняя информация доверенного домена, включая информацию, относящуюся к пользователю, была сокрыта или удалена из информационного потока, передаваемого через интерфейс с другим доверенным или не являющимся доверенным доменом), включая учет различий в политике.

  ПРИМЕЧАНИЕ. – Под этим не подразумевается, что все службы и/или функциональные возможности службы могут взаимодействовать. Данные требования могут дополнительно применяться только к взаимодействию между определенными конкретными (и, наиболее вероятно, аналогичными или идентичными) службами и/или функциональными характеристиками службы.

18.3.1 Взаимодействие с КТСОП/ЦСИС

Требуется, чтобы при соединении сети СПП и КТСОП/ЦСИС поддерживались следующие функции:

1) Взаимодействие между услугами КТСОП/ЦСИС и услугами эмуляции КТСОП /ЦСИС. Требуется, чтобы при взаимодействии сетей обеспечивался высокий уровень функциональной совместимости с услугами эмулированной КТСОП/ЦСИС. Обеспечиваемая

степень функциональной совместимости услуг зависит от операторов и, в некоторых случаях, от национальных регуляторных органов.

2) Взаимодействие между услугами КТСОП/ЦСИС и услугами моделирования КТСОП/ЦСИС: Требуется, чтобы при взаимодействии сетей обеспечивалась функциональная совместимость услуг моделирования КТСОП/ЦСИС с дополнительными услугами КТСОП/ЦСИС, хотя такое взаимодействие может дополнительно привести к ограничению возможностей услуги.

3) Взаимодействие между КТСОП/ЦСИС и мультимедийными IP-услугами сети СПП, хотя такое взаимодействие может привести к ограничению возможностей услуги.

ПРИМЕЧАНИЕ 1. – Под этим не подразумевается, что все услуги СПП и/или свойства услуг могут взаимодействовать с КТСОП/ЦСИС и наоборот. Данные требования могут дополнительно применяться только к взаимодействию между определенными конкретными (и, наиболее вероятно, аналогичными или идентичными) услугами и/или свойствами услуги, которые предоставляются как со стороны СПП, так и КТСОП/ЦСИС.

ПРИМЕЧАНИЕ 2. – Корпоративные сети с коммутацией каналов поддерживаются либо посредством соединения с сетью СПП через существующие сети КТСОП/ЦСИС, либо, когда реализована эмуляция КТСОП/ЦСИС, через шлюз взаимодействия.

18.3.2 Взаимодействие с другими сетями

1) Требуется, чтобы сеть СПП обеспечивала возможность прямого присоединения для сетей с коммутацией каналов, включая, как минимум, кабельные сети, радиовещательные сети и сети сухопутной подвижной связи общего пользования. Для всех сетей с коммутацией каналов требования по взаимодействию, такие же, как и требования к КТСОП/ЦСИС.

Требуется, чтобы сеть СПП поддерживала возможность для присоединения, ориентированного на установление соединения, с сетями, которые не являются СПП, но основаны на протоколе IP.

Требуется, чтобы сеть СПП поддерживала возможность для присоединения, ориентированного на установление соединения, с сетями, которые не являются СПП, но основаны на протоколе IP, и в которых используется различные версии IP.

Требуется, чтобы СПП не исключала возможность присоединения, ориентированного на услугу, с сетями, которые не являются СПП, но основаны на протоколе IP.

Если присоединенная сеть предусматривает все возможности взаимодействия, как указано в пункте 18.3, такие присоединения сетей могут дополнительно поддерживаться при развертывании. Определения характеристик и функциональные возможности сетей, не являющихся сетями СПП, но основанных на протоколе IP, являются достаточно разнообразными и многочисленными, поэтому неизменные требования для присоединения установить невозможно.

2) Требуется, чтобы в сети СПП не было преднамеренного исключения присоединений с сетями, не являющимися сетями СПП, но основанными на протоколе IP.

ПРИМЕЧАНИЕ. – Требования безопасности содержатся в пункте 10.6.

18.4 Неразглашение информации в интерфейсах NNI и ANI

Требуется, чтобы в СПП имелись возможности, позволяющие, если это необходимо, например в соответствии с регламентарным положением, законом, государственными или региональными условиями:

– препятствовать раскрытию внутренней информации или информации пользователей услуг другим объектам в интерфейсах NNI;

– препятствовать раскрытию информации, содержащейся внутри сети, а также информации пользователей сети другим объектам в интерфейсах NNI;

– препятствовать раскрытию внутренней информации или информации пользователей услуг другим объектам в интерфейсах ANI;

– препятствовать раскрытию информации, содержащейся внутри сети, а также информации пользователей сети другим объектам в интерфейсах ANI.

18.5 Обмен информацией, связанной с пользователями, между поставщиками

Требуется, чтобы в целях совместимости услуг в СПП поддерживались механизмы для обмена информацией, связанной с пользователями, если это необходимо, например в соответствии с регламентарным положением или законом.

19 Требования, характерные для услуг

19.1 Эмуляция КТСОП/ЦСИС

Эволюция сетей в СПП зависит от выбора поставщиков и их потребностей. Поставщики сетевых услуг могут дополнительно выбирать эволюционный путь в зависимости от их реальных ресурсов, бизнес-планов и стратегий. Таким образом, они могут дополнительно выбрать разные технологии и временные рамки.

Требуется, чтобы в переходном периоде от КТСОП/ЦСИС к СПП в СПП обеспечивались следующие возможности:

1) возможности эмуляции КТСОП/ЦСИС;
2) возможности моделирования КТСОП/ЦСИС.

Далее приведены требования к данным возможностям.

19.1.1 Общие требования

Требуется, чтобы в сети СПП предоставлялся по меньшей мере один уровень услуги эмуляции КТСОП/ЦСИС, обеспечивающий возможности, которые идентичны или лучше возможностей, предлагаемых сетями с коммутацией каналов.

19.1.2 Оконечное оборудование

Требуется, чтобы сеть СПП поддерживала действующие терминалы (например, традиционные телефоны КТСОП, текстовые телефоны, устройства факсимильной связи и другие типы существующего оконечного оборудования КТСОП/ЦСИС), которые соединены не с помощью интерфейса UNI СПП, а через КТСОП/ЦСИС, похожие на UNI.

ПРИМЕЧАНИЕ. – Эмуляция всей услуги КТСОП/ЦСИС может быть дополнительно невозможна, а также поддержка услуги может быть дополнительно ограничена для некоторых типов оконечного оборудования, то есть действующего оконечного оборудования или оборудования пользователя, которое ведет себя как действующее оконечное оборудование.

19.1.3 Услуги

Применительно к эмуляции КТСОП/ЦСИС к услуге предъявляются следующие требования:

1) Требуется, чтобы в СПП для поставщиков услуг обеспечивалась возможность эмулировать одну или более из их услуг КТСОП/ЦСИС.
2) Требуется, чтобы в СПП поддерживались определения возможности, унаследованные из действующей спецификации КТСОП/ЦСИС.

ПРИМЕЧАНИЕ. – При развертывании конкретной СПП могут не поддерживаться все возможности и интерфейсы, представленные в КТСОП/ЦСИС.

19.2 Мультимедийные диалоговые услуги в реальном времени, включая моделирование КТСОП/ЦСИС

19.2.1 Общие требования

Требуется, чтобы в СПП поддерживались услуги моделирования КТСОП/ЦСИС, создающие у пользователя впечатление, что он работает в КТСОП/ЦСИС.

19.2.2 Оконечное оборудование

Требуется, чтобы сеть СПП поддерживала оконечное оборудование, не являющееся устаревшим, для услуг моделирования КТСОП/ЦСИС. Она также может дополнительно поддерживать устройства адаптации для обеспечения возможности подсоединения действующего оконечного оборудования к СПП (например, обычные телефоны, текстовые телефоны и устройства факсимильной связи).

19.2.3 Услуга

Ниже приведены требования услуги для моделирования КТСОП/ЦСИС:

1) Требуется, чтобы в СПП поддерживались возможности услуг, аналогичных услугам КТСОП/ЦСИС и использующих управление сеансом связи посредством IP-интерфейсов и инфраструктуры.

2) Рекомендуется, чтобы СПП предоставляла поставщику услуг возможность моделировать услуги КТСОП/ЦСИС.

3) Не требуется, чтобы СПП предоставляла услуги, идентичные услугам сетей КТСОП/ЦСИС.

ПРИМЕЧАНИЕ. – Предполагается, что в услугах моделирования КТСОП/ЦСИС не применяются модели вызовов или протоколы сигнализации КТСОП/ЦСИС.

19.3 Услуги IPTV

При предоставлении СПП услуг IPTV применяется следующее описание.

В том, что касается требований к СПП по поддержке услуг IPTV, в настоящей Рекомендации содержатся требования высокого уровня.

Для того чтобы услуги IPTV поддерживались СПП, возможности СПП, в принципе, поддерживают требования, описанные в [ITU-T Y.1901], с учетом замены текста "архитектура IPTV" на текст "среда СПП", содержащийся в требованиях [ITU-T Y.1901]. Конкретные аспекты, например какие конкретные возможности СПП поддерживают требования СПП, определенные в [ITU-T Y.1901] и применяются ли эти возможности в равной мере ко всем услугам IPTV, подлежат дальнейшему исследованию.

19.3.1 Предложение услуг

Требуется, чтобы архитектура СПП поддерживала механизмы в отношении услуг IPTV, предоставляемых по запросу (включая видео по запросу (VoD) с оперативной доставкой VoD [ITU-T Y.1901]), услуг вещания с повторной передачей [ITU-T Y.1901] (включая линейное ТВ [ITU-T Y.1901]), а также интерактивных услуг. Рекомендуется, чтобы архитектура СПП поддерживала механизмы для cPVR [ITU-T Y.1901] и nPVR [ITU-T Y.1901]. Для реализации некоторых услуг IPTV рекомендуется, чтобы поддерживалась функциональная возможность спецрежима [ITU-T Y.1901].

Рекомендуется, чтобы архитектура СПП поддерживала механизмы, с помощью которых конечные пользователи могут обеспечивать доступ других конечных пользователей к созданному ими контенту.

Требуется, чтобы архитектура СПП обеспечивала конечным пользователям возможность выбирать предпочтительный язык (звук, субтитры [ITU-T Y.1901], бегущую строку [ITU-T Y.1901], дополнительный контент [ITU-T Y.1901], а также звуковые описания [ITU-T Y.1901]) на разных языках, которые заранее определены поставщиком контента и доставлены поставщиком услуги.

ПРИМЕЧАНИЕ. – Дополнительная информация, касающаяся услуг по запросу, представлена в [b-ITU-T Y.Sup.5].

19.3.2 Транспортировка и мобильность

В целях поддержки услуг IPTV применяются требования к транспортировке, описанные в пункте 6, включая поддержку многоадресной передачи.

Для обеспечения услуг IPTV применяются содержащиеся в пункте 12 требования к обслуживанию, связанному с мобильностью.

19.3.3 Средства подключения услуг

Требуется, чтобы архитектура СПП поддерживала для контента и услуг IPTV возможности обнаружения и выбора, а также возможность перемещения.

Рекомендуется, чтобы архитектура СПП поддерживала отслеживание зрителями изменения данных наряду с защитой, при необходимости, конфиденциальности пользователя.

Рекомендуется, чтобы архитектура СПП позволяла собирать статистические данные об использовании контента, а также прослеживать контент.

Рекомендуется, чтобы архитектура СПП располагала средствами, позволяющими просматривать контент только соответствующей аудиторией в соответствии с определенными географическими районами, родительской оценкой и точно указанными группами. В частности, требуется, чтобы архитектура СПП поддерживала механизмы блокирования передачи контента в точно указанные географические районы во всех случаях, когда применяются требования по прекращению передачи.

19.3.4 Промежуточное программное обеспечение и метаданные

Требуется, чтобы архитектура СПП не препятствовала какому бы то ни было использованию промежуточного программного обеспечения и метаданных, определенных для услуг IPTV.

19.3.5 QoS

Требуется, чтобы сети, поддерживающие IPTV, поддерживали классы QoS протокола IP, а также удовлетворяли требованиям к качественным показателям, соответствующим этим классам и указанным в [ITU-T Y.1541]. К этим требованиям относится обеспечение точного временного управления для целей синхронизации, например синхронизация изображения и звука. Рекомендуется, чтобы архитектура СПП поддерживала средства для обеспечения достаточной оценки пользователем качества услуги (QoE) применительно к времени переключения канала [ITU-T Y.1901].

Требуется, чтобы СПП обеспечивала основу для определения компонентов и контрольных точек (включая устройства конечных пользователей) в целях измерения качества обслуживания (QoSM).

19.3.6 Безопасность

Требуется, чтобы архитектура СПП обеспечивала защиту услуги и контента.

19.3.7 Управление

Рекомендуется, чтобы архитектура СПП поддерживала (дистанционное) обновление и загрузку программного обеспечения для устройств IPTV.

19.3.8 Среда передачи

Требуется, чтобы архитектура СПП не препятствовала какому бы то ни было использованию форматов видео- и аудиозаписи (включая разрешения видеоизображения, форматы видеокадров, частоты дискретизации звука и разрядности звука), указанных для услуг IPTV.

Требуется, чтобы архитектура СПП не препятствовала какому бы то ни было использованию видео- и аудиокодеков, указанных для услуг IPTV.

Требуется, по возможности, избегать в архитектуре СПП перекодировки во время доставки контента IPTV.

19.3.9 Начисление платы

Требуется, чтобы в архитектуре СПП поддерживались механизмы для сбора данных для целей учета и отчетности, расчетов с партнерами и сверки использования конечными пользователями, такие как подписка, покупка и транзакции применительно к услуге. Это необходимо для поддержки вариантов учета, таких как плата за каждый отдельный просмотр [ITU-T Y.1901].

19.3.10 Аспекты оконечного оборудования

Требуется, чтобы оконечное устройство, поддерживающее услуги IPTV, имело возможность выбирать, получать и воспроизводить многие виды звуковой и видеоинформации, а также относящейся к ней управляющей информации для регулировки предоставления услуг.

Рекомендуется, чтобы архитектура СПП поддерживала такие возможности оконечного оборудования и использовала эти возможности для регулирования предоставления услуг.

19.3.11 Взаимодействие

Требования к обеспечению взаимодействия услуг IPTV подлежат дальнейшему исследованию.

19.3.12 Общественный интерес

Требуется, чтобы архитектура СПП поддерживала оконечные устройства для услуг IPTV, которые ведут постоянное прослушивание сообщений, содержащих оповещения о чрезвычайных ситуациях (EAN).

Требуется, чтобы архитектура СПП поддерживала возможность характеристик доступности (бегущая строка, субтитры, звуковые описания и много видеопотоков, например для кинетической речи), а также их синхронизацию с основным контентом при просмотре в режиме обычного воспроизведения.

Рекомендуется, чтобы архитектура СПП поддерживала передачу видеоданных с достаточным качеством для восприятия кинетической речи, включая чтение с губ. Для этого требуется передавать достаточное количество кадров в секунду и достаточное пространственное разрешение для подробного воспроизведения движений рук, лица, губ, глаз и туловища лица, использующего кинетическую речь [b-ITU-T H.Sup.1].

19.4 Услуги предприятия

19.4.1 Услуга виртуальных арендованных линий

В настоящей Рекомендации не определяется никаких требований к конкретной услуге.

19.4.2 Приложение транкинга для коммерческой деятельности

В настоящей Рекомендации не определяется никаких требований к конкретной услуге.

19.4.3 Размещаемые услуги предприятия

При предоставлении размещаемых услуг предприятия (HES) требуется, чтобы СПП:

– обеспечивала связь для предприятий, к которым относятся как пользователи, поддерживаемые с помощью КСПП, так и пользователи, поддерживаемые с помощью HES;

– позволяла любому пользователю на предприятии перемещаться между местоположением КСПП и местоположением, обеспечиваемым с помощью HES, без необходимости информирования об этом изменении партнера, с которым осуществляется связь;

– позволяла любому пользователю на предприятии перемещать свое оконечное оборудование между местоположением КСПП и местоположением, обеспечиваемым с помощью HES с минимальным изменением конфигурации.

19.5 Приложения и услуги, в которых используется идентификация на основе ярлыков

При предоставлении СПП приложений и услуг, в которых используется идентификация на основе ярлыков, в [ITU-T Y.2213] определяются соответствующие требования к конкретной услуге.

19.6 Услуги с управляемой доставкой

При предоставлении СПП услуг с управляемой доставкой, в [ITU-T Y.2212] определяются соответствующие требования к конкретной услуге.

19.7 Услуги визуального наблюдения

Услуга визуального наблюдения посредством связи между оконечными устройствами позволяет одному оконечному устройству получать и контролировать мультимедийную информацию, созданную другим оконечным устройством (источником), а также осуществлять дистанционное управление оконечным устройством-источником.

Услуга визуального наблюдения посредством связи сервера с оконечным устройством позволяет многим оконечным устройствам получать и контролировать одинаковую мультимедийную информацию, созданную одним сервером источником.

Услуга визуального наблюдения посредством связи оконечного устройства с сервером позволяет одному серверу собирать много фрагментов или один накопленный фрагмент мультимедийной информации, созданной многими оконечными устройствами (источниками).

При предоставлении услуг визуального наблюдения требуется, чтобы СПП поддерживала:

– услуги визуального наблюдения посредством связи между оконечными устройствами (включая связь одного с одним и одного со многими) (например, услугу визуального наблюдения для системы домашней безопасности);

– услуги визуального наблюдения посредством связи сервера с оконечным устройством (включая связь одного с одним и одного со многими) (например, услугу визуального наблюдения для контроля движения общественного транспорта).

Требования к услугам визуального наблюдения посредством связи оконечного устройства с сервером подлежит дальнейшему исследованию.

19.7.1 Услуга визуального наблюдения посредством связи сервера с оконечным устройством

Требуется, чтобы СПП поддерживала возможности обнаружения и отбора, а также возможность перемещения для услуги визуального наблюдения посредством связи сервера с оконечным устройством.

Рекомендуется, чтобы СПП позволяла собирать статистические данные об использовании контента, а также прослеживать контент.

Рекомендуется, чтобы СПП располагала средствами, позволяющими просматривать контент только соответствующей аудиторией, в соответствии с определенными географическими районами, родительской оценкой и точно указанными группами. В частности, требуется, чтобы архитектура СПП поддерживала механизмы блокирования передачи контента в точно указанные географические районы, во всех случаях, когда применяются требования по прекращению передачи.

Требуется, чтобы СПП обеспечивала защиту услуги и контента.

Рекомендуется, чтобы архитектура СПП поддерживала (дистанционное) обновление и загрузку программного обеспечения для устройств визуального наблюдения посредством связи сервера с оконечным устройством.

19.7.2 Услуга визуального наблюдения посредством связи между оконечными устройствами

Для обеспечения услуги визуального наблюдения посредством связи между оконечными устройствами требуется, чтобы СПП поддерживала требования, изложенные в следующих подпунктах.

19.7.2.1 Обработка сеанса связи

Требуется, чтобы СПП поддерживала управление допуском к сеансу применительно к информации, связанной с визуальным наблюдением.

Требуется, чтобы СПП поддерживала обработку сеанса применительно к информации, связанной с визуальным наблюдением (например, данные о конкретной услуге, такой как дистанционное управление).

19.7.2.2 Маршрутизация

Требуется, чтобы СПП поддерживала маршрутизацию с учетом возможностей оборудования, расположенного в исходящем пункте и/или в пункте завершения (например, поддержку среды передачи).

19.7.2.3 Кодеки

Требуется, чтобы архитектура СПП поддерживала любое использование видео- и аудиокодеков, определенных для услуг визуального наблюдения.

Требуется, по возможности, избегать в архитектуре СПП перекодировки во время доставки информации визуального наблюдения.

19.8 Приложения и услуги повсеместно распространенных сенсорных сетей (USN)

Требования к конкретной услуге подлежат дальнейшему исследованию.

19.9 Услуги центра мультимедийной связи

Требования к конкретной услуге подлежат дальнейшему исследованию.

19.10 Услуги VPN в СПП

При предоставлении СПП услуг виртуальной частной сети (VPN), в [ITU-T Y.2215] определяются соответствующие требования к конкретной услуге.

20 Аспекты общественных интересов

Требуется, чтобы в СПП предоставлялись возможности для поддержки услуг общественных интересов, востребованных правилами и законами государственных или региональных администраций и международными договорами. В эти услуги общественных интересов могут входить, кроме прочих, услуги, описанные в этих пунктах.

20.1 Законный перехват

1) Требуется, чтобы поставщик транспорта СПП и/или поставщик услуг СПП выполняли требования законного перехвата. Таким образом, требуется, чтобы в СПП предоставлялись механизмы, которые сделают законный перехват возможным, там где это необходимо согласно правилам или законам страны в их области применения.

2) Требуется, чтобы с помощью механизмов законного перехвата предоставлялся доступ к содержимому передаваемой информации (CC) и сведениям, полученным в результате перехвата (IRI) правоохранительными органами (LEA) по требованиям со стороны администраций или в соответствии с международными договорами.

Так как характер законного перехвата зависит от государственных/региональных регуляторных положений и законов, то требования зависят от регуляторной среды каждого государства.

20.2 Идентификация вредоносной связи

Требуется, чтобы в СПП предусматривалась возможность идентификации источника вредоносной связи, например получение идентификаторов оконечного оборудования или данных о местоположении инициатора связи.

20.2.1 Идентификация вредоносной связи на предприятии

Требуется, чтобы передаваемая информация, которая идентифицируется как трафик сети общего пользования, обрабатывалась в соответствии с требованиями об идентификации вредоносной связи, предъявляемыми к СПП.

Идентификация вредоносной связи в трафике частной сети выходит за рамки данной Рекомендации. Требуется, чтобы СПП не обрабатывала такую передаваемую информацию. Это требование также применяется к размещаемой возможности КСПП.

ПРИМЕЧАНИЕ. – К трафику частной сети могут применяться отдельные регуляторные требования.

20.3 Незапрашиваемые сообщения

Требуется, чтобы в СПП предоставлялись возможности для предотвращения передачи незапрашиваемых сообщений (UC).

Требуется, чтобы в СПП предоставлялась возможность обработки обнаруженных и помеченных попыток передачи сообщений в целях реагирования на эти попытки (например, переадресация сообщения на почтовый ящик, голосовой почтовый ящик или в папку нежелательной почты).

Рекомендуется, чтобы в СПП обеспечивались механизмы противодействия UC (например, применение черных/белых списков, систем проверки репутации, маскирования адреса, фильтрации контента).

ПРИМЕЧАНИЕ 1. – Более подробная информация об этих механизмах представлена в [b-ITU-T X.1244].

Рекомендуется, чтобы в СПП обеспечивался механизм, позволяющий пользователям СПП представлять отчет о получении UC.

Рекомендуется, чтобы в СПП обеспечивался механизм проверки отчетов о получении UC, представленных пользователями СПП.

Рекомендуется, чтобы СПП:

- обеспечивала возможность для затронутых UC пользователей делать запрос о маркировке (осуществлении оценки) UC;
- обеспечивала возможность для затронутых UC пользователей исправлять маркировку UC.

ПРИМЕЧАНИЕ 2. – Более подробная информация об осуществлении оценки UC представлена в [b-ETSI TS 187.009].

20.4 Электросвязь в чрезвычайных ситуациях

В электросвязь в чрезвычайных ситуациях (включая поддержку и раннее предупреждение) входят:

– связь от отдельного субъекта к органу власти, например вызов экстренных служб;

– связь между органами власти, например связь для оказания помощи при бедствии (TDR);

– связь от органа власти к отдельному субъекту, например услуги массового оповещения.

ПРИМЕЧАНИЕ. – Кроме электросвязи от органа власти к органу власти TDR и служба электросвязи в чрезвычайных ситуациях (ETS) могут также дополнительно использоваться для электросвязи от органа власти к отдельному субъекту.

В [ITU-T Y.1271], [ITU-T E.106] и [ITU-T E.107] представлены "Структура требований к сетям и возможностям электросвязи в чрезвычайных ситуациях в развивающихся сетях с коммутацией каналов и с коммутацией пакетов", "Международная схема предпочтений оказания помощи в чрезвычайных ситуациях (IEPS) для действий по оказанию помощи при бедствиях" и "Служба электросвязи в чрезвычайных ситуациях, и структура взаимодействия для государственной реализации ETS" соответственно.

Требуется, чтобы в СПП были созданы возможности сети, доступные для приложений раннего предупреждения, например для предоставления информации о географическом местоположении для доставки предупредительных сообщений только тем, кто, возможно, будет затронут надвигающимся бедствием.

Для поддержания электросвязи в чрезвычайных ситуациях и раннего предупреждения от СПП требуется надежная работа и высокая готовность.

Требуется, чтобы сеть СПП:

1) включала возможности уровня обслуживания и транспортного уровня, для того чтобы электросвязь в чрезвычайных ситуациях поддерживалась с использованием схем приоритетности/предпочтения. Требуется, чтобы у контроля вызова/сеанса электросвязи в чрезвычайных ситуациях и канала передачи трафика электросвязи в чрезвычайных ситуациях имелось преимущество в условиях перегрузки/сбоя;

2) обеспечивала необходимое взаимодействие и отображение механизмов приоритета между разными компонентами СПП (например, между сетью доступа и базовой сетью и между уровнем обслуживания и транспортным уровнем) и между сетями СПП (например, между двумя базовыми сетями поставщиков услуг), чтобы обеспечить надлежащую сквозную электросвязь, с учетом приоритетности/предпочтения;

3) поддерживала существующие услуги электросвязи, включая услуги, эквивалентные всем существующим услугам электросвязи КТСОП/ЦСИС, в чрезвычайных ситуациях, даже если один или несколько взаимодействующих объектов присоединены к СПП, а один или несколько объектов присоединены к КТСОП/ЦСИС;

4) активировала новые средства электросвязи в чрезвычайных ситуациях (например услуги мгновенных сообщений), для того чтобы она поддерживалась властями (такими как поставщики услуг в чрезвычайных ситуациях) в будущих применениях;

5) обеспечивала непрерывное взаимодействие органов электросвязи в чрезвычайных ситуациях по всем сетям общего пользования внутри административного домена (чрезвычайной ситуации);

6) обеспечивала маршрутизацию электросвязи в чрезвычайных ситуациях к соответствующим органам власти;

7) обеспечивала маршрутизацию электросвязи в чрезвычайных ситуациях от органа власти к отдельным субъектам;

8) обеспечивала, если это возможно, непрерывную электросвязь в чрезвычайных ситуациях между органом власти и отдельными субъектами до тех пор, пока орган власти не завершит сеанс, даже если отдельный субъект мог дополнительно повесить трубку;

9) предоставляла органу власти информацию о географическом местоположении отдельного субъекта, а так же о его идентификаторе, в соответствии с требованиями государственных или региональных регуляторных положений. Если это требуется в соответствии с регламентарным положением или законом, то эта информация может быть получена органом власти, даже если отдельный субъект просил ее не сообщать;

10) предоставляла возможности как санкционированного, так и не санкционированного доступа к услугам электросвязи в чрезвычайных ситуациях в соответствии с требованиями государственных или региональных регуляторных положений. Например, требуется, чтобы СПП предоставляла возможность аутентификации доступа пользователя к электросвязи ETS/TDR;

11) поддерживала снятие с электросвязи в чрезвычайных ситуациях определенных ограничивающих функций управления сетью;

12) поддерживала электросвязь в чрезвычайных ситуациях в альтернативной или множественной среде передачи, если это требуется (например, в соответствии с регуляторным положением или законом). Видео, текст и голос и любая другая комбинация из этого набора, как и различные формы сообщений, имеют значение для электросвязи, предоставляемой экстренным службам для людей с ограниченными возможностями;

13) предоставляла гарантии распространения только санкционированных сообщений раннего предупреждения;

14) предоставляла возможности предотвращения бесцельных и не являющихся необходимыми сообщений, похожих на сообщения о раннем предупреждении.

20.4.1 Электросвязь в чрезвычайных ситуациях для предприятия

Электросвязь в чрезвычайных ситуациях для предприятия может дополнительно осуществляться путем передачи трафика сети общего пользования и трафика частной сети.

1) Требуется, чтобы сообщения электросвязи в чрезвычайных ситуациях для предприятия, идентифицированные как трафик сети общего пользования, обрабатывались в соответствии с требованиями к СПП в отношении электросвязи в чрезвычайных ситуациях.

2) В случае передачи сообщения электросвязи в чрезвычайных ситуациях в трафике сети общего пользования требуется, чтобы СПП передавала информацию о географическом местоположении, полученную от КСПП, и по возможности использовала ее для маршрутизации сообщений электросвязи к соответствующим органам власти. Это может зависеть как от требований к конфиденциальности, так и от регуляторных требований.

3) Маршрутизация сообщений, идентифицированных как сообщения электросвязи в чрезвычайных ситуациях в трафике частной сети, выходит за рамки документов по СПП. Требуется, чтобы СПП не обрабатывала такие сообщения. Это требование также применяется к размещаемой возможности КСПП.

4) В соответствии с национальными регуляторными положениями и законами, частные планы нумерации или планы набора номера, используемые на предприятии, могут дополнительно повторно использовать национальные номера экстренных служб для других целей и могут дополнительно использовать другие номера для обозначения электросвязи в чрезвычайных ситуациях.

5) В соответствии с национальными регуляторными положениями и законами, в случае если предприятие эксплуатирует частный пункт PSAP, то СПП, в зависимости от обстоятельств, может дополнительно поддерживать маршрутизацию сообщений электросвязи в чрезвычайных ситуациях для предприятия, передаваемых в трафике сетей общего пользования, к частному PSAP (или к одному из нескольких частных PSAP), либо к PSAP общего пользования. Например, если вызывающий абонент физически находится в месте расположения конкретного предприятия, то для данного места может потребоваться маршрутизация к частному PSAP, в то время как для вызывающих абонентов, которые физически находятся в каком-либо ином месте, может потребоваться маршрутизация к PSAP общего пользования.

20.5 Представление идентификатора пользователя и конфиденциальность

1) Требуется, чтобы в СПП существовала возможность для представления идентификатора исходящей стороны.

2) Требуется, чтобы в СПП существовала возможность для представления идентификатора входящей стороны.

3) Требуется, чтобы в СПП существовала возможность для подавления представления идентификатора исходящей стороны.

4) Требуется, чтобы в СПП существовала возможность для подавления представления идентификатора входящей стороны.

ПРИМЕЧАНИЕ. – Требования для поддержки электросвязи в чрезвычайных ситуациях могут дополнительно обходить подавление.

20.6 Выбор поставщика услуги или сети

Требуется, чтобы в СПП поддерживалась возможность для выбора поставщика, если это необходимо, например согласно регуляторному положению или закону.

20.7 Пользователи с ограниченными возможностями

Основная потребность пользователей с ограниченными возможностями заключается в том, что им требуются средства для контроля и использования оконечного оборудования и услуг другими возможными способами и в других возможных режимах, подходящих для разных возможностей и предпочтений. Таким требованиям лучше всего отвечает совокупная разработка основного представления оконечного оборудования и услуг.

1) Требуется, чтобы в СПП предоставлялось средство, необходимое для вызова услуг ретрансляции. Услуги ретрансляции осуществляют преобразование в разные режимы связи, которые представляют интерес для людей с ограниченными возможностями (например кинетическая речь, чтение по губам, текст, голос). Вызов услуг ретрансляции может дополнительно основываться на предпочтениях пользователя, на преобразовании адреса или команд пользователя.

2) Требуется, чтобы в СПП существовала возможность вызова услуг ретрансляции любым участником электросвязи в чрезвычайных ситуациях.

ПРИМЕЧАНИЕ 1. – Другие потребности пользователей с ограниченными возможностями при пользовании услугами электросвязи в чрезвычайных ситуациях рассмотрены в пункте 20.4.

ПРИМЕЧАНИЕ 2. – См. также [b-ITU-T Accessibility] и [b-ITU-T F.790].

20.8 Переносимость номера

Переносимость номера – это возможность сетей КТСОП/ЦСИС.

Эквивалентной возможностью в СПП является идентификация переносимости (пункт 10.2). Эмуляция КТСОП/ЦСИС не налагает новых требований для поддержки переносимости номера, потому что эмулированные услуги образованы от КТСОП/ЦСИС (см. пункт 19.1.3).

20.9 Разделение услуг

Во многих государственных сферах применения требуется, чтобы поставщики услуг "разделили" свои предложения, чтобы дать клиентам возможность выбирать поставщиков разнообразных услуг, а поставщикам – предлагать услуги клиентам на конкурентной основе.

Там где это необходимо, например, в соответствии с регуляторным положением или законом, требуется, чтобы сеть СПП поддерживала механизмы реализации разделения услуг.

20.10 Отклонение анонимных сообщений

Требуется, чтобы СПП обеспечивала механизм, позволяющий пользователю отклонять входящие сообщения, если вызывающий абонент неизвестен.

20.10.1 Отклонение анонимных сообщений для предприятия

Требуется, чтобы любое сообщение, идентифицированное как трафик сети общего пользования, обрабатывалось в соответствии с требованием к СПП относительно отклонения анонимных сообщений.

Требования к обработке анонимных сообщений в трафике частной сети выходят за рамки данной Рекомендации. Требуется, чтобы СПП не обрабатывала такие сообщения. Это требование также применяется к размещаемой возможности КСПП.

ПРИМЕЧАНИЕ. – К трафику частной сети могут дополнительно применяться отдельные регуляторные требования.

Дополнение I

Основные различия между настоящим вариантом Рекомендации МСЭ-Т Y.2202 (Y.2201 (Rev. 1)) и предыдущим вариантом Рекомендации МСЭ-Т Y.2201 (2007 г.) с точки зрения требований и возможностей высокого уровня

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

В настоящем Дополнении перечислены основные различия между настоящей Рекомендацией и Рекомендацией МСЭ-Т Y.2201 (04/2007 г.) [ITU-T Y.2201] с точки зрения требований и возможностей высокого уровня.

ПРИМЕЧАНИЕ. – Завершение настоящего Дополнения является предметом дальнейшего исследования.

Возможность в Рекомендации МСЭ-Т Y.2201(Rev.1)	**Пункт в настоящей Рекомендации**	**Пункт в Рекомендации МСЭ-Т Y.2201 (2007 г.) (если применимо)**	**Улучшения по сравнению с Рекомендацией Y.2201 (2007 г.)**	**Новая возможность**
OAM			Отсутствуют	–
Мобильность			Поддержка эстафетной передачи вызова	–
Информированность о контексте		–	–	X

Дополнение II

Преобразование услуг в средства подключения услуг

(Данное Дополнение не является неотъемлемой частью данной Рекомендации.)

ПРИМЕЧАНИЕ. – Завершение настоящего Дополнения является предметом дальнейшего исследования.

В данном Дополнении представлен пример преобразования выбранных услуг в выбранные средства подключения услуг (пункт 7.2). Данное преобразование не претендует на полноту и не представляет требования, которые необходимо поддерживать.

Таблица II.1 – Наглядный пример преобразования услуг в средства подключения услуг

Услуги/средства подключения услуг	Присут-ствие	Управле-ние местопо-ложением	Управ-ление группой	Обработка сообщений	Поддержка много-адресной передачи	Принуди-тельная доставка	Обработ-ка сеанса связи	Управление персональ-ной инфор-мацией	Управление устройством	Поддержка приложе-ний на базе веб	Синхро-низация данных
Диалоговые голосовые услуги в реальном времени							X				
Мультимедийные диалоговые услуги в реальном времени							X				
Передача текста в реальном времени							X				
Услуги передачи сообщений	X		X	X			X				
Разговор в сетях СПП "нажми, чтобы говорить"	X		X				X				
Мультимедийные интерактивные услуги связи пункта с пунктом			X				X				
Объединенные интерактивные услуги связи		X	X				X				
Услуги на базе метода "нажми, чтобы говорить"		X				X					

Таблица II.1 – Наглядный пример преобразования услуг в средства подключения услуг

Услуги/средства подключения услуг	Присутствие	Управление местоположением	Управление группой	Обработка сообщений	Поддержка многоадресной передачи	Принудительная доставка	Обработка сеанса связи	Управление персональной информацией	Управление устройством	Поддержка приложений на базе веб	Синхронизация данных
Услуги широковещательной/многоадресной передачи					X						
Информационные услуги	X	X				X					
Присутствие и услуги общего уведомления	X	X	X								
Услуги на основе OSA 3GPP версия 6 и 3GPP2 версия A	X	X	X	X	X	X	X				
Приложения поиска данных	X					X					
Услуги VPN			X		X						
Приложения и услуги, использующие идентификацию на основе ярлыков					X				X		
Услуги визуального наблюдения							X		X		
Услуги IPTV											
Услуги предприятия: Услуга виртуальной арендованной линии											
Услуги предприятия: Приложение транкинга для коммерческой деятельности											
Услуги предприятия: Размещаемые услуги предприятия											
Услуги с управляемой доставкой											

Библиография

В следующих документах содержится информация, которая может представлять ценность для читателей этой Рекомендации. В них представлена дополнительная информация о темах, охваченных данной Рекомендацией, но они не существенны для понимания данной Рекомендации.

Рекомендации МСЭ

[b-ITU-T E.351] Recommendation ITU-T E.351 (2000), *Routing of multimedia connections across TDM-, ATM- and IP-based networks*.

[b-ITU-T F.703] Recommendation ITU-T F.703 (2000), *Multimedia conversational services*.

[b-ITU-T F.724] Рекомендация МСЭ-Т F.724 (2005 г.), *Описание услуг и требования к услугам видеотелефонной связи, предоставляемым по IP-сетям.*

[b-ITU-T F.733] Рекомендация МСЭ-Т F.733 (2005 г.), *Описание услуг и требования к услугам мультимедийных конференций, предоставляемым через IP-сети.*

[b-ITU-T F.741] Рекомендация МСЭ-Т F.741 (2005 г.), *Описание услуг и требования к аудиовизуальным услугам по запросу.*

[b-ITU-T F.742] Рекомендация МСЭ-Т F.742 (2005 г.), *Описание службы и требования к службам дистанционного обучения.*

[b-ITU-T F.790] Рекомендация МСЭ-Т F.790 (2007 г.), *Руководящие принципы по доступности электросвязи для пожилых людей и людей с ограниченными возможностями.*

[b-ITU-T Climate] ITU-T ICTs and Climate Change (2009), *Deliverable 2: "Gap Analysis and Standards Roadmap"*.

[b-ITU-T G.729A] Recommendation ITU-T G.729 Annex A (1996), *Reduced complexity 8 kbit/s CS-ACELP speech codec*.

[b-ITU-T G.780] Recommendation ITU-T G.780/Y.1351 (2004), *Terms and definitions for synchronous digital hierarchy (SDH) networks*.

[b-ITU-T G.799.1] Recommendation ITU-T G.799.1/Y.1451.1 (2004), *Functionality and interface specifications for GSTN transport network equipment for interconnecting GSTN and IP networks*.

[b-ITU-T G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks*.

[b-ITU-T G.809] Рекомендация МСЭ-Т G.809 (2003 г.), *Функциональная архитектура многоуровневых сетей без установления соединения.*

[b-ITU-T G.1000] Recommendation ITU-T G.1000 (2001), *Communications Quality of Service: A framework and definitions*.

[b-ITU-T G.1010] Recommendation ITU-T G.1010 (2001), *End-user multimedia QoS categories*.

[b-ITU-T H.510] Recommendation ITU-T H.510 (2002), *Mobility for H.323 multimedia systems and services*.

[b-ITU-T H-Sup.1] ITU-T H-series Recommendations – Supplement 1 (1999), *Application profile – Sign language and lip-reading real-time conversation using low bit rate video communication*.

[b-ITU-T I.230] Recommendation ITU-T I.230 (1988), *Definition of bearer service categories*.

[b-ITU-T I.250] Recommendation ITU-T I.250 (1988), *Definition of supplementary services*.

[b-ITU-T I.570] Recommendation ITU-T I.570 (1993), *Public/private ISDN interworking*.

[b-ITU-T M.3017] Рекомендация МСЭ-Т M.3017 (2003 г.), *Принципы интегрального управления смешанными сетями с коммутацией каналов/пакетов.*

[b-ITU-T Q.833.1] Recommendation ITU-T Q.833.1 (2001), *Asymmetric digital subscriber line (ADSL) – Network element management: CMIP model*.

[b-ITU-T Q.1200] Recommendation ITU-T Q.1200 Series (1997), *General series Intelligent Network Recommendation structure*.

[b-ITU-T Q.1236] Recommendation ITU-T Q.1236 (1999), *Intelligent Network Capability Set 3 – Management Information Model Requirements and Methodology*.

[b-ITU-T Q.1702] Recommendation ITU-T Q.1702 (2002), *Long-term vision of network aspects for systems beyond IMT-2000.*

[b-ITU-T Q.1741.1] Рекомендация МСЭ-Т Q.1741.1 (2002 г.), *Ссылки из IMT-2000 для версии 1999 года эволюционировавшей из GSM базовой сети UMTS с использованием сети доступа UTRAN.*

[b-ITU-T Q.1741.2] Recommendation ITU-T Q.1741.2 (2002), *IMT-2000 references to release 4 of GSM evolved UMTS core network with UTRAN access network.*

[b-ITU-T Q.1741.3] Рекомендация МСЭ-Т Q.1741.3 (2003 г.), *Ссылки IMT-2000 на версию 5 центральной сети UMTS развитой GSM.*

[b-ITU-T Q.1741.4] Рекомендация МСЭ-Т Q.1741.4 (2005 г.), *Ссылки, касающиеся IMT-2000, на версию 6 центральной сети UMTS, развитой на основе GSM.*

[b-ITU-T Q.1742.4] Рекомендация МСЭ-Т Q.1742.4 (2005 г.*), Эталонные спецификации IMT-2000 (утверждены по состоянию на 30 июня 2004 года) для развитой базовой сети ANSI-41 с сетью доступа cdma2000.*

[b-ITU-T Q.1761] Recommendation ITU-T Q.1761 (2004), *Principles and requirements for convergence of fixed and existing IMT-2000 systems.*

[b-ITU-T T.140] Recommendation ITU-T T.140 (1998), *Protocol for multimedia application text conversation*.

[b-ITU-T X.501] Recommendation ITU-T X.501 (2008) | ISO/IEC 9594-2:2008, *Information technology – Open Systems Interconnection – The Directory: Models*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.511] Recommendation ITU-T X.511 (2008) | ISO/IEC 9594-3:2008, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*.

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-ITU-T Y.1411] Recommendation ITU-T Y.1411 (2003), *ATM-MPLS network interworking – Cell mode user plane interworking*.

[b-ITU-T Y.2052] Recommendation ITU-T Y.2052 (2008), *Framework of multi-homing in IPv6-based NGN.*

[b-ITU-T Y.2053] Recommendation ITU-T Y.2053 (2008), *Functional requirements for IPv6 migration in NGN.*

[b-ITU-T Y.2054] Recommendation ITU-T Y.2054 (2008), *Framework to support signalling for IPv6-based NGN.*

[b-ITU-T Y-Sup.1] ITU-T Y.2000-series Recommendations – Supplement 1 (2006), *ITU-T Y.2000 series – Supplement on NGN release 1 scope.*

[b-ITU-T Y-Sup.5] ITU-T Y.1900 series Recommendations – Supplement 5 (2008), *ITU-T Y.1900 series – Supplement on IPTV service use cases.*

[b-ITU-T Y-Sup.7] ITU-T Y-series Recommendations – Supplement 7 (2008), *ITU-T Y.2000 series – Supplement on NGN release 2 scope.*

[b-ITU-R M.1645] Recommendation ITU-R M.1645 (2003), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000.*

Руководства МСЭ-Т

[b-ITU-T Accessibility] ITU-T Technical Paper (2006), *FSTP-TACL Telecommunications Accessibility Checklist.*

Технические спецификации ETSI

[b-ETSI TR 121 905] ETSI TR 121 905 V7.3.0 (2007), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications.*

[b-ETSI TS 101 331] ETSI TS 101 331 V1.2.1 (2006), *Lawful Interception (LI); Requirements of Law Enforcement Agencies.*

[b-ETSI TS 122 057] ETSI TS 122 057 V6.0.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Mobile Execution Environment (MExE) service description; Stage 1.*

[b-ETSI TS 122 071] ETSI TS 122 071 V3.5.0 (2004), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Location Services (LCS); Stage 1.*

[b-ETSI TS 122 078] ETSI TS 122 078 V7.6.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Customized Applications for Mobile network Enhanced Logic (CAMEL); Service description.*

[b-ETSI TS 122 127] ETSI TS 122 127 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); Service requirement for the Open Services Access (OSA); Stage 1.*

[b-ETSI TS 122 140] ETSI TS 122 140 V6.7.0 (2005), *Universal Mobile Telecommunications System (UMTS); Multimedia Messaging Service (MMS); Stage 1.*

[b-ETSI TS 122 146] ETSI TS 122 146 V7.2.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Multimedia Broadcast/Multicast Service (MBMS); Stage 1.*

[b-ETSI TS 122 174] ETSI TS 122 174 V6.2.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Push service; Stage 1.*

[b-ETSI TS 122 240] ETSI TS 122 240 V6.5.0 (2005), *Universal Mobile Telecommunications System (UMTS); Service requirements for 3GPP Generic User Profile (GUP); Stage 1.*

[b-ETSI TS 122 250] ETSI TS 122 250 V6.0.0 (2005), *Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS) Group Management; Stage 1.*

[b-ETSI TS 123 141] ETSI TS 123 141 V7.2.0 (2006), *Universal Mobile Telecommunications System (UMTS); Presence service; Architecture and functional description; Stage 2.*

[b-ETSI TS 123 228] ETSI TS 123 228 V7.7.0 (2007), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2.*

[b-ETSI TS 126 235] ETSI TS 126 235 V6.4.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Packet switched conversational multimedia applications; Default codecs.*

[b-ETSI TS 133 106] ETSI TS 133 106 V7.0.1 (2006), *Universal Mobile Telecommunications System (UMTS); Lawful interception requirements.*

[b-ETSI TS 142 033] ETSI TS 142 033 V7.0.0 (2007), *Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 1.*

[b-ETSI TS 181 005] ETSI TS 181 005 V2.4.1 (2007), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements.*

[b-ETSI TS 181 019] ETSI TS 181 019 V2.0.0 (2007), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business Communication Requirements.*

[b-ETSI TS 187 009] ETSI TS 187 009 V2.1.1 (2008), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN.*

Стандарты Американского института национальных стандартов (ANSI)

[b-ANSI-J-STD-025] ANSI-J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance (CALEA).*

[b-ATIS 1000678] ATIS 1000678-2006, *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, Version 2.*

[b-T1.724] ANSI T1.724-2004, *UMTS Handover Interface for Lawful Interception.*

[b-TIA-127-A] TIA-127-A (2004), *Enhanced Variable Rate Codec Speech Option 3 for Wideband Spread Spectrum Digital Systems.*

[b-TIA-1016-A] TIA-1016-A (2006), *Source-Controlled Variable-Rate Multimode Wideband Speech Codec (VMR-WB) – Service Options 62 and 63 for Spread Spectrum Systems.*

[b-TIA-1066] TIA-1066 (2006), *LAES for cdma2000 VoIP.*

[b-TIA-1072] TIA-1072 (2006), *LAES for cdma2000 push-to-talk over cellular.*

Спецификации IETF

[b-IETF RFC 2486] IETF RFC 2486 (1999), *The Network Access Identifier.*

[b-IETF RFC 4594] IETF RFC 4594 (2006), *Configuration Guidelines for DiffServ Service Classes.*

Спецификации открытого альянса мобильной связи

[b-OMA-DS] OMA specification (2006), *Data Synchronization V1.2.*

[b-OMA-DM] OMA specification (2007*), Device Management V1.2.*

[b-OMA-OSE] OMA specification (2007), *Service Environment V1.0.*

[b-OMA-PoC] OMA specification (2006), *Push to talk over Cellular V1.0.1.*

[b-OMA-PS] OMA specification (2006), *Presence Simple V1.0.1.*

[b-OMA-WS] OMA specification (2006), *Web Services V1.1.*

[b-OMA-XML] OMA specification (2006), *XML Document Management.*

[b-OMA-LS] OMA specification (2006), *Mobile Location Service V1.1.*

[b-OMA-XDM] OMA specification (2006), *XML Document Management V1.0.1.*

[b-OMA-Push] OMA specification (2005), *Push V2.1*.

Открытый доступ к услугам (OSA)

[b-OSA-Parlay-X] ETSI ES 202 391-x (2006), *Open Service Access (OSA), Parlay X Web Services, Parts 1-14.*

[b-OSA-Parlay-4] ETSI ES 202 915-x V1.3.1 (2006), *Open Service Access (OSA); Application Programming Interface (API); Parts 1-14 (Parlay 4).*

[b-OSA-Parlay-5] ETSI ES 203 915-x V1.1.1 (2007), *Open Service Access (OSA); Application Programming Interface (API); Parts 1-15 (Parlay 5).*

Услуги ИС

[b-TIA/EIA/IS-771-1] TIA/EIA/IS 771-1 (1999), *Wireless Intelligent Network – Addendum 1 (2001).*

[b-TIA-873.002] TIA-873.002 (2003), *All IP Core Network Multimedia Domain – IP Multimedia Subsystem – Stage-2 (2003).*

Спецификации UDDI

[b-OASIS-UDDI] OASIS specification (2004), *UDDI Version 3.0.2.*

Спецификации SOA

[b-OASIS-SOA] OASIS specification (2006), *Reference Model for Service Oriented Architecture 1.0.*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование услуг и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией услуг
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных услуг
Серия T	Оконечное оборудование для телематических услуг
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных и взаимосвязь открытых систем
Серия Y	**Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2010 г.