Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2205

(05/2011)

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

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

Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения

Рекомендация МСЭ-Т Y.2205

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
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	
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	Y.1900–Y.1999
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
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
Будущие сети	Y.3000–Y.3099

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

Рекомендация МСЭ-Т Y.2205

Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения

Резюме

В Рекомендации МСЭ-Т Y.2205 изложены технические соображения, которые в необязательном порядке могут применяться в сетях последующих поколений (СПП) для обеспечения электросвязи в чрезвычайных ситуациях (ЕТ). Кроме того, в этой Рекомендации приводятся основополагающие технические принципы, используемые при обеспечении ЕТ.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т Y.2205	12.09.2008 г.	13-я
2.0	МСЭ-Т Y.2205	20.05.2011 г.	13-я

Ключевые слова

Архитектура, раннее предупреждение (EW), электросвязь в чрезвычайных ситуациях, служба электросвязи в чрезвычайных ситуациях (ETS), СПП, предпочтительная электросвязь, приоритетная электросвязь, QoS (качество обслуживания), электросвязь для оказания помощи при бедствиях (TDR).

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

Введение

В [ITU-T Y.1271] содержится описание требований к сети и возможностей сети для обеспечения электросвязи в чрезвычайных ситуациях. Как показывает опыт деятельности органов власти, ответственных за координацию операций по оказанию помощи при бедствиях с использованием сетей общего пользования, осуществление приоритетной электросвязи на основе этих требований может привести к созданию новых механизмов, а также к повторному использованию на основе межсетевого взаимодействия существующих механизмов. Электросвязь в чрезвычайных ситуациях должна пользоваться преимущественным режимом по сравнению с обычными услугами сетей общего пользования. Термин "предпочтительная электросвязь" используется в ряде Рекомендаций МСЭ-Т для охвата услуг, требующих приоритетного режима. Служба электросвязи в чрезвычайных ситуациях – это одна из категорий служб, которая рассматривается как пользующаяся преимущественным режимом. Эти два термина "предпочтительная электросвязь" и "электросвязь в чрезвычайных ситуациях" используются взаимозаменяемо.

Идея приоритетной электросвязи, используемой в чрезвычайных ситуациях, не нова; в течение многих лет сети с коммутацией каналов обеспечивали работу таких систем, в основном, для голосовых вызовов (см., например, [ITU-T E.106]). Однако что касается технических методов, используемых для обеспечения выполнения этих основополагающих требований к электросвязи в чрезвычайных ситуациях в среде СПП, то они развиваются. Традиционные методы установления приоритета, используемые при коммутации каналов, могут не применяться в СПП вследствие различий, присущих электросвязи с коммутацией каналов и с коммутацией пакетов.

В [ITU-T Y.1271] в общем и теоретическом виде изложены требования и возможности. [ITU-T Y.1271] является нейтральной в технологическом отношении.

В связи с тем что СПП основаны на технологии коммутации пакетов, которая принципиально отличается от технологии коммутации каналов, требуется рассмотреть технические вопросы и возможные решения, которые могли бы использоваться для реализации возможностей электросвязи в чрезвычайных ситуациях в СПП.

В настоящей Рекомендации определяются технические соображения, которые могут применяться в СПП для обеспечения электросвязи в чрезвычайных ситуациях, а также для реализации используемых основополагающих принципов.

Рекомендация МСЭ-Т Y.2205

Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения

1 Сфера применения

В настоящей Рекомендации описываются технические соображения, которые могут применяться в сетях последующих поколений (СПП) для обеспечения электросвязи в чрезвычайных ситуациях (ЕТ). Кроме того, в данной Рекомендации приводятся основополагающие технические принципы, используемые для обеспечения ЕТ. В Рекомендации определяются требования и возможности ЕТ, помимо тех, которые установлены в отношении СПП в [ITU-T Y.2201] (как определено в [ITU-T Y.2001] и далее описано в [ITU-T Y.2011]).

К электросвязи в чрезвычайных ситуациях (включая обеспечение некоторых элементов раннего предупреждения (см. рисунок 1)) относится:

- электросвязь в чрезвычайных ситуациях между отдельным лицом и органом власти, например звонки оператору службы экстренного вызова;
- электросвязь в чрезвычайных ситуациях между органами власти;
- электросвязь в чрезвычайных ситуациях между органом власти и отдельным лицом, например службы оповещения общественности.

В Дополнении I представлена дополнительная информация, касающаяся перечисленных выше категорий ЕТ.

Определен также ряд требований и возможностей в отношении раннего предупреждения. Возможности электросвязи в чрезвычайных ситуациях между отдельным лицом и органом власти не рассматриваются и выходят за рамки сферы применении настоящей Рекомендации.

Некоторые технические средства, описанные в этом документе, могли бы также использоваться для электросвязи в чрезвычайных ситуациях между отдельным лицом и органом власти или между отдельными лицами, однако эти категории не рассматриваются в настоящей Рекомендации.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

2.1 МСЭ-Т

[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 G.808.1] Рекомендация МСЭ-Т G.808.1 (2010 г.), *Обобщенная защитная коммутация – Линейная защита канала и подсети*.

[ITU-T G.841] Рекомендация МСЭ-Т G.841 (1998 г.), *Типы и характеристики защитных архитектур SDH сетей*.

[ITU-T G.842] Recommendation ITU-T G.842 (1997), *Interworking of SDH network protection architectures*.

[ITU-T G.873.1] Рекомендация МСЭ-T G.873.1 (2006 г.), *Оптическая транспортная сеть (OTN): Линейная защита*.

[ITU-T G.983.1] Рекомендация МСЭ-T G.983 (2005 г.), *Оптические системы широкополосного доступа, базирующиеся на пассивной оптической сети (PON).*

[ITU-T G.8031] Recommendation ITU-T G.8031/Y.1342 (2009), *Ethernet linear protection switching*.

[ITU-T G.8032] Recommendation ITU-T G.8032/Y.1344 (2010*), Ethernet ring protection switching*.

[ITU-T G.8131] Recommendation ITU-T G.8131/Y.1382 (2007), *Linear protection switching for transport MPLS (MPLS-TP) networks*.

[ITU-T H.248.1] Recommendation ITU-T H.248.1 (2005), *Gateway control protocol: Version 3*.

[ITU-T H.248.81] Recommendation ITU-T H.248.81 (2011), *Gateway control protocol: Guidelines on the use of the international emergency preference scheme (IEPS) call indicator and priority indicator in ITU-T H.248 profiles*.

[ITU-T H.323] Recommendation ITU-T H.323 (2009), *Packet-based multimedia communications systems*.

[ITU-T H.460.4] Recommendation ITU-T H.460.4 (2007), *Call priority designation and country/international network of call origination identification for H.323 priority calls*.

[ITU-T I.630] Recommendation ITU-T I.630 (1999), *ATM protection switching*.

[ITU-T J.260] Рекомендация МСЭ-T J.260 (2005 г.), *Требования к предпочтительному использованию средств электросвязи в сетях IPCablecom*.

[ITU-T J.261] Recommendation ITU-T J.261 (2009), *Framework for implementing preferential telecommunications in IPCablecom and IPCablecom2 networks*.

[ITU-T J.262] Recommendation ITU-T J.262 (2009), *Specifications for authentication in preferential telecommunications over IPCablecom2 networks*.

[ITU-T J.263] Recommendation ITU-T J.263 (2009)*, Specification for priority in preferential telecommunications over IPCablecom2 networks*.

[ITU-T Q.812] Recommendation ITU-T Q.812 (2004), *Upper layer protocol profiles for the Q and X interfaces.*

[ITU-T Q.1741.6] Recommendation ITU-T Q.1741.6 (2009), *IMT-2000 references to Release 8 of GSM-evolved UMTS core network*.

[ITU-T Q.3303.3] Recommendation ITU-T Q.3303.3 (2008), *Resource control protocol No. 3 – Protocols at the Rw interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE): Diameter*.

[ITU-T Q.3321.1] Recommendation ITU-T Q.3321.1 (2010), *Resource control protocol No. 1, version 2 – Protocol at the Rs interface between service control entities and the policy decision physical entity*.

[ITU-T Q-Sup.57] ITU-T Q-series Recommendations – Supplement 57 (2008), *Signalling requirements to support the emergency telecommunications service (ETS) in IP networks*.

[ITU-T X.660] Recommendation ITU-T X.660 (2008) | ISO/IEC 9834-1:2008, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the International Object Identifier tree*.

[ITU-T X.674] Recommendation ITU-T X.674 (2011), *Procedures for the registration of arcs under the Alerting object identifier arc*.

[ITU-T X.1303] Recommendation ITU-T X.1303 (2007), *Common alerting protocol (CAP 1.1*).

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

[ITU-T Y.1271] Рекомендация МСЭ-T 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-T Y.1541 (2006 г.), *Требования к сетевым показателям качества для служб, основанных на протоколе IP*.

[ITU-T Y.1720] Recommendation ITU-T Y.1720 (2006), *Protection switching for MPLS networks*.

[ITU-T Y.2001] Рекомендация МСЭ-T Y.2001 (2004 г.), *Общий обзор СПП*.

[ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

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

[ITU-T Y.2171] Рекомендация МСЭ-T Y.2171 (2006 г.), *Уровни приоритета при управлении доступом в сетях последующих поколений.*

[ITU-T Y.2172] Recommendation ITU-T Y.2172 (2007), *Service restoration priority levels in Next Generation Networks*.

[ITU-T Y.2201] Рекомендация МСЭ-T Y.2201 (2007 г.), *Требования к СПП МСЭ-T и возможности этих сетей*.

[ITU-T Y.2701] Рекомендация МСЭ-T Y.2701 (2007 г.), *Требования к безопасности для сетей последующих поколений версии 1*.

[ITU-T Y.2702] Рекомендация МСЭ-T Y.2702 (2008 г.), *Требования к аутентификации и авторизации для СПП варианта 1*.

[ITU-T Y.2704] Рекомендация МСЭ-T Y.2704 (2010 г.), *Механизмы и процедуры безопасности для сетей последующих поколений*.

[ITU-T Y.2720] Рекомендация МСЭ-T Y.2720 (2009 г.), *Структура управления определением идентичности в СПП.*

[ITU-T Y.2721] Recommendation ITU-T Y.2721 (2010*), NGN identity management requirements and use cases*.

[ITU-T Y.2722] Recommendation ITU-T Y.2722 (2011), *NGN identity management mechanisms*.

2.2 IETF

[IETF RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification.*

[IETF RFC 3168] IETF RFC 3168 (2001), *The Addition of Explicit Congestion Notification (ECN) to IP*.

[IETF RFC 3246] IETF RFC 3246 (2002), *An Expedited Forwarding PHB (Per-Hop Behavior)*.

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[IETF RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP)*.

[IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[IETF RFC 4340] IETF RFC 4340 (2006), *Datagram Congestion Control Protocol (DCCP)*.

[IETF RFC 4412] IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP)*.

[IETF RFC 4542] IETF RFC 4542 (2006), *Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite*.

[IETF RFC 4594] IETF RFC 4594 (2006), *Configuration Guidelines for DiffServ Service Classes*.

[IETF RFC 5865] IETF RFC 5865 (2010), *A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic*.

2.3 ETSI

[ETSI TS 183 017] ETSI TS 183 017 V3.2.1 (2010), *TISPAN Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification.*

2.4 Broadband Forum

[BBF TR-058] Broadband Forum TR-058 (2003), *Multi-Service Architecture and Framework Requirements*.

[BBF TR-059] Broadband Forum TR-059 (2003), *DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services*.

[BBF TR-101] Broadband Forum TR-101 (2011), *Migration to Ethernet-Based DSL Aggregation*.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 оповещение (alert) [ITU-T X.674]: Сообщение, предназначенное для предупреждения или оповещения о грозящей опасности или возможной проблеме.

3.1.2 оповещающее учреждение (alerting agency) [ITU-T X.674]: Национальная, региональная или международная структура, ответственная за обеспечение оповещения.

3.1.3 служба электросвязи в чрезвычайных ситуациях (ETS) (emergency telecommunications service) [ITU-T E.107]: Национальная служба, предоставляющая приоритетную электросвязь авторизованным пользователям ETS в период бедствий и чрезвычайных ситуаций.

3.1.4 сети последующих поколений (next generation network) (СПП) [ITU-T Y.2001]: Сеть с пакетной коммутацией, пригодная для предоставления услуг электросвязи и для использования нескольких широкополосных технологий транспортирования с включенной функцией QoS, в которой связанные с обслуживанием функции не зависят от применяемых технологий, обеспечивающих транспортирование. Она обеспечивает свободный доступ пользователей к сетям и конкурирующим поставщикам услуг и/или выбираемым ими услугам. Она поддерживает универсальную подвижность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 электросвязь в чрезвычайных ситуациях (emergency telecommunications) (ET): ET означает любую службу, связанную с чрезвычайными ситуациями, для которой требуется специальная обработка со стороны СПП, по сравнению с другими службами. К таким службам относятся службы экстренного вызова, уполномоченные властями, и службы общественной безопасности.

3.2.2 предпочтительная электросвязь (preferential telecommunications): Это категория служб, для которой обеспечивается преимущественный доступ к ресурсам сети электросвязи и/или их использование.

3.2.3 электросвязь для оказания помощи при бедствиях (telecommunications for disaster relief) (TDR): TDR представляет собой возможности использования международной и национальной электросвязи для целей оказания помощи при бедствиях. Для TDR могут использоваться на постоянной или совместной основе международные сетевые средства, которые уже введены в действие и эксплуатируются; временные сетевые средства, которые предоставляются конкретно для TDR, либо подходящая комбинация из этих двух вариантов.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения:

AAA	Authentication, Authorization, and Accounting	Аутентификация, авторизация и учет
AF	Application Function	Прикладная функция
ANMS	Access Node Management System	Система управления узлами доступа
APS	Automatic Protection Switching	Автоматическая защитная коммутация
AQM	Active Queue Management	Активное управление очередью
ASN	Access Service Network	Служебная сеть доступа
ASN.1	Abstract Syntax Notation One	Абстрактно-синтаксическая нотация 1
BNG	Broadband Network Gateway	Шлюз широкополосной сети
BS	Base Station	Базовая станция
CAC	Call Admission Control	Управление допуском вызова
CAP	Common Alerting Protocol	Протокол общего оповещения
CPE	Customer Premises Equipment	Оборудование в помещении клиента
DCCP	Data Congestion Control Protocol	Протокол управления перегрузкой данных
DoS	Denial of Service	Отказ в обслуживании
DSCP	Diff-Serv Code Points	Указатели кода дифференцированного обслуживания
DSLAM	Digital Subscriber Line Access Multiplexer	Мультиплексор доступа к цифровой абонентской линии

EAS	Emergency Alert System		Система оповещения о чрезвычайной ситуации
ECN	Explicit Congestion Notification		Явное уведомление о перегрузке
EF	Expedited Forwarding		Срочная пересылка данных
E-MTA	Embedded Muti-terminal adapter		Встроенный мультимедийный адаптер терминала
ENI	ETS National Implementation		Реализованная на национальном уровне служба ETS
ET	Emergency Telecommunications		Электросвязь в чрезвычайных ситуациях
ETH	Ethernet Layer Network		Сеть уровня Ethernet
ETS	Emergency Telecommunications Service		Служба электросвязи в чрезвычайных ситуациях
EW	Early Warning		Раннее предупреждение
GETS	Government Emergency Telecommunications Service		Служба правительственной электросвязи в чрезвычайных ситуациях
IEPS	International Emergency Preference Scheme		Международная система предпочтений при чрезвычайных ситуациях
IP	Internet Protocol		Протокол Интернет
ISDN	Integrated Services Digital Network	ЦСИС	Цифровая сеть с интеграцией служб
LAN	Local Area Network	ЛВС	Локальная сеть
LSP	Label Switched Path		Тракт, коммутируемый с использованием меток
MDF	Main Distribution Frame		Главный коммутационный щит
MMPS	Multimedia Priority Service		Приоритетное обслуживание мультимедийного трафика
MPS	Multimedia Priority Service		Приоритетное обслуживание мультимедийного трафика
MPLS	MultiProtocol Label Switching		Многопротокольная коммутация с использованием меток
MS	Multiplex Section		Мультиплексная секция
NID	Network Interface Device		Устройство сопряжения с сетью
NOAA	National Oceanic and Atmospheric Administration		Национальное управление океанических и атмосферных исследований
NGN	Next Generation Network	СПП	Сети последующих поколений
ODUk	Optical channel Data Unit k		Блок данных оптического канала k
OLT	Optical Line Termination		Окончание оптической линии
OMCI	ONT Management and Control Interface		Интерфейс контроля и управления ONT
ONT	Optical Network Termination		Оконечное оборудование оптической сети
OTN	Optical Transport Network		Оптическая транспортная сеть
P-CSC-FE	Proxy Call Session Control Functional Entity		Прокси-функциональный объект управления вызовом/сеансом
PCC	Policy and Charging Control		Управление политикой и начислением платы
PDP	Policy Decision Point		Точка выбора правил
PEP	Policy Enforcement Point		Точка применения правил
PF	Policy Function		Функция политики
PHB	Per Hop Behaviour		Пошаговый режим работы
PIN	Personal Identification Number		Персональный идентификационный номер
PLMN	Public Land Mobile Network		Сеть сухопутной подвижной связи общего пользования

PON	Passive Optical Network		Пассивная оптическая сеть
POTS	Plain Old Telephone Service		Традиционная аналоговая телефонная служба
PSAP	Public Safety Answering Point		Пункт сообщений общественной безопасности
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования
RACF	Resource and Admission Control Function		Функция управления ресурсами и допуском
RPH	Resource Priority Header		Заголовок приоритета ресурса
RSVP	Resource ReSerVation Protocol		Протокол резервирования ресурсов
QoS	Quality of Service		Качество обслуживания
SAME	Specific Area Message Encoding		Протокол кодирования сообщений для конкретного района
SCF	Service Control Function		Функция управления обслуживанием
SDH	Synchronous Digital Hierarchy	СЦИ	Синхронная цифровая иерархия
SIP	Session Initiation Protocol		Протокол инициации сеанса
SLA	Service Level Agreement		Соглашение об уровне обслуживания
SNC	SubNetwork Connection		Соединение подсети
SNCP	SubNetwork Connection Protection		Защита соединений подсети
SS7	Signalling System No.7		Система сигнализации № 7
TCP	Transmission Control Protocol		Протокол управления передачей
TDM	Time Division Multiplexing		Временное разделение каналов
TDR	Telecommunications for Disaster Relief		Электросвязь для оказания помощи при бедствиях
T-MPLS	Transport MPLS		Транспортная MPLS
UDP	User Datagram Protocol		Протокол дейтаграмм пользователя
UE	User Equipment		Оборудование пользователя
UN/ISDR	United Nations International Strategy for Disaster Reduction		Международная стратегия ООН уменьшения опасности бедствий
USI	Universal Services Interface		Универсальный интерфейс услуг
VC	Virtual Channel		Виртуальный канал
VLAN	Virtual LAN		Виртуальная ЛВС
VoIP	Voice over IP		Передача голоса по протоколу IP
VP	Virtual Path		Виртуальный маршрут
W-CDMA	Wideband Code Division Multiple Access		Широкополосный многостанционный доступ с кодовым разделением каналов
WPS	Wireless Priority Service		Беспроводная приоритетная служба
xDSL	Any variant of Digital Subscriber Line		Любой вариант цифровой абонентской линии
XML	Xtensible Markup Language		Расширяемый язык разметки
XSD	XML Schema Definition		Определение схемы XML

5 Описание электросвязи в чрезвычайных ситуациях (ET) и раннего предупреждения

5.1 Общие положения

В настоящей Рекомендации используются следующие термины:

- электросвязь в чрезвычайных ситуациях – ET;
- служба электросвязи в чрезвычайных ситуациях – ETS;

- электросвязь для оказания помощи при бедствиях – TDR;
- раннее предупреждение – EW.

Важно отметить, что имеется согласие и понимание в отношении различных вариантов использования этих терминов. В связи с этим, приведенные ниже термины используются следующим образом:

- ET – обобщающий термин для любой службы, связанной с чрезвычайными ситуациями, для которой требуется специальная обработка со стороны СПП, по сравнению с другими службами;
- ETS – определение этого термина дано в [ITU-T E.107];
- TDR – общий термин для обозначения возможности использования электросвязи для целей оказания помощи при бедствиях;
- EW – общий термин для обозначения всех типов систем, возможностей и служб раннего предупреждения.

Такой порядок образует дерево, в котором корнем всех видов деятельности является ET. Использование терминов и их взаимосвязь отображены на рисунке 1, ниже.

Как было отмечено во введении, в ряде Рекомендаций МСЭ-Т, в особенности в Рекомендациях МСЭ-Т серии J.26x, термин "предпочтительная электросвязь" используется для включения служб, которые требуют специальной обработки по сравнению с другими службами. В настоящей Рекомендации термин "предпочтительная электросвязь" используется только в контексте Рекомендаций МСЭ-Т серии J.26x. В Рекомендациях МСЭ-Т серии J.26x термин "предпочтительная электросвязь" включает ETS, TDR и EW.

* Включая некоторые аспекты раннего предупреждения.
** Может также применяться к электросвязи между органом власти и отдельным лицом.

Y.2205(11)_F01

Рисунок 1 – Структура терминологического взаимоотношения для электросвязи в чрезвычайных ситуациях

5.2 Электросвязь в чрезвычайных ситуациях

Электросвязь в чрезвычайных ситуациях (ET) означает любую службу, связанную с чрезвычайными ситуациями, для которой требуется специальная обработка со стороны СПП, по сравнению с другими службами. К таким службам относятся службы экстренного вызова, уполномоченные властями, и службы общественной безопасности. Ниже приводятся конкретные примеры служб в рамках электросвязи в чрезвычайных ситуациях:

1) Электросвязь для оказания помощи при бедствиях (TDR)

TDR представляет возможности использования международной и национальной электросвязи для целей оказания помощи при бедствиях. Для TDR могут использоваться на постоянной или совместной основе международные сетевые средства, которые уже введены в действие и эксплуатируются; временные сетевые средства, которые предоставляются конкретно для TDR, либо подходящая комбинация из этих двух вариантов.

2) Служба электросвязи в чрезвычайных ситуациях (ETS)

ETS является национальной службой, предоставляющей приоритетную электросвязь авторизованным пользователям ETS в период бедствий и чрезвычайных ситуаций. Описание ETS определяется в [ITU-T E.107]. В [ITU-T E.107] приводится руководство, которое позволит обеспечивать электросвязь между одной реализованной на национальном уровне ETS (ENI) и другой (другими) ENI (электросвязь между органами власти).

3) Национальные/региональные/местные службы экстренного вызова и общественной безопасности

К другим примерам ЕТ относятся национальные, региональные, местные службы экстренного вызова и общественной безопасности. Они являются специализированными службами для целей обеспечения экстренного вызова и общественной безопасности на национальном, региональном, местном уровне. Эти службы экстренного вызова зависят от национальных, региональных или местных условий и подлежат стандартизации на национальном или региональном уровне.

5.3 Раннее предупреждение

Международная стратегия ООН уменьшения опасности бедствий (МСУОБ ООН) в своем докладе [b-UN Global Survey] Генеральному секретарю Организации Объединенных Наций (ООН), сентябрь 2006 года, озаглавленном "Глобальный обзор систем раннего предупреждения", раннее предупреждение определяет как "предоставление через конкретные учреждения своевременной и эффективной информации, позволяющей подвергающимся опасности лицам принять меры для того, чтобы избежать риска или снизить его и подготовиться к эффективному реагированию". В этом докладе ООН приводится оценка способностей, разрывов и возможностей, связанных с созданием всеобъемлющей глобальной системы раннего предупреждения обо всех стихийных бедствиях.

6 Общие соображения, касающиеся электросвязи в чрезвычайных ситуациях и раннего предупреждения

До разработки [ITU-T Y.1271] требования к возможностям электросвязи в чрезвычайных ситуациях относились прежде всего к сетям с коммутацией каналов, например коммутируемым телефонным сетям общего пользования (КТСОП).

Эти требования основывались на определенных характеристиках сетей с коммутацией каналов и учитывали преимущества таких сетей. Например:

- при управлении допуском используется жесткая связь между ресурсами сигнализации и среды передачи;
- весь трафик медиаданных, для которого требуется равномерная полоса пропускания, передается с постоянной скоростью;
- полоса пропускания резервируется для каждого потока данных;
- разделение трафика управления и трафика данных.

Эти характеристики необязательно обеспечиваются в современных сетях с коммутацией пакетов с негарантированным обслуживанием, при котором:

- в сетях с коммутацией пакетов обычно совместно используются ресурсы и организуются очереди, с тем чтобы компенсировать неравномерный характер трафика; сочетание этих способов обычно и составляет основу негарантированного обслуживания;
- управление допуском может вызывать трудности: многие приложения не сообщают о полосе пропускания, которая требуется для них, и сигнализация не связана со средой передачи;
- приложениям и услугам требуется разная полоса пропускания, и они могут передавать данные с динамически устанавливаемыми скоростями;
- для различных потоков пакетов совместно используется полоса пропускания, обеспечиваемая за счет статистического мультиплексирования;
- для трафика управления и данных могут совместно использоваться одни и те же ресурсы сети.

Кроме того, если не принимать специальных мер, то в СПП с пакетной коммутацией пакеты могут "бороться" за имеющуюся полосу пропускания. На чистом транспортном уровне пакетам не может быть свободно отказано в обслуживании и к ним не может быть свободно применено управление потоком. Кроме того, расчет нагрузки в сетях с коммутацией пакетов существенно отличается

от расчета для сетей с коммутацией каналов в части, касающейся стандартных общепринятых подходов. На заданный "поток" пакетов могут воздействовать другие потоки пакетов, совместно использующие ресурсы, если соответствующим образом не применяются меры, доступные в СПП. С другой стороны, разделение обслуживания и транспортирования в СПП может обеспечивать преимущество с точки зрения предоставления более гибких и разнообразных возможностей для электросвязи в чрезвычайных ситуациях.

Эти условия означают, что предоставление возможностей электросвязи в чрезвычайных ситуациях не является чем-то совершенно понятным, очевидным и простым. Также нельзя просто воздействовать на транспортирование, как это было в случае сетей с коммутацией каналов. Другие существенные различия между сетями с коммутацией каналов и с коммутацией пакетов, а также между разными технологиями пакетной коммутации, будут оказывать воздействие на обеспечение и выполнение различных требований, указанных в [ITU-T Y.1271].

Следовательно, данная Рекомендация предназначена для того, чтобы указать, какие свойства и механизмы СПП могут быть использованы для содействия выполнению требований обеспечения электросвязи в чрезвычайных ситуациях, а также некоторых аспектов раннего предупреждения. Вместе с тем, при рассмотрении протоколов, механизмов и средств обеспечения электросвязи в чрезвычайных ситуациях, желательно избегать введения функций или требований, так как даже полезные новшества могут привести к усложнению без существенного выигрыша. При добавлении, например, новых функций для "приоритета", следует тщательно учитывать расходование ресурсов на служебные цели и прочие последствия.

7 Общие функциональные требования и возможности

К числу функциональных требований и возможностей относятся указанные в [ITU-T Y.1271] и [ITU-T Y.2201] для СПП, а также те, которые выявлены по результатам проведенного ООН Глобального обзора систем раннего предупреждения в отношении развития СПП [b-UN Global Survey].

7.1 Электросвязь в чрезвычайных ситуациях

В таблице 1 перечислены функциональные требования и возможности электросвязи в чрезвычайных ситуациях.

Таблица 1 – Список функциональных требований и возможностей электросвязи в чрезвычайных ситуациях

Функциональные требования и возможности электросвязи в чрезвычайных ситуациях
Усовершенствованный приоритетный режим
Защищенные сети
Конфиденциальность данных о местоположении
Восстанавливаемость
Возможность установления соединения с сетью
Возможность взаимодействия
Мобильность
Повсеместное покрытие
Живучесть/долговечность
Передача в реальном времени: голос/текст в реальном времени и видео/изображения (если позволяет полоса пропускания)
Передача не в реальном времени: сообщения/потоки данных не в реальном времени (аудио/видео)
Расширяемость полосы пропускания
Надежность/готовность

Цель состоит в том, чтобы обеспечить высокую степень уверенности и вероятности того, что критически важная связь доступна авторизованным пользователям, например имеющим непосредственное отношение к электросвязи в чрезвычайных ситуациях, и надежно работает. В [ITU-T Y.1271] приводятся "Концептуальные требования и сетевые ресурсы для обеспечения экстренной связи по сетям связи, находящимся в стадии перехода от коммутации каналов к коммутации пакетов".

В случае передачи видео и изображений следует учитывать наличие полосы пропускания (например, вида ресурса).

Специальные сетевые функции электросвязи в чрезвычайных ситуациях можно разделить по следующим категориям: вызов услуги, аутентификация и авторизация, сквозной приоритетный режим, присоединение сетей и взаимодействие протоколов.

Вызов услуги относится к взаимодействию пользователя с пользовательским элементом (например, телефоном) и сети с информацией, которая означает запрос службы электросвязи в чрезвычайных ситуациях к сети поставщика услуг. Для распознавания запроса существуют различные подходы, включая предусмотренные в контракте условия. Информация о контракте используется для авторизации определенных запросов службы.

Аутентификация и авторизация выполняются поставщиком услуг в целях предоставления пользователю доступа или отказа в доступе к вызываемой услуге для электросвязи в чрезвычайных ситуациях. Предполагается, что авторизация осуществляется базовой сети.

Сквозной приоритетный режим – это набор возможностей, используемых сетью (сетями) при обеспечении высокой вероятности установления и поддержания обслуживания, от исходящей сети до сети, завершающей связь, включая все транзитные сети. Приоритетный режим существует, начиная с вызова услуги и до ее завершения. Приоритетный режим включен в управление допуском и распределение сетевых ресурсов, а также в транспортирование сигнализации и пакетов медианосителей элементами сети, поддерживающими эту услугу.

Присоединение сетей и взаимодействие протоколов необходимы для обеспечения сквозного приоритетного режима для транспортирования сигнализации и медиа-транспортирования по многим сетям, которые принадлежат разным поставщикам и в которых используются разные технологии. В качестве примера уровни приоритета могут изменяться в зависимости от используемой технологии в нескольких сетях, и может потребоваться отображение с одного уровня, определенного в данной технологии, на другой.

7.2 Раннее предупреждение

Для систем раннего предупреждения необходима эффективная система связи, отличающаяся надежностью и устойчивостью. К числу задач, которые должны выполняться для обеспечения систем раннего предупреждения в условиях СПП как систем связи, относятся:

- возможность непрерывной работы; системы должны находиться в исправном состоянии, быть устойчивыми и доступными в любой момент времени;
- предоставление требуемых возможностей электросвязи для передачи в реальном времени (например, сейсмической информации и данных об уровне моря);
- использование в качестве основы согласованных на международном уровне стандартов;
- обеспечение целостности систем раннего предупреждения и целостности и аутентичности сообщений (то есть обеспечение отправки только авторизованных сообщений);
- передача предупреждающих сообщений только тем, кто, возможно, будет затронут надвигающимся бедствием, и предотвращение передачи не целевых и не требующихся сообщений (например, сообщений, отправленных не тем лицам и/или сообщений, не содержащих полезной и важной информации).

Для обеспечения передачи предупреждающих сообщений только тем, кто, возможно, будет затронут надвигающимся бедствием, перед системами раннего предупреждения могут стоять задачи, связанные с фильтрацией сообщений, с тем чтобы выбирать:

- группы пользователей;
- район или географическую область и т. д.

(например, вид "сотового вещания").

8 Общие руководящие принципы и требования в отношении безопасности

8.1 Общие руководящие принципы

Сетевые элементы, системы, ресурсы, данные и услуги, используемые для обеспечения электросвязи в чрезвычайных ситуациях, могут стать объектом кибератак. Целостность, конфиденциальность и готовность электросвязи в чрезвычайных ситуациях, особенно подвергаясь атакам, будут зависеть от услуг и практических мер безопасности, реализованных в СПП, а также от возможностей безопасности (например, функции аутентификации и авторизации пользователей), реализованных как часть прикладной функции для электросвязи в чрезвычайных ситуациях. Общие руководящие принципы, которые следует рассматривать при планировании электросвязи в чрезвычайных ситуациях, включают (в том числе) следующие:

- Все аспекты электросвязи в чрезвычайных ситуациях, включая сигнализацию и управление, носитель/медиа, и данные и информацию, связанные с управлением (например, информация профиля пользователя) необходимо защищать от угроз безопасности. Угрозы безопасности могут возникать на разных слоях (например, транспортный, управление обслуживанием или обеспечение обслуживания) и в разных сегментах сети (то есть доступ, базовая сеть и интерфейсы присоединения).
- Установление и обеспечение выполнения политики и практических мер безопасности, специально предназначенных для электросвязи в чрезвычайных ситуациях. Следует определять и реализовывать возможности ослабления для обеспечения защиты от различных угроз безопасности. В частности, для электросвязи в чрезвычайных ситуациях необходимо определять и реализовывать возможности ослабления и практические меры безопасности, превышающие те, которые предназначены для общих прикладных услуг. К ним относятся стратегические меры для защиты данных управления и сохраняемой информации (например, информация профилей пользователей), относящихся к электросвязи в чрезвычайных ситуациях.
- Реализация и использование процедур для аутентификации и авторизации пользователей, устройств и сочетания пользователя и устройства для защиты от несанкционированного доступа к услугам, ресурсам и информации (например, информация о пользователях в серверах аутентификации и системах управления), связанные с электросвязью в чрезвычайных ситуациях. Например, следует реализовать функции аутентификации и авторизации в целях предотвращения использования ресурсов, предназначенных для электросвязи в чрезвычайных ситуациях, неавторизованными пользователями, с тем чтобы предотвратить отказ в обслуживании (DoS) и другие формы атак.
- Ответственность в рамках каждой сети за безопасность в пределах своего домена сообщений, которые пересекают несколько доменов поставщиков сетей, так чтобы могла гарантироваться сквозная связь. Поскольку электросвязь в чрезвычайных ситуациях может включать сообщения, проходящие через домены разных поставщиков сетевых услуг в национальных и международных сетях (то есть стран и администраций), необходимо установить и реализовать политику безопасности, доверительные отношения, методы и процедуры идентификации трафика электросвязи в чрезвычайных ситуациях, управление определением идентичности и аутентификацию пользователей и сетей в пределах многих доменов административного управления сетью.

Более подробная информация содержится в [b-ATIS-1000010].

8.2 Общие требования

Рекомендации по безопасности, содержащиеся в [ITU-T Y.2701], [ITU-T Y.2702] и [ITU-T Y.2704], и Рекомендации по управлению определением идентичности (IdM), содержащиеся в [ITU-T Y.2720], [ITU-T Y.2721] и [ITU-T Y.2722], действительны для обеспечения безопасности электросвязи в чрезвычайных ситуациях.

8.2.1 Контроль доступа

Доступ к электросвязи в чрезвычайных ситуациях и любым связанным с ней ресурсам должен разрешаться только авторизованным пользователям. Должен быть предотвращен любой несанкционированный доступ, такой как доступ злоумышленников, маскирующихся под авторизованных пользователей.

8.2.2 Аутентификация

Для защиты безопасности необходимы механизмы и возможности идентификации, аутентификации и авторизации доступа пользователя, устройства или сочетания пользователя и устройства электросвязи в чрезвычайных ситуациях, на основе политики[1] и уровня гарантирования, применимых к конкретной услуге (например, передача голоса, данных, видео).

8.2.3 Конфиденциальность и неприкосновенность частной жизни

Необходима защита конфиденциальности и неприкосновенности частной жизни в среде электросвязи в чрезвычайных ситуациях и защита информации конечных пользователей. Это включает защиту сигнализации, трафика управления и носителя электросвязи в чрезвычайных ситуациях в отношении конфиденциальности и неприкосновенности частной жизни и защиту информации конечных пользователей (например, идентичность, информация контракта и местонахождения) и деятельности в соответствующих случаях.

8.2.4 Безопасность связи

Необходима защита электросвязи в чрезвычайных ситуациях от проникновений (например, предотвращение незаконного прослушивания, перехвата или повторной передачи сигнализации или трафика носителя).

8.2.5 Целостность данных

Необходима защита целостности (например, защита от несанкционированного изменения, удаления, создания или повторного использования). Это включает защиту целостности информации электросвязи в чрезвычайных ситуациях и любых данных конфигурации (например, маркирование приоритета, информация о приоритетах, сохраняемая в функциях стратегических решений, уровень приоритета пользователя и т. д.).

8.2.6 Готовность

Должна обеспечиваться защита готовности электросвязи в чрезвычайных ситуациях. В частности, электросвязь в чрезвычайных ситуациях и все связанные с ней ресурсы должны защищаться от отказа в обслуживании (DoS) и других форм атак.

9 Механизмы и возможности обеспечения электросвязи в чрезвычайных ситуациях в СПП

9.1 Общие положения

Отделение управления обслуживанием/приложениями от транспортирования, позволившее раздельно предлагать прикладные услуги и транспортные услуги и обеспечивать их независимое развитие, является важной характеристикой СПП. Такое отделение можно представить в виде двух раздельных блоков или страт функциональных возможностей. Функции транспортирования располагаются в страте транспортирования, а функции управления обслуживанием, относящиеся к приложениям, например телефонии, располагаются в страте обслуживания. Каждая страта обычно имеет собственный набор ролей, участников и административных доменов (см. [ITU-T Y.110]). Роли, связанные с предоставлением услуги (услуг), не зависят от ролей, связанных с обеспечением возможности соединения для целей транспортирования. Каждая страта может рассматриваться отдельно с технической точки зрения. Функции управления ресурсами и допуском (RACF) исполняют роль арбитра для этих страт при выполнении резервирования (и проведении переговоров), связанных с QoS. В [ITU-T Y.2111] определяется функциональная архитектура и требования функциям управления ресурсами и допуском в сетях последующих поколений, в которых могут встречаться разнообразные технологии доступа и базовой транспортирования, а также может иметься множество доменов. Принимаемые RACF решения, связанные с QoS, опираются на SLA, приоритет обслуживания, профили пользователя, правила работы оператора сети, а также наличие ресурсов, как для сетей доступа, так и для базовых сетей. Требуется, чтобы пользователи электросвязи

[1] Политика в данном контексте включает все применимые стратегии, такие как формируемые на основании решений поставщиков СПП, регуляторных требований и других введенных государственными органами правил.

в чрезвычайных ситуациях были идентифицированы и чтобы, после того как они прошли аутентификацию и авторизацию, RAFC предоставила им приоритет в управлении допуском.

Если в СПП необходимо отличать трафик электросвязи в чрезвычайных ситуациях от обычного трафика, то требуется, чтобы были доступны соответствующие отличительные метки, также называемые маркерами. В данном контексте используется термин маркировка (трафика).

В сквозной (т. е. сегменты сети доступа и базовой сети) многоуровневой (т. е. страты транспортирования и обслуживания) архитектуре протоколов СПП возможно существование различных видов меток на разных уровнях протоколов, как вертикальных (т. е. взаимодействие между различными уровнями протоколов), так и горизонтальных (т. е. взаимодействие между устанавливающими связь сетевыми элементами). Метки могут передаваться в пакетах сигнализации и/или вставляться в заголовок пакетов данных для идентификации и маркировки вызовов или сеансов электросвязи в чрезвычайных ситуациях. Метки, используемые для идентификации и маркировки вызовов или сеансов и/или трафика электросвязи в чрезвычайных ситуациях, зависят от протокола. Для получения специализированного (например, предпочтительного или приоритетного) режима, являющегося сквозным для всех аспектов вызова или сеанса электросвязи в чрезвычайных ситуациях (например, управление вызовом/сеансом, трафик и управление носителем), требуется обеспечить соответствующее преобразование меток, используемых в различных протоколах, и взаимодействие между этими метками. Например, содержащаяся в заголовке протокола SIP информация о приоритете ресурса, используемая на уровне управления для идентификации приоритетного вызова или сеанса, могла бы преобразовываться в соответствующие указатели кода дифференцированного обслуживания (DSPC) для маркировки трафика электросвязи в чрезвычайных ситуациях на уровне IP-сети. Аналогично указатели кода дифференцированного обслуживания (DSPC) на третьем уровне могли бы преобразовываться в конкретные параметры приоритета в сетях VLAN и Ethernet на втором уровне в транспортном протоколе. Протокол SIP описывается в [IETF RFC 3261], а его обновления – в [b-IETF RFC 3265], [b-IETF RFC 3853], [b-IETF RFC 4320], [b-IETF RFC 4916], [b-IETF RFC 4032] и [b-IETF RFC 5027].

В страте обслуживания услуги обычно используют конкретные заданные наборы протоколов. Следовательно, методы, которые могут эффективно использоваться для конкретных услуг электросвязи в чрезвычайных ситуациях, будут меняться в зависимости от рассматриваемых услуг и возможностей конкретных протоколов, о которых идет речь, связанных с услугой.

В страте транспортирования может использоваться протокол Интернет (IP). Версия IP может изменяться от поставщика к поставщику, а возможность установления сквозного соединения может требовать адаптации разных версий путем применения, например, туннелирования одной версии в пределах другой. Однако это не должно влиять на транспортирование информации, относящейся к обслуживанию электросвязи в чрезвычайных ситуациях.

Кроме того, протоколы, используемые в инфраструктурах локального (последняя миля) доступа, могут отличаться от протоколов, используемых в базовых инфраструктурах. Инфраструктуры локального доступа могут строиться с использованием проводных (т. е. фиксированный доступ) технологий, беспроводных технологий, или на основе их сочетания.

Таким образом, для организации заданного сквозного маршрута данных вызова или сеанса электросвязи в чрезвычайных ситуациях может использоваться широкий диапазон технологий транспортирования.

В следующих ниже пунктах описываются различные характеристики и возможности конкретных технологий, которые могут эффективно использоваться для удовлетворения требований электросвязи в чрезвычайных ситуациях.

В связи с тем, что в страте транспортирования возможно применение протокола IP (и ряда связанных с ним протоколов), которые определены IETF, например TCP или UDP, целесообразно использовать для обеспечения электросвязи в чрезвычайных ситуациях, где это применимо, определенные IETF соответствующие возможности. Эти вопросы будут обсуждаться в дальнейших пунктах.

Важно проводить различие между разработкой IETF спецификаций (RFC) и их применением в среде интернет и СПП. В обоих случаях, фактически используемые спецификации будут зависеть от того, какая сеть развернута конкретным заинтересованным поставщиком. Однако поскольку среда интернет выходит за пределы сферы действия МСЭ-Т, не могут быть сделаны никакие предположения относительно качества обслуживания или возможностей маршрутов на основе протокола Интернет, описанных в [b-IETF RFC 4190][2]. С другой стороны, более жесткие требования к международной электросвязи в чрезвычайных ситуациях в сетях СПП на основе протокола IP находятся в пределах сферы действия МСЭ-Т и могут быть предложены поставщикам услуг СПП в виде Рекомендаций МСЭ-Т.

В [IETF RFC 4542] описываются возможные решения в отношении "предпочтительного обслуживания в чрезвычайных ситуациях в интернете". Многие методы, изложенные в этом документе, применяются к ETS в среде СПП.

Из этого следует, что в СПП, где страты обслуживания и транспортирования независимы, на успешное обеспечение электросвязи в чрезвычайных ситуациях влияют следующие факторы:

i) идентификация и маркировка трафика электросвязи в чрезвычайных ситуациях;

ii) политика управления допуском;

iii) политика распределения полосы пропускания;

iv) аутентификация и авторизация настоящих пользователей электросвязи в чрезвычайных ситуациях.

9.1.1 Приоритетный режим

В целом приоритетный режим является основным элементом обеспечения электросвязи в чрезвычайных ситуациях, которая по определению должна считаться более важной, чем обычные услуги электросвязи. Если на предоставление обычных услуг уходит подавляющая часть ограниченных ресурсов сети, то электросвязь в чрезвычайных ситуациях вынуждена конкурировать за те же самые ограниченные ресурсы, что может негативно сказаться на ней. Значит, следует разработать какие-то средства предоставления экстренным службам приоритетного режима по сравнению с обычными услугами электросвязи.

В первую очередь, к таким средствам относятся:

a) распознавание и авторизация пользователей электросвязи в чрезвычайных ситуациях;

b) предоставление авторизованным пользователям электросвязи в чрезвычайных ситуациях приоритета в обслуживании.

В уровневой архитектуре СПП, определенной в [ITU-T Y.2012], индикатор приоритета, передаваемый функцией управления обслуживанием (SCF) функции управления ресурсами и допуском (RACF), должен быть способен указывать категории приоритетов, предоставляемых пользователям, с тем чтобы позволить применение различных правил и установление различий между многими видами приоритетных приложений. Например, персоналу больницы может быть предоставлена более низкая категория приоритета пользователя, чем координаторам службы скорой помощи.

9.1.2 Идентификация, аутентификация и авторизация, а также управление доступом

Необходимо предотвращать неавторизованный доступ к услугам и ресурсам электросвязи в чрезвычайных ситуациях, например, со стороны злоумышленников, маскирующихся под авторизованных пользователей. Следовательно, должны обеспечиваться механизмы и возможности аутентификации пользователей или устройств электросвязи в чрезвычайных ситуациях, либо и тех, и других, в зависимости от случая, а также авторизации доступа, на основе политики, применимой к конкретной службе (например, ETS или TDR).

Необходимо идентифицировать вызов или сеанс электросвязи в чрезвычайных ситуациях (например, с помощью специального набора номера, входных данных, профилей пользователя или подписки). Поставщики услуг СПП должны ускорять аутентификацию авторизованных пользователей электросвязи в чрезвычайных ситуациях. Требуется использовать конкретные механизмы и методы для аутентификации и авторизации, основанные на политике, применимой к конкретным видам

---

[2] В [b-IETF RFC 4190] указано, что:

"Постоянной неотъемлемой чертой развития интернета является предоставление наилучшего уровня обслуживания из возможных в качестве модели обслуживания по умолчанию"; и

"взаимодействие между доменами при ETS не должно основываться на повсеместной или даже широко распространенной поддержке по всему маршруту между оконечными точками".

электросвязи в чрезвычайных ситуациях (например, использовать персональный идентификационный номер (PIN), а также профили пользователя и контракты).

Примеры подходов к аутентификации и авторизации ETS описаны в Дополнении II [ITU-T Y.2702] и включают:

a) Использование персонального идентификационного номера (PIN): при таком подходе используется аутентификация и авторизация пользователя по номеру PIN. При этом мы идентифицируем пользователя, а не устройство пользователя. Следовательно, этот метод обычно применяется в тех случаях, когда пользователю разрешено вызывать услугу ETS с любого устройства.

b) Использование профиля подписки/обслуживания: при этом подходе для обозначения подписки ETS подготавливается профиль оконечного устройства пользователя. Пользовательский терминал аутентифицируется, и профиль обслуживания пользователя определяется как часть обычной процедуры регистрации поставщика СПП (то есть поставщика ETS). Если пользователь инициирует запрос, на основании проверки профиля обслуживания пользователя определяется, имеет ли пользователь авторизацию для ETS. Запрос ETS удовлетворяется, если подписка ETS является действительной для пользовательского терминала.

c) Использование сочетания PIN и профиля обслуживания: возможно также сочетание методов с использованием PIN и профиля обслуживания для аутентификации как пользователя, так и устройства пользователя в целях обеспечения более высоких уровней гарантированности.

d) Использование специальных жетонов безопасности и биометрических данных. Кроме описанных выше подходов в целях обеспечения более высоких уровней гарантированности подлинности при выполнении аутентификации и авторизации пользователей ETS могут применяться более сложные подходы на основе использования специальных жетонов безопасности и биометрических данных.

После того как пользователь или устройство, либо они оба, аутентифицированы и авторизованы на основе применяемой политики, трафик вызова или сеансов электросвязи в чрезвычайных ситуациях должен быть маркирован и указан в прямом направлении к последующим сетям. Также после прохождения аутентификации и авторизации требуется, чтобы приоритет предоставлялся по всем аспектам вызова/сессии электросвязи в чрезвычайных ситуациях, сигнализации/управлению, трафику носителя и любому применимому управлению.

Необходимо учитывать аутентификацию и авторизацию при эстафетной передаче и при приеме вызовов или сеансов электросвязи в чрезвычайных ситуациях между поставщиками услуг СПП, с учетом наличия многих поставщиков услуг и разделения управления обслуживанием и транспортирования. Аутентификация и авторизация поставщиков услуг СПП для эстафетной передачи и приема вызовов или сеансов и трафика электросвязи в чрезвычайных ситуациях должна основываться на SLA и применимой политике.

Учитывать аутентификацию и авторизацию необходимо также и для передачи и приема вызовов или сеансов электросвязи в чрезвычайных ситуациях между поставщиками СПП, принимая во внимание среду с несколькими поставщиками и разделение функций управления обслуживанием и транспортирования при обслуживании. Аутентификация и авторизации поставщиков СПП для передачи и приема вызовов/сеансов и трафика электросвязи в чрезвычайных ситуациях должны базироваться на SLA и применяемой политике.

Возможности IdM ([ITU-T Y.2720], [ITU-T Y.2721] и [ITU-T Y.2722]) могут использоваться для обеспечения более высокого уровня конфиденциальности информации идентичности для приложений электросвязи в чрезвычайных ситуациях. В Дополнении III [ITU-T Y.2721] приведены примеры использования IdM в связи с ETS. В этих примерах описываются способы использования возможностей IdM для обеспечения приложений ETS и охватываются следующие темы:

- гарантия обеспечения аутентификации с использованием сочетания устройства и пользователя (например, корреляция аутентификации пользователя и устройства);
- более высокий уровень аутентификации пользователей ETS для приоритетных услуг последующих поколений (например, использование жетонов, цифровых сертификатов, распознавание голоса и биометрические данные);
- аутентификация вызывающей стороны и источников передачи данных (например, гарантирование источников сообщений и данных);
- идентификация и аутентификация поставщиков услуг в среде с несколькими поставщиками (например, идентификация поставщиков доступа, контента и сетевых услуг);
- однократная регистрация в системе и однократный выход из системы (например, доступ к нескольким приложениям без необходимости представления своих полномочий для каждого приложения).

9.1.3 Соображения относительно управления допуском для обеспечения более высокой вероятности допуска

Одной из задач функции управления ресурсами и допуском (RACF) является обеспечение управления QoS, включая допуск к ресурсам и резервирование ресурсов, если пожелает поставщик услуги. В связи с этим в периоды высокой потребности в обслуживании со стороны пользователей в некоторых запросах на обслуживание, возможно, придется отказать. Если такие отказы не происходят, то СПП не может полностью гарантировать качество обслуживания в чрезвычайных ситуациях. Процессы RACF, связанные с QoS, включают авторизацию на основе профилей пользователя, SLA, правил работы оператора сети, приоритета обслуживания и наличия ресурсов для доступа и базового транспортирования. В настоящей Рекомендации предполагается, что RACF должна иметь возможность установления приоритетов запросов на обслуживание путем использования приоритета обслуживания. (Сеть, которая просто выдает отказ авторизованным запросам вследствие мгновенной перегрузки, обеспечивала бы плохое обслуживание клиентов, неоднократно заставляя их повторно направлять запросы). Таким образом, в настоящей Рекомендации утверждается, что приоритет обслуживания является фактором первостепенной важности, который должен учитываться в методах планирования для принятия решения о распределении ресурсов применительно к допуску с ожиданием/общему допуску. Механизмы, позволяющие реализовать данную функциональную возможность, обсуждаются ниже.

Высокоуровневые требования RACF состоят в работе над авторизованными запросами в отношении QoS с использованием профилей и приоритета пользователя. Одно конкретное требование заключается в том, чтобы при управлении допуском для приоритетной обработки использовалась информация о приоритете обслуживания. Существуют различные методы, которые могут использоваться для приоритета обслуживания при управлении допуском на основе ресурсов.

Один из возможных методов состоит в том, чтобы для трафика электросвязи в чрезвычайных ситуациях использовались более высокие пороги допуска и, таким образом, обеспечивалась возможность некоторого дополнительного допуска для приоритетных запросов, когда обычным запросам выдается отказ. При применении данного метода временно повышается использование ресурсов сети. Однако вследствие большого объема ресурсов СПП и того обстоятельства, что на любом заметном временном интервале некоторые ресурсы, естественно, станут доступными (например, при завершении других сеансов), пропускная способность системы восстановится до своего установленного рабочего текущего уровня. Более того, если предположить, что объем приоритетного трафика относительно невелик и что сеть редко или почти никогда не работает с полной 100-процентной пропускной способностью, становится очевидно, что более высокий порог решения о допуске для приоритетного трафика не должен создавать никакой угрозы общей работоспособности сети или QoS другого трафика.

Существуют системы управления допуском на основе резервирования, которые разрешают запросы на обслуживание только в том случае, если запрос в отношении требуемой полосы пропускания является успешным. В этом случае в методе обслуживания механизма планирования, в качестве первоочередной задачи, должен учитываться приоритет обслуживания.

В заключение отметим, что возможны также другие способы, позволяющие обойти механизм управления допуском (например, RACF для обхода приоритетным трафиком). Пример такого способа в настоящее время описывается в IETF.

9.1.3.1 Управление допуском вызова (CAC)

CAC представляет собой набор действий и правил, применяемых сетью на этапе установления вызова или сеанса, для того чтобы принять или отклонить обслуживание на основе запрашиваемой информации и критериев приоритета, а также наличия необходимых ресурсов.

В традиционной сети КТСОП/ЦСИС управление допуском вызова означает буквально то, что канал либо предоставляется, либо не предоставляется, на основе авторизации. Более того, предоставление канала по определению подразумевает наличие маршрута с требуемой полосой пропускания. В связи с тем, что имеется информация о состоянии сети, касающаяся статуса отдельных каналов (речевых каналов), сеть КТСОП/ЦСИС может:

a) направлять экстренные вызовы по специально зарезервированным для экстренного трафика маршрутам (если имеются);

b) дожидаться, пока освободится канал (постановка в очередь).

Поскольку в сетях на основе протокола IP отсутствует информация о состоянии отдельных маршрутов или канала, с помощью лишь аутентификации и авторизации при входе в сеть нельзя гарантировать наличие сквозного маршрута или достаточной сквозной полосы пропускания для данного вызова или сеанса. В сети на основе протокола IP входной сетевой элемент не имеет или почти не имеет сведений о преобладающих состояниях сети за пределами своего домена. Следовательно, CAC во входном сетевом элементе является недостаточным для того, чтобы

гарантировать наличие сквозного маршрута, если оно не было расширено с помощью дополнительных средств.

Из этого далее следует, что выходной сетевой элемент никаким образом не управляет удаленным входным сетевым элементом, который может пытаться установить с ним вызов или сеанс, или не имеет об этом элементе никаких сведений. Однако в сетях КТСОП/ЦСИС выходной сетевой элемент способен управлять возможным входным сетевым элементом, который пытается установить вызов/сеанс, с помощью механизмов связанной сигнализации.

В [ITU-T Y.2171] определяется приоритет управления допуском для сигналов услуг электросвязи, добивающихся вхождения в сеть, в частности, в период чрезвычайных ситуаций, когда ресурсы сети могут быть сокращены. В частности, рекомендованы три уровня приоритета управления допуском для сигналов служб, добивающихся вхождения в СПП. Уровень приоритета 1 (наибольший) рекомендован для электросвязи в чрезвычайных ситуациях (включая ETS) по СПП. Трафик с этим уровнем приоритета получает наибольшую гарантию допуска в СПП.

9.2 Страта обслуживания

9.2.1 Общие положения

У стран имеется или они создают ETS для того, чтобы позволять приоритетный режим в отношении авторизованного трафика с целью обеспечения операций по оказанию помощи в чрезвычайных ситуациях и при бедствиях в пределах своих национальных границ. Однако могут возникать кризисные ситуации, при которых важно, чтобы пользователь ETS в одной стране мог установить связь с пользователями в другой стране. В этом случае важно, чтобы исходящий из какой-либо страны вызов или сеанс ETS получил сквозной приоритетный режим, т. е. приоритетный режим в стране-отправителе и в стране-получателе. Для этого может потребоваться взаимодействие двух реализованных на национальных уровнях ETS по международной сети, в которой либо предоставляется возможность приоритетного режима, либо обеспечивается прозрачная передача приоритета между обеими странами.

В нижеследующих пунктах описывается ряд механизмов протоколов, используемых для подачи сигнала и получения приоритетного режима на уровне управления обслуживанием в контексте СПП с пакетной коммутацией. Также освещаются конкретные возможности применения этих механизмов протоколов к ETS. Эти возможности, обеспечиваемые протоколами, необходимы для международного применения, в случае осуществления связи между реализованными на национальных уровнях ETS по международной сети (например, взаимодействие двух реализованных на национальных уровнях ETS).

9.2.2 Приоритет ресурсов для SIP

В [IETF RFC 4412] к SIP добавлены два поля заголовков, а именно поле "приоритет ресурса" и поле "принять приоритет ресурса", а также определяются процедуры их использования. Поле заголовка "приоритет ресурса" может использоваться агентами пользователя SIP, шлюзовыми станциями и оконечным оборудованием коммутируемой телефонной сети общего пользования (КТСОП), а также серверами-посредниками SIP с целью воздействия на обработку ими запросов SIP.

Для того чтобы обеспечить эквивалентность некоторых существующих систем, приоритет, соответствующий нескольким различным "стандартизованным" системам, может быть обозначен путем определения "пространства имен", соответствующего конкретной системе, и количества уровней приоритета в этой системе. Приведенные ниже пространства имен и связанное с ними количество уровней приоритета, предназначенные для использования в ETS, определены в [IETF RFC 4412].

Пространства имен	Уровни
ets	5
wps	5

Все вызовы/сеансы ETS в среде с использованием протокола IP обозначаются с помощью пространства имен "ets", имеющего пять уровней приоритета, с помощью которых на прикладном уровне (в элементах SIP) передается информация о важности. Входящим вызовам или сеансам ETS присваивается обозначение "ets" в заголовке "приоритет ресурса". Вызовы/сеансы ETS распознаются по наличию значения заголовка "приоритет ресурса" в пространстве имен "ets" в сообщении SIP, и им предоставляется "высокий" приоритет для резервирования/присвоения ресурсов, при котором на транспортном уровне может быть установлен предпочтительный режим. Точно так же для выделения вызовов или сеансов может назначаться пространство имен "wps", которому соответствует пять уровней приоритета, в случае если ресурсы ограничены или перегружены, как, например, при радиодоступе в сетях беспроводной связи.

9.2.3 IEPS

В [ITU-T E.106] описываются функциональные требования к международной системе предпочтений при чрезвычайных ситуациях (IEPS), ее свойства, доступ к IEPS и оперативное управление системой. IEPS дает возможность взаимодействия различных систем приоритетов/предпочтений, реализованных на национальном уровне. Тем самым обеспечивается сквозной предпочтительный режим для авторизованных узкополосных голосовых вызов и вызовов для передачи данных.

Сфера применения [ITU-T E.106] сформулирована для случаев КТСОП, ЦСИС или сети сухопутной подвижной связи общего пользования (PLMN). IEPS предоставляет авторизованным пользователям приоритетный режим для службы международной телефонной связи на сетях электросвязи с установлением соединения. Следовательно, на основе двусторонних/многосторонних соглашений между странами/администрациям можно было бы использовать IEPS при таком сценарии для обеспечения взаимодействия реализованных на национальном уровне ETS.

9.2.4 Протоколы управления в системе Рекомендации МСЭ-Т H.323

В настоящем пункте описываются протоколы, используемые в системе Рекомендации МСЭ-Т H.323 для обеспечения приоритетной электросвязи.

В [ITU-T H.460.4] определяется обозначение приоритета вызова и идентификация сети страны/международной сети происхождения вызова для приоритетных вызовов в системе Рекомендации МСЭ-Т H.323. Параметр для обозначения приоритета вызова в системе Рекомендации МСЭ-Т H.460.4 поддерживает индикатор приоритетного вызова и пять уровней приоритета.

В [ITU-T H.248.1] определяются протоколы, используемые между элементами физически распределенного мультимедийного шлюза, который применяется в соответствии с архитектурой, указанной в [ITU-T H.323]. Для санкционированных правительством экстренных служб (например, ETS), в [ITU-T H.248.1] определяются индикатор вызова и индикатор приоритета IEPS. В индикаторе вызова IEPS передается указание на приоритет между функциями контроллера и шлюза. В индикаторе приоритета передаются уровни приоритета между функциями контроллера и шлюза. Индикатор приоритета в системе H.248 поддерживает 16 уровней приоритета. Индикаторы вызова и индикатор приоритета IEPS удовлетворяют требованиям ETS в отношении указания контекста ETS и переносы уровня приоритета, соответственно. Для служб общественной безопасности в [ITU-T H.248.1] определяются индикаторы экстренного вызова для передачи указания на приоритет между функциями контроллера и шлюза.

[ITU-T H.248.81] обеспечивает руководящие указания по использованию индикатора вызова и индикатора приоритета IEPS в профилях Рекомендации МСЭ-Т H.248 для систем Рекомендации МСЭ-Т H.323 и систем СПП в целях обеспечения приоритетных служб (например, ETS).

9.2.5 Diameter

Протокол Diameter [IETF RFC 3588] поддерживает аутентификацию, авторизацию и учет (AAA) для сетевых функций и приложений, таких как доступ в сеть и мобильность на основе IP.

Для использования в протоколе Diameter с целью обеспечения приоритетных служб (например, ETS) предназначены следующие пары значений атрибутов (AVP):

- MPS-Идентификатор;
- Резервирование-Приоритет;
- Приоритет-Уровень (как часть AVP Сохранение распределения-Приоритет (ARP));
- Сеанс-Приоритет.

AVP AF-Идентификатор определена в рамках 3GPP в [b-3GPP TS 29.214]. AVP MPS-Идентификатор используется для обозначения приоритетной службы (например, запрос на ETS/MPS) по интерфейсу Rx. AVP MPS-Идентификатор содержит национальный вариант наименования приоритетной службы.

AVP Резервирование-Приоритет определена Европейским институтом стандартизации электросвязи (ЕТСИ) в [ETSI TS 183 017]. В [ITU-T Q.3321.1] и [ITU-T Q.3303.3] определено использование AVP Резервирование-Приоритет в интерфейсах Rs и Rw функции управления ресурсами и допуском (RACF) [ITU-T Y.2111], соответственно, для обеспечения приоритетных служб. Аналогично в [b-3GPP TS 29.214] (Policy and charging control over Rx reference point) и [ITU-T Q.1741.6] определено использование AVP Резервирование-Приоритет в интерфейсе Rx управления политикой и начислением платы (PCC) для обеспечения приоритетных служб (например, ETS). AVP Резервирование-Приоритет поддерживает 16 уровней приоритета, которые могут использоваться для

запроса приоритетного режима. Значения от 0 до 15 используются в порядке возрастания, при этом "15" означает наивысший приоритет, "0" – низший. AVP "Резервирование-Приоритет" обозначает значение приоритета пользователя.

AVP Приоритет-Уровень (как часть AVP Сохранение распределения-Приоритет (ARP)) определена в рамках 3GPP в [b-3GPP TS 29.212] (Policy and charging control over Gx reference point) и [ITU-T Q.1741.6]. В [ITU-T Q.1741.6] описано применение AVP Приоритет-Уровень в интерфейсе Gx управления политикой и начислением платы (PCC) для обеспечения приоритетных служб (например, ETS). AVP Приоритет-Уровень поддерживает 15 уровней приоритета, которые могут использоваться для запроса приоритетного режима. Значения от 1 до 15 используются в порядке убывания, при этом "1" означает наивысший приоритет, "15" – низший. Значения приоритета от 1 до 8 присваиваются службам, которые авторизованы для получения приоритетного режима (например, ETS, MPS) Значение приоритета "0" зарезервировано и при получении трактуется как логическая ошибка. AVP приоритет-Уровень отражает значение приоритета пользователя.

AVP Сеанс-Приоритет определяется в [b-3GPP TS 29.229] (Cx and Dx interfaces based on the Diameter protocol; Protocol details) и [ITU-T Q.1741.6]. В [b-3GPP TS 29.229] определяется использование AVP Сеанс-Приоритет в интерфейсах Cx и Dx для обеспечения приоритетных служб (например, ETS). Аналогично в [b-3GPP TS 29.329] (Sh interface based on the Diameter protocol; Protocol details) и [ITU-T Q.1741.6] определяется использование AVP Сеанс-Приоритет в интерфейсе Sh для обеспечения приоритетных служб. AVP Сеанс-Приоритет поддерживает 5 уровней приоритета, которые могут использоваться для запроса приоритетного режима по интерфейсам Cx, Dx и Sh. Значения от 0 до 4 определены для использования в порядке убывания, при этом "0" означает наивысший приоритет, "4" – низший.

9.3 Страта транспортирования

9.3.1 Общие положения

В основе необходимости в специальных соглашениях (например, SLA) для обработки сигналов ЕТ в СПП, которая надлежащим образом спроектирована и имеет подходящие размеры, лежит предположение о том, что сетевых ресурсов недостаточно для того объема трафика, который поступает в сеть и что при таких условиях трафик электросвязи в чрезвычайных ситуациях мог бы оказаться отклоненным либо существенно задержанным и/или прерванным, ниже того уровня, при котором он может использоваться, либо даже его передача могла бы отмениться. В случае если объем принимаемого трафика, предусмотренный в статистической модели или в модели с максимально возможным уровнем обслуживания, превышает пропускную способность данного приемного сетевого элемента (например, IP-маршрутизатора) и выходную пропускную способность, которой обладает данный элемент, единственной возможностью, доступной для данного сетевого элемента, является прекращение передачи избыточного трафика. Это означает, что если не разрешены специальные меры предпочтительной обработки (например, определенные в SLA), передача трафика электросвязи в чрезвычайных ситуациях была бы прекращена наряду с трафиком, не являющимся трафиком электросвязи в чрезвычайных ситуациях. Форум ТМ подготовил руководящие принципы спецификации и управления соглашениями SLA [b-TM Forum GB917] и, в частности, рассмотрел вопрос о возможном применении этих принципов к ETS.

В качестве решения иногда предлагаются методы избыточного обеспечения ресурсами. Однако во многих случаях избыточное обеспечение может оказаться невозможным или нецелесообразным. Что еще более важно, некоторые виды чрезвычайных ситуаций могут возникать в результате преднамеренного или случайного разрушения или повреждения участков сети, и, таким образом, исключаются любые пути или элементы с избыточным обеспечением, которые обычно могут быть доступными. Если СПП должна быть в состоянии справиться со всеми видами чрезвычайных ситуаций при неблагоприятных обстоятельствах, то будет необходимо обеспечить наличие конкретных средств для предоставления трафику электросвязи в чрезвычайных ситуациях предпочтительного режима.

В нижеследующих пунктах описывается ряд механизмов, используемых для получения приоритетного режима на транспортном уровне в условиях СПП с пакетной коммутацией.

9.3.2 Управление полосой пропускания с использованием RSVP

Одной из возможных характеристик сети на основе протокола IP, за счет которой обеспечивается определенное (грубое) соответствие распределенной полосе пропускания в сетях с коммутацией каналов, является применение механизма распределения и резервирования полосы пропускания

на основе протокола IP. Данный механизм представляет собой процедуру, определенную IETF в своем протоколе резервирования ресурсов (RSVP), который указан в [IETF RFC 2205] и в его обновлениях: [b-IETF RFC 2750], [b-IETF RFC 3936] и [b-IETF RFC 4495].

Определение параметров управления ресурсами, которое необходимо для протокола инициации сеанса (SIP) в страте обслуживания и которое должно использоваться совместно с протоколом RSVP (в страте транспортирования), указано в [IETF RFC 3312]. Данное определение параметров позволяет использовать процедуры сигнализации RSVP до процедуры сигнализации SIP, во время них и/или вместе с ними. Ряд таких примеров приведен в Дополнении A к [IETF RFC 4542]. Однако в [IETF RFC 4542] используется метод преимущественного права.

IETF в настоящее время разрабатывает расширения протокола RSVP, которые могут использоваться, чтобы обеспечивать возможность установления приоритета допуска на сетевом уровне. В этом документе указываются новые расширения протокола RSVP для повышения вероятности завершения вызова без применения преимущественного права. Для выполнения условий "приоритета допуска", который требуется на сети электросвязи в чрезвычайных ситуациях, поддерживающей протокол RSVP, используются методы проектирования пропускной способности с использованием моделей распределения полосы пропускания. В частности, эти расширения определяют два новых элемента политики протокола RSVP, позволяющие передавать информацию о приоритете допуска в сообщениях сигнализации RSVP, с тем чтобы узлы RSVP могли исполнять решения, касающиеся управления выборочным допуском к полосе пропускания, на основе приоритета допуска вызова.

9.3.3 Управление очередностью с использованием дифференцированного обслуживания

В [IETF RFC 4594] излагается рекомендуемое преобразование классов обслуживания в указатели кода дифференцированного обслуживания (DSCP). На рисунке 3 в [IETF RFC 4594] приводится таблица преобразования, в которой для приложений телефонной связи выделяется класс срочной пересылки данных (EF). Это позволяет включать в пакеты протокола IP значения DSCP, выделенные для класса срочной пересылки данных.

Более того, в [ITU-T Y.1541] рекомендуется также, чтобы голосовой трафик в пакетах протокола IP маркировался (помечался) с использованием DSCP, соответствующего срочной пересылке данных. При получении пакетов, маркированных как EF, сетевые элементы (маршрутизаторы) в страте транспортирования обеспечат своевременную доставку трафика, требующего немедленной обработки, по сравнению с трафиком, не требующим немедленной обработки, с использованием правил срочной пересылки данных, которые определены для указателя кода EF и описаны в [IETF RFC 3246].

Однако код EF используется для обычного телефонного трафика. Следовательно, по-прежнему может существовать необходимость в том, чтобы каким-то образом различать трафик телефонной связи в чрезвычайных ситуациях от трафика, не являющегося трафиком телефонной связи в чрезвычайных ситуациях (см. следующий пункт).

9.3.4 EF DSCP для трафика, имеющего допуск к пропускной способности

В стандарте [IETF RFC 5865] VOICE-ADMIT DSCP определяется для класса трафика, к которому применяется строгая процедура CAC и который включает трафик ETC. Это дает возможность передавать трафик в реальном времени, соответствующий правилам поведения на каждом шаге при срочной пересылке данных (EF), с использованием процедуры CAC, которая предусматривает аутентификацию, авторизацию и допуск к пропускной способности (см. пп. 9.3.1 и 9.3.2, выше), в отличие от класса трафика в реальном времени, соответствующего поведению на каждом шаге при срочной пересылке данных, к которому не применяется допуск к пропускной способности.

9.3.5 Явное уведомление о перегрузке (ECN)

В [IETF RFC 3168] определяется двухуровневая архитектура ECN, как работающая на сетевом уровне (т. е. IP) и на транспортном уровне (например, TCP). Задачей ECN является обеспечение своевременной явной обратной связи с источником перегрузки в нисходящем направлении, но при минимальном уровне потери пакетов и, следовательно, при минимальном нарушении потоков. Передача этой информации выполняется с использованием промежуточных узлов, поддерживающих активное управление очередью (AQM), которое помечает пакеты с уведомлением о перегрузке и не отбрасывает, а направляет их в нисходящем направлении. Конечная точка потока отправляет затем индикацию обратной связи (то есть, ECN) обратно к источнику через транспортный протокол верхнего уровня. В [IETF RFC 4340] была расширена поддержка ECN и включен протокол управления перегрузкой (DCCP).

Как в случае TCP, так и DCCP ECN запускает внутренние алгоритмы снижения потерь, которые для приложений являются прозрачными. Основным преимуществом, обеспечиваемым этой функцией, является то, что приложения становятся более ориентированным на сеть и снижают входную нагрузку, позволяя таким образом использовать сеть большему числу пользователей/приложений. В этом прозрачном для приложения сценарии ECN не обеспечивает предпочтения пользователям ETS перед всеми пользователями. Напротив, ECN содействует непрерывному использованию ресурсов сети как пользователями ETS, так и пользователями из числа широкой общественности.

В рабочей группе по сетям IETF в настоящее время изучается, как ECN может использоваться для потоков RTP, проходящих по UDP/IP, использующих RTCP в качестве механизма обратной связи. Решение заключается в передаче отправителю по обратной связи отметок перегрузки ECN, используя RTCP, сквозной верификации функциональных возможностей ECN и того, как инициировать ECN. Текущие исследования IETF направлены на добавление обеспечения ECN приложениям реального времени (например, передача голоса и видео) с использованием RTP/RTCP. В этом случае уведомление о перегрузке становится доступным приложениям, которые могут совершенно по-разному реагировать на это уведомление. Можно ожидать, что реакция по умолчанию будет соответствовать TCP и DCCP, когда приложения снижают входную нагрузку на сеть.

9.4 Технологическое обеспечение доступа по СПП

9.4.1 Общие положения

Существует много методов доступа по СПП, зависящих от технологии. В соответствии с [ITU-T Y.2012] сеть доступа включает функции, зависящие от сочетания метода доступа и технологии. Например, для технологии W-CDMA и доступа по xDSL. В зависимости от технологии, используемой для доступа к услугам СПП, сеть доступа включает функции, относящиеся к:

1) кабельному доступу;
2) доступу по xDSL;
3) беспроводному доступу (например, с использованием технологий [b-IEEE 802.11] и [b-IEEE 802.16], а также доступа по 3G RAN);
4) оптическому доступу.

Для обеспечения электросвязи в чрезвычайных ситуациях в сегменте доступа по СПП также необходимы специальные соглашения. В основе необходимости в специальных соглашениях лежит допущение о том, что ресурсы доступа ограничены точно так же, как и ресурсы базовой сети. Следовательно, в зависимости от объема трафика, который поступает в сегмент сети доступа, на трафик электросвязи в чрезвычайных ситуациях могло бы быть оказано воздействие (например, он мог бы оказаться отклоненным либо существенно задержанным и/или прерванным, ниже того уровня, при котором он может использоваться, либо даже его передача могла бы отмениться).

Следовательно, если СПП должна быть в состоянии справиться со всеми видами чрезвычайных ситуаций при неблагоприятных обстоятельствах, в сегменте доступа по СПП должно быть обеспечено наличие конкретных средств для предоставления трафику электросвязи в чрезвычайных ситуациях предпочтительного режима. Это включает в себя, помимо прочего, механизмы и возможности для:

- распознавания трафика электросвязи в чрезвычайных ситуациях;
- предпочтительного/приоритетного доступа к ресурсам/средствам;
- предпочтительной/приоритетной маршрутизации трафика электросвязи в чрезвычайных ситуациях;
- предпочтительного/приоритетного установления сеансов/вызовов электросвязи в чрезвычайных ситуациях.

При установлении приоритетного режима для электросвязи в чрезвычайных ситуациях рассматриваются следующие аспекты: классификация или присвоение меток трафику для приоритетного обслуживания, сигнализация для установления маршрута транспортирования этого трафика и механизмы, включая политику обеспечения запрошенного приоритета. Некоторые аспекты, такие как выбор механизмов, политика и соответствующие реализации не стандартизируются и могут различаться в зависимости от региона.

9.4.2 Беспроводной радиодоступ

Требуется, чтобы сети беспроводного радиодоступа обеспечивали конкретные механизмы и возможности предоставления авторизованным сеансам или вызовам электросвязи в чрезвычайных ситуациях предпочтительного/приоритетного режима. Для предоставления такого режима могут использоваться механизмы и возможности, зависящие от технологии. Это включает, помимо прочего, механизмы и возможности для:

- распознавания трафика электросвязи в чрезвычайных ситуациях: такое распознавание включает идентификацию и маркировку авторизованного трафика электросвязи в чрезвычайных ситуациях;
- предпочтительного/приоритетного доступа к ресурсам/средствам: это облегчает доставку в СПП запроса на электросвязь в чрезвычайных ситуациях, если имеющиеся ресурсы доступа ограничены;
- предпочтительной/приоритетной маршрутизации трафика электросвязи в чрезвычайных ситуациях: это может предполагать такие свойства, как постановку в очередь на имеющиеся ресурсы, исключение из определенных ограничительных функций управления сетью и резервирование некоторых маршрутов/путей для трафика электросвязи в чрезвычайных ситуациях;
- предпочтительного/приоритетного установления вызовов или сеансов электросвязи в чрезвычайных ситуациях.

9.4.2.1 Универсальная система подвижной электросвязи (UMTS) и долгосрочное развитие (LTE)

Приоритетное обслуживание и приоритетное обслуживание мультимедийного трафика для систем 3GPP определено в [b-3GPP TS 22.153]. В 3GPP приоритетное обслуживание и приоритетное обслуживание мультимедийного трафика было определено как позволяющее авторизованным пользователям получать приоритетный доступ к следующим имеющимся радиоканалам (трафик передачи голоса или данных) раньше других пользователей в ситуациях, когда в результате перегрузки блокируются попытки вызовов. Приоритетное обслуживание поддерживает приоритетное прохождение вызова и завершение вызова в целях обеспечения сквозного приоритетного вызова из подвижной в подвижную сеть, из подвижной в фиксированную сеть и из фиксированной в подвижную сеть. Приоритетное обслуживание мультимедийного трафика поддерживает приоритетное прохождение и завершение мультимедийных сеансов в целях обеспечения сквозных приоритетных мультимедийных сеансов из подвижной в подвижную сеть, из подвижной в фиксированную сеть и из фиксированной в подвижную сеть.

На основе [b-3GPP TS 22.153] в рамках 3GPP разрабатывается Технический отчет этапа 2 по усовершенствованию приоритетного обслуживания мультимедийного трафика [b-3GPP TR 23.854] в целях выявления того, какие изменения необходимы для существующих спецификаций 3GPP Этапа 2 (например, [b-3GPP TS 23.401], [b-3GPP TS 23.203], [b-3GPP TS 23.328] и [b-3GPP TS 23.272]), для обеспечения MPS, включая мультимедийную IP-подсистему (IMS) и аспекты управления политикой и начислением платы (PCC). Этот технический отчет предназначен для пояснения архитектурных требований и потоков вызовов или сеансов для MPS. На основании требований 3GPP Этапа 2 будут определены изменения к действующим спецификациям 3GPP Этапа 3 в целях обеспечения MPS для технологий доступа UMTS и LTE.

9.4.2.2 Усовершенствованный доступ с оптимизацией передачи данных (EV-DO)

Аналогично 3GPP, в 3GPP2 определено приоритетное обслуживание мультимедийного трафика (MMPS) для систем 3GPP2. Спецификацией 3GPP2 для MMPS является [b-3GPP2 S.R0117-0]. В стандарты сетевого интерфейса систем 3GPP2 включен ряд возможностей, таких как обновление приоритетных уровней несущей, и эти возможности могут использоваться для обеспечения MMPS. Аналогичным образом ряд возможностей, таких как организация очередей, включены в стандарты радиоинтерфейсов систем 3GPP2, и эти возможности могут использоваться для обеспечения MMPS.

9.4.2.3 Доступ по сетям WiMAX

В [b-WFM Stage1-r1] определены требования Этапа 1 для электросвязи в чрезвычайных ситуациях (ETS) по сетям WiMAX для варианта 1.6 на основе радиоинтерфейса [b-IEEE 802.16 2009]. В [b-WFM Stage1-r2] расширены требования Этапа 1 для ETS по WiMAX варианта 1.6 для варианта 2.0 в целях обеспечения радиоинтерфейса [b-IEEE 802.16m].

В [b-WFM Stage2-a1] для ETS определена концепция сетевого решения WiMAX этапа 2 для варианта 1.6 в целях обеспечения требований Этапа 1. В этой концепции определяется индикация приоритета по инициативе сети и приоритетный режим для архитектуры аутентификации, авторизации и учета (AAA). Концепция ETS, основанная на архитектуре контроля политики и начисления платы (PCC) и механизмах приоритетов, инициируемых UE, разрабатывается для варианта 2.0.

В [b-WFM Stage3-a1] определены сетевые процедуры и сообщения WiMAX этапа 3 для варианта 1.6, поддерживающие индикацию приоритетов и приоритетный режим на основе концепции решения Этапа 2. Поле индикации приоритета добавляется к параметру дескриптора QoS сообщений WiMAX RADIUS и Diameter. В этом документе также описаны процедуры индикации приоритета для архитектуры AAA по инициативе сети, а также механизмы приоритетного режима в BS, шлюзе ASN и функциональных объектах служебной сети, обеспечивающей возможность установления соединения (CSN). Ключевыми областями обеспечения ETS в сети WiMAX являются следующие:

1) При первом входе в сеть для UE, связанного с контрактом, включающим WiMAX, индикация приоритета, связанная с начальными потоками обслуживания для UE, поступает от сервера аутентификации, авторизации и учета (AAA) на шлюз служебной сети доступа (ASN), на базовую станцию (BS). BS применяет приоритетный режим к распределению ресурсов и составлению графика потоков приоритетного обслуживания.

2) После вызова ETS, поступившего от UE, индикация приоритета, связанная с потоками обслуживания для UE, поступает от прикладной функции (AF) на сервер AAA/функции политики (PF), на шлюз ASN, на BS. BS применяет приоритетный режим к распределению ресурсов и составлению графика потоков приоритетного обслуживания.

3) После передачи обслуживания индикация приоритета, связанная с потоками обслуживания для UE, сохраняется от служебной BS на целевую BS для передачи облуживания в пределах ASN и от шлюза служебной ASN на шлюз целевой ASN. Базовые станции применяют приоритетный режим к распределению ресурсов и составлению графика по всем потокам приоритетного обслуживания в ходе подготовки и выполнения передачи обслуживания.

4) После поискового вызова на UE в нерабочем режиме индикация приоритета, связанная с потоком обслуживания поступает от шлюза ASN с функцией маршрута данных на контроллер поисковых вызовов привязки и далее на BS. BS применяет приоритетный режим к распределению ресурсов и составлению графика для потоков приоритетного обслуживания в радиовещательных сообщениях поисковых вызовов. В ответ на приоритетный поисковый вызов, когда UE входит в сеть, BS распознает приоритет входящего вызова ETS и предоставляет приоритетный режим для UE для выхода из нерабочего режима, а также добавление/изменение служебного потока для вызова ETS в UE, завершающее вызов.

Для версии 2.0, которая включает индикацию приоритета и режим для запроса диапазона, создания потока обслуживания и универсального интерфейса услуг (USI), разрабатываются дополнительные процедуры и сообщения Этапа 3 ETS.

9.4.3 Фиксированный доступ

Требуется, чтобы сети фиксированного доступа обеспечивали конкретные механизмы и возможности предоставления авторизованным вызовам или сеансам электросвязи в чрезвычайных ситуациях предпочтительного/приоритетного режима. Для предоставления такого режима могут использоваться механизмы и возможности, зависящие от технологии (например, [b-802.1p] с xDSL, IPCablecom, Packet Cable 2). Это включает, помимо прочего, механизмы и возможности для:

- распознавания трафика электросвязи в чрезвычайных ситуациях: такое распознавание включает идентификацию и маркировку авторизованного трафика электросвязи в чрезвычайных ситуациях;
- предпочтительного/приоритетного доступа к ресурсам/средствам: это облегчает доставку в СПП запроса на электросвязь в чрезвычайных ситуациях, если имеющиеся ресурсы доступа ограничены;

- предпочтительной/приоритетной маршрутизации трафика электросвязи в чрезвычайных ситуациях: это может предполагать такие свойства, как постановку в очередь на имеющиеся ресурсы, исключение из определенных ограничительных функций управления сетью и резервирование некоторых маршрутов/путей для трафика электросвязи в чрезвычайных ситуациях;
- предпочтительного/приоритетного установления сеансов или вызовов электросвязи в чрезвычайных ситуациях.

В следующих далее подпунктах приводятся соображения, касающиеся технологий.

9.4.3.1 Доступ по сети IPCablecom

В [ITU-T J.260] определены требования для услуги предпочтительной электросвязи по сетям IPCablecom. В [ITU-T J.261] определена концепция разработки спецификаций для обеспечения этих требований по обеим – IPCablecom и IPCablecom 2 – сетям. В этой концепции рассматриваются две ключевые области: приоритет и аутентификация. Другие области, такие, как обеспечение для восстанавливаемости, определены для будущих версий. Концепция по определению включает общие аспекты, а также различия, обусловливаемые используемой в сетях IPCablecom и IPCablecom 2 архитектурой (на основе IMS). IPCablecom и IPCablecom 2 – это сети с коммутацией пакетов, свойства которых рассматривались в пункте 6, например совместное использование ресурсов для трафика передачи данных и управления. Концепция [ITU-T J.261] классифицирует требования к приоритету в [ITU-T J.260] в аспектах сигнализации, маркирования и механизмов.

В [ITU-T J.262] определена спецификация для обеспечения требований аутентификации в сетях IPCablecom 2. В [ITU-T J.262] включены примеры потоков для иллюстрации обмена сообщениями для разных сценариев, соответствующих аутентификации на основе PIN, использованию заголовка приоритета ресурса SIP: агент пользователя, инициирующий вызов VoIP пользователю КТСОП, используя PIN; агент пользователя, инициирующий вызов VoIP другому агенту пользователя VoIP, используя PIN и аутентификацию на основе контракта.

В [ITU-T J.263] определена спецификация для обеспечения приоритетной сигнализации для предпочтительного обслуживания с использованием заголовка приоритета ресурса SIP [IETF RFC 4412]. В спецификацию включены два варианта: 1) UA инициирует запрос, включающий заголовок приоритета ресурса; 2) на основании информации запроса заголовок приоритета ресурса с соответствующим значением уровня приоритета включается в P-CSC-FE. В приложения к [ITU-T J.263] включены пространство имени и значения уровня приоритета, которые должны использоваться в разных регионах. В ряде регионов требуется поддерживать значения, определенные в [IETF RFC 4412]. В [ITU-T J.263] также описана взаимосвязь с потоками обслуживания, которые формируются в процессе обеспечения встроенного мультимедийного адаптера терминала (E-MTA) на уровне DOCSIS MAC в целях отображения требуемых параметров QoS для предпочтительной электросвязи. Механизм маркирования, определенный для передачи данных, отсутствует, поскольку RTP не включает маркировки для индикации приоритета. Поддерживающие приоритеты механизмы для резервирования ресурсов и осуществления управления допуском поддерживаются путем установки вентилей, определенных как часть динамического качества обслуживания (DQoS) в IPCablecom.

9.4.3.2 Доступ по сети xDSL

Эталонная архитектура агрегирования DSL на базе Ethernet описана в [BBF TR-101]. Управление политикой в сети доступа DSL основано на спецификациях, определенных а [BBF TR-058] и [BBF TR-059].

Базовый подход к обеспечению возможностей ETS сети доступа DSL заключается в использовании существующих возможностей QoS для предоставления приоритета вызову/сеансу ETS. При этом подходе сервер политики/точка выбора правил (PDP) – единственное "знающее о ETS" устройство, и оно устанавливает соответствующий приоритет, который должен применяться к потокам с использованием возможностей QoS в шлюзе широкополосной сети (BNG).

В силу неблокирующего характера устройства сопряжения с сетью (NID) и главного коммутационного щита (MDF) в этих сетевых элементах не требуется наличия функций ETS. Ширина полосы обеспечивается и фиксируется между NID и мультиплексором доступа к цифровой абонентской линии (DSLAM), и DSLAM также спроектирован неблокирующим. Таким образом, выбранным подходом является использование возможностей QoS шлюза BNG для управления

потоком данных через DSLAM, с тем чтобы гарантировать, что этот трафик не приведет к перегрузке DSLAM.

Функция агрегирования Ethernet разработана для транспортирования всего трафика между BNG и DSLAM и является, следовательно, еще одним неблокирующим элементом.

Шлюз доступа к оборудованию в помещении клиента (CPE) может знать или не знать о ETS. Если он знает о ETS, то шлюз доступа может устанавливать приоритет трафика ETS для обеспечения передачи в сеть доступа DSL и для обеспечения того, что не произойдет перегрузки DSLAM.

Сервер политики/точка выбора правил отвечает за применение надлежащей политики для трафика ETS к BNG. Для ETS сервер политики/точка выбора правил реализует правила управления допуском, для того чтобы обеспечить высокую вероятность успешного осуществления вызова или сеанса ETS. Правила касаются установления, поддержания и завершения вызова или сеанса ETS через сеть доступа DSL к сети в помещении клиента. В качестве исходного условия принимается, что сервер политики/точка выбора правил будет получать запрос вызова или сеанса ETS от СПП (например, прокси-функционального объекта управления вызовом/сеансом (P-CSC-FE)). Сервер политики/точка выбора правил распознает запрос с соответствующей информацией ETS и даст надлежащим образом команду BNG об обеспечении приоритетного режима.

BNG отвечает за обеспечение приоритета для трафика ETS. BNG применяет команды сервера политики/точки выбора правил, резервируя и устанавливая соответствующие ресурсы для обработки вызова или сеанса ETS. Он применяет приоритетный режим, включая маркирование пакетов носителя для приоритетного режима в целях передачи на шлюз доступа к CPE и в региональную широкополосную сеть.

9.4.3.3 Доступ по волоконной сети (FTTx)

Эталонная архитектура пассивной оптической сети (PON) для волоконного доступа описана в [ITU-T G.983.1]. Эталонная архитектура относится к системе управления узлами доступа (ANMS) для управления окончанием оптической линии (OLT) и оконечным оборудованием оптической сети (ONT). ANMS обеспечивает функциональные возможности точки выбора правил (PDP), которые усиливаются точками применения правил (PEP), расположенными в OLT и ONT.

В настоящее время прямое управление политикой или применение правил в волоконных сетях доступа не используется. Вместе с тем для обеспечения обработки установления вызова или сеанса с приоритетом ETS в волоконной сети доступа ANMS потребуется поддерживать динамические функции управления политикой. Базовый подход к обеспечению возможностей ETS в волоконной сети доступа заключается в использовании существующих возможностей QoS для обеспечения приоритета в рамках вызова или сеанса ETS. При этом подходе ANMS (например, сервер политики) – единственное "знающее о ETS" устройство, и оно устанавливает соответствующий приоритет, который должен применяться к потокам с использованием возможностей QoS в OLT и ONT. Политика ETS передается посредством сигнализации по интерфейсу Q3 (который определен в [ITU-T Q.812]) в OLT и отображается из OLT в ONT через интерфейс контроля и управления ONT (OMCI).

ANMS отвечает за обеспечение соответствующей политики для трафика ETS в OLT. ANMS реализует для ETS правила управления допуском, для того чтобы обеспечить высокую вероятность успешного осуществления вызова или сеанса ETS. Правила касаются установления, поддержания и завершения вызова или сеанса ETS в волоконной сети доступа. ANMS принимает окончательные решения относительно политики и обеспечивает достаточную информацию, в соответствии с которой OLT и ONT выполняют управление ресурсами для ETS. В качестве исходного условия принимается, что ANMS будет получать запрос вызова или сеанса ETS от СПП (например, прокси-функционального объекта управления вызовом или сеансом (P-CSC-FE)). ANMS распознает запрос с соответствующей информацией ETS и даст надлежащим образом команду OLT об обеспечении приоритетного режима.

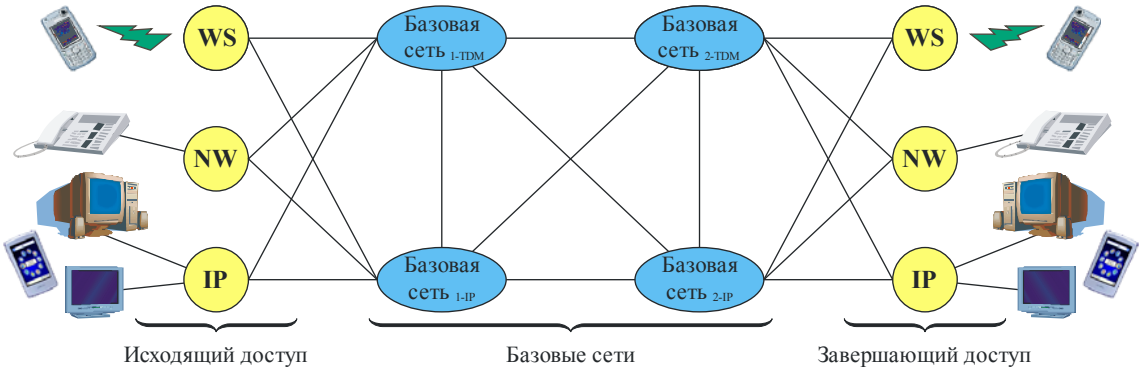
OLT и ONT разработаны для транспортирования всего трафика ETS. OLT отвечает за обеспечение приоритета для трафика ETS. OLT применяет команды ANMS, резервируя и устанавливая соответствующие ресурсы для обработки вызова или сеанса ETS. Он применяет приоритетный режим, включая маркирование пакетов носителя для приоритетного режима в целях передачи.

10 Сквозное обеспечение электросвязи в чрезвычайных ситуациях

На рисунке 2 представлена матрица сквозного вызова или сеанса для обеспечения разных протоколов вызова или сеанса ETS. Она иллюстрирует вызовы или сеансы:

- исходящие и завершающиеся при доступе по IP (например, кабель и DSL), узкополосном проводном доступе (например, телефон КТСОП) и при беспроводном доступе (например, телефон GSM и CDMA); и
- прохождение по базовым сетям IP и с коммутацией каналов (TDM).

Обеспечение сквозной ETS требует взаимодействия по характерной для ETS информации между доменом технологии IP и доменами других технологий (например, доменами беспроводного или проводного TDM). Это включает необходимое взаимодействие для сквозного вызова или сеанса ETS, который может пересекать домены разных технологий, показанные на рисунке 2. Например, необходимо передавать посредством сигнализации характерную для ETS информацию (например, маркировку вызова ETS, уровень приоритета) через интерфейс сеть-сеть (NNI) между поставщиками присоединенных СПП.



WS – беспроводный доступ
NW – узкополосный проводный доступ

ПРИМЕЧАНИЕ. – Базовая сеть является аутентифицирующей сетью, транзитной сетью или и той, и другой.

Y.2205(11)_F02

Рисунок 2 – Матрица сквозного вызова или сеанса

Сценарии вызова или сеанса, связанные с рисунком 2, представлены в [b-ATIS-1000010]. В [b-ATIS-1000010] определены процедуры и возможности, требуемые для обеспечения ETS в рамках сетей и между сетями поставщиков услуг на базе IP. На основе представленной на рисунке 2 матрицы возможны следующие сценарии вызова или сеанса:

– Исходящий доступ к базовой сети 1
  - исходящий проводной доступ к базовой IP-сети;
  - исходящий беспроводный доступ к базовой IP-сети;
  - исходящий IP-доступ к базовой IP-сети;
  - исходящий IP-доступ к базовой сети TDM.
– Базовая сеть 1 к базовой сети 2
  - базовая сеть TDM к базовой IP-сети;
  - базовая IP-сеть к базовой сети TDM;
  - базовая IP-сеть 1 к базовой IP-сети 2.
– Базовая сеть 2 к завершающему доступу
  - базовая IP-сеть к проводному завершающему доступу;
  - базовая IP-сеть к беспроводному завершающему доступу;
  - базовая IP-сеть к IP завершающему доступу;
  - базовая TDM сеть к IP завершающему доступу.

Установление вызова или сеанса ETS требует тщательной реализации необходимых протоколов сигнализации, которые перенесут нужную информацию, отвечающую критическому характеру ETS. Для обеспечения сквозного приоритетного режима важно поддерживать отображение информации о приоритете для содействия "бесшовному" взаимодействию протоколов при использовании в рамках сети разных протоколов (например, вертикальное взаимодействие протоколов между управлением вызовом или сеансом и управлением носителем) или между сетями разных типов (например, взаимодействие управления вызовом или сеансом между двумя сетями), включая КТСОП. Аналогично исключительно важно разрешать отображение информации о приоритете для содействия "бесшовному" взаимодействию между транспортированием разных типов, то есть между разными типами среды. Без такого взаимодействия/отображения сквозной приоритетный режим может быть недостижим.

МСЭ-Т в настоящее время подготавливает руководящие принципы отображения требуемых атрибутов протокола сигнализации (информация о приоритете ETS) для обеспечения надлежащего установления и допуска ETS для разных "горизонталей" (например, ISUP, SIP, ITU-T H.225.0) и "вертикалей" (например, ITU-T H.248.0, Diameter).

В [ITU-T Q-Sup.57] представлены требования к сигнализации для обеспечения предпочтительных возможностей в рамках IP-сетей для ETS. Пример потока вызова из [ITU-T Q-Sup.57], иллюстрирующий успешную аутентификацию и установление вызова или сеанса ETS, представлен в Дополнении III.

11 Механизмы и возможности для обеспечения некоторых аспектов раннего предупреждения в СПП

11.1 Общие положения

Системы оповещения, используемые для раннего предупреждения, можно отнести к моделям двух классов: с принудительным оповещением и с оповещением по запросу.

Модели с принудительным оповещением основаны на регистрации контактной информации участников (например, адресов электронной почты) в центральной службе. Когда происходит событие, эти зарегистрированные участники оповещаются о нем с потенциально большим числом указателей на дополнительную информацию. Ключевым элементом проекта архитектуры в данной модели является то, что центральный орган определяет вопрос о том, должна ли распространяться данная информация, и что это повлечет за собой. Сильной стороной данной модели является то, что в ней решается вопрос о выполнении работы, связанной с мониторингом событий, и, таким образом, пользователи имеют возможность продолжать выполнять свои обычные обязанности и не заниматься мониторингом потенциальных бедствий и чрезвычайных ситуаций.

Модель с принудительным оповещением представляет собой механизм распространения от "одного" ко "многим", и она может быть реализована как в страте обслуживания, так и в страте транспортирования (например, многоадресная передача).

Отличие модели с оповещением по запросу от модели с принудительным оповещением состоит в том, что она основана на обмене информацией по принципу запрос-ответ. В то время как обе модели основаны на регистрации со стороны отдельных участников, в модели с оповещением по запросу ответственность за мониторинг и получение информации возлагается на отдельных пользователей. Преимуществом данной системы является то, что информация предоставляется исключительно по мере необходимости или по запросу.

В заключение следует отметить, что в системах оповещения используются существующие приложения и основополагающие возможности, присущие сетям на основе протокола IP. Добавление принципов принудительного оповещения или оповещения по запросу помогает сделать эти системы более приспособленными к потребностям и ожиданиям пользователей. Применение каждого из видов систем оповещения может также осуществляться в тандеме: модели с принудительным оповещением могут осуществлять периодический автоматический мониторинг и уведомление, а модели с оповещением по запросу могут использоваться для получения конкретной информации по запросу.

Примеры моделей с принудительным оповещением и с оповещением по запросу приведены в Дополнении II.

11.2 Протокол общего оповещения (CAP)

В данном пункте описывается протокол общего оповещения (CAP), определенный в [ITU-T X.1303], который может использоваться для обеспечения приложений раннего предупреждения. CAP использует расширяемый язык разметки (XML) и обеспечивает стандартные форматы обмена данными для структурированной информации.

В [ITU-T X.1303] определяется общий формат для обмена оповещениями о чрезвычайной ситуации и предупреждения населения обо всех видах угроз по всем типам сетей. CAP позволяет одновременно распространять предупреждающие сообщения по многим различным системам предупреждения и таким образом повысить эффективность предупреждения, упростив при этом задачу по предупреждению. CAP также способствует обнаружению на основе местных предупреждающих сообщения различного типа такого варианта развития событий, который может указывать на скрытую угрозу или враждебное действие. CAP также обеспечивает шаблон для эффективных предупреждающих сообщений на основе передового опыта, полученного из научного исследования и реальных событий.

CAP обеспечивает открытый непатентованный формат сообщения для всех типов оповещений и уведомлений. Он не относится ни к какому конкретному приложению или методу электросвязи. Формат CAP совместим с новыми методами, например веб-службами и ускоренными веб-службами МСЭ-Т, а также с существующими форматами, включая кодирование сообщений для конкретной территории (SAME), которое используется Национальным управлением океанических и атмосферных исследований (NOAA) Соединенных Штатов Америки для системы метеорологической радиосвязи и системы оповещения о чрезвычайных ситуациях (EAS), и при этом предоставляет следующие усовершенствованные возможности:

- гибкое географическое позиционирование с использованием широтно-долготных профилей и других трехмерных геопространственных изображений;
- передачу многоязычных сообщений и сообщений, рассчитанных на многочисленную аудиторию;
- распределение и задержку эффективного времени действия и истечения времени действия;
- усовершенствованные характеристики обновления и отмены сообщений;
- поддержку шаблонов для формирования полных и эффективных предупреждающих сообщений;
- обеспечение возможности цифрового шифрования и цифровой подписи; а также
- средство для передачи цифровых изображений и звука.

CAP обеспечивает снижение затрат и простоту эксплуатации путем устранения необходимости в многочисленных интерфейсах на основе заказного программного обеспечения, используемых для многих источников предупреждения и систем распространения, задействованных в предупреждении обо всех видах угроз. Формат сообщения CAP можно преобразовать в прямом и обратном направлении для "родных" форматов всех видов датчиков и методов оповещения и тем самым создать основу для независимого в технологическом отношении национального и международного "предупреждающего интернета".

Протокол CAP, определенный в [ITU-T X.1303], технически соответствует общему протоколу оповещения OASIS стандарта V1.1 и совместим с ним. OASIS также определяет CAP V1.2, содержащий обновления CAPV1.1.

В [ITU-T X.1303] представлена соответствующая спецификация ASN.1, которая допускает компактное двоичное кодирование и использование ASN.1, а также средств определения схемы XML (XSD) для создания и обработки сообщений CAP. [ITU-T X.1303] обеспечивает для существующих систем, например систем H.323, возможность более простого кодирования, транспортирования и декодирования сообщений CAP.

11.3 Процедуры регистрации дуг в рамках дуги идентификатора оповещающего объекта

В [ITU-T X.674], *Процедуры регистрации дуг в рамках дуги идентификатора оповещающего объекта*, представлена регистрация дуг идентификатора объекта (OID) для идентификации разных видов оповещений и оповещающих учреждений. В частности, в Рекомендации описаны процедуры регистрации дуг для идентификации (всех видов) оповещений и оповещающих учреждений в дуге идентификатора оповещающего учреждения {joint-iso-itu-t(2) alerting(49)} согласно [ITU-T X.660].

[ITU-T X.674] упрощает распределение и использование OID для идентификации оповещающих учреждений (например, оповещающие учреждения, назначенные государствами – членами Всемирной метеорологической организации (ВМО).

ПРИМЕЧАНИЕ. – ВМО ведет реестр оповещающих органов. Реестр размещен по адресу: http://www-db.wmo.int/alerting/authorities.html.

12 Приоритет восстановления обслуживания

В случае отказа или нарушения работы сети работа критических служб (например, экстренных служб) может быть прервана, и, возможно, для нее потребуется более высокая вероятность успешного восстановления по сравнению с другими службами. В [ITU-T Y.2172] определяется три уровня приоритета восстановления для служб СПП. Это позволяет установить такую классификацию приоритетов, используемых в сигнальных сообщениях, при которой для рассматриваемого вида обслуживания может быть предоставлено установление вызова или сеанса с желаемым приоритетом восстановления. Таким образом, критическим службам будет обеспечена более высокая вероятность успешного восстановления по сравнению с другими службами.

13 Защитная коммутация и восстановление

13.1 Общие соображения

Ряд обобщенных понятий, общих для многих технологий транспортирования, описан в [ITU-T G.808.1]. Некоторые важные вопросы, которые следует принять во внимание при обеспечении защиты трафика электросвязи в чрезвычайных ситуациях, определены в [ITU-T G.808.1].

13.1.1 Индивидуальная защита

Понятие индивидуальной защиты применяется к таким ситуациям, когда целесообразно обеспечивать защиту только части сигналов трафика, для которых необходима высокая надежность.

13.1.2 Групповая защита

Это допускает защитную коммутацию посредством логического связывания транспортных объектов в единый объект после начала защитных действий.

13.1.3 Типы архитектуры

В [ITU-T G.808.1] определены следующие типы архитектуры, которые кратко представлены ниже.

13.1.3.1 Архитектура защиты 1+1

В архитектуре защиты 1+1 защитный транспортный объект назначается резервным средством рабочего транспортного объекта.

13.1.3.2 Архитектура защиты 1:n

В архитектуре 1:n защитный транспортный объект назначается общим резервным средством n рабочих транспортных объектов.

13.1.3.3 Архитектуры защиты m:n

В архитектуре m:n m выделенных защитных транспортных объектов являются общими резервными средствами n рабочих транспортных объектов, где, как правило, $m \leq n$.

13.1.4 Тип коммутации

Защитная коммутация по типу может подразделяться на однонаправленную коммутацию и двунаправленную коммутацию.

Следует заметить, что все типы коммутации, за исключением однонаправленной коммутации 1+1, требуют канала связи между двумя концами защищаемого домена; такой канал называется каналом автоматической защитной коммутации (APS).

Перечень достоинств и недостатков применения разных типов коммутации ко всем вышеперечисленным случаям, содержится в [ITU-T G.808.1].

В контексте электросвязи в чрезвычайных ситуациях на базе IP достаточной может быть однонаправленная коммутация, поскольку, в общем, маршруты в каждом направлении не связаны напрямую в силу однонаправленного характера трасс/маршрутов по сетям на базе IP.

13.1.5 Типы срабатывания

По типу срабатывания защита может быть невозвратная или возвратная.

При возвратном срабатывании сигнал трафика (услуга) всегда возвращается в рабочий транспортный объект (или остается в нем), по его восстановлении после дефекта.

При невозвратном срабатывании сигнал трафика (услуга) не возвращается в исходный рабочий транспортный объект.

Как отмечено в [ITU-T G.873.1], защита 1+1 обеспечивается, в основном, как невозвратная, поскольку эта защита является полностью выделенной в любом случае, в результате чего устраняется второй "выброс" в трафике. Вместе с тем могут возникнуть причины для обеспечения такой защиты как возвратная (например, так чтобы трафик использовал "короткое" направление по кольцу, кроме ситуации отказа). Правила ряда операторов также предусматривают возвратное срабатывание даже для 1+1).

13.2 Архитектура защиты СЦИ

В [ITU-T G.841] содержатся необходимые спецификации на уровне оборудования для реализации разных выборов архитектуры защиты для сетей с синхронной цифровой иерархией (СЦИ).

Диапазон защищаемых объектов может простираться от одиночной мультиплексной секции СЦИ (например, линейная защита мультиплексной секции) до части сквозного маршрута СЦИ (например, защита соединения подсети) или до целого сквозного маршрута СЦИ. Физическая реализация таких видов архитектуры защиты может включать кольцевые или линейные цепочки узлов. Все классификации защиты включают руководящие принципы по сетевым задачам, архитектуре, прикладным функциональным возможностям, критериям коммутации, протоколам и алгоритмам.

Кроме того, в [ITU-T G.842] содержатся спецификации для взаимодействия сетевых архитектур защиты. В частности, охватываются присоединения одиночных и двойных узлов между кольцами защиты, использующими MS, и кольцами защиты соединений подсети (SNCP) подобного или иного типов.

13.3 Оптическая транспортная сеть (ОТС)

В [ITU-T G.873.1] определен протокол автоматической защитной коммутации (APS) и функционирование защитной коммутации для схем линейной защиты для оптической транспортной сети на уровне блока данных оптического канала (ODUk).

В [ITU-T G.873.1] рассматриваются следующие схемы защиты:

– защита соединения подсети ODUk с внутренним контролем (1+1, 1:n);

– защита соединения подсети ODUk с ненарушающим контролем (1+1);

– защита соединения подсети ODUk с контролем подуровня(1+1, 1:n).

Для данного направления передачи "головной конец" защищаемого сигнала может выполнять функции моста, который при необходимости поместит копию сигнала нормального трафика в защитный объект. "Хвостовой конец" будет выполнять функцию селектора, где возможен выбор сигнала нормального трафика либо из его обычного рабочего объекта, либо из защитного объекта. В случае двунаправленной передачи, где защищаются оба направления передачи, оба конца защищаемого сигнала будут, как правило, обеспечивать обе функции – моста и селектора.

13.4 Линейная защитная коммутация Ethernet

В [ITU-T G.8031] описана конкретная защитная коммутация для сигналов VLAN Ethernet. Включена подробная информация о характеристиках и архитектуре защиты сети уровня Ethernet (ETH), а также протоколе APS.

В [ITU-T G.8031] определены варианты архитектуры линейной защитной коммутации 1+1 и 1:1 с однонаправленной и двунаправленной коммутацией.

В архитектуре линейной защитной коммутации 1+1 каждому рабочему транспортному объекту выделяется защитный транспортный объект. Нормальный трафик копируется и передается обоим объектам – рабочему и защитному – с постоянным мостом в источнике защищаемого домена. Трафик в рабочем и защитном транспортных объектах передается одновременно к приемнику защищаемого домена, где делается выбор между рабочим и защитным транспортным объектами на основе ряда определенных заранее критериев, таких как индикация дефекта сервера.

Поскольку выбор делается только в приемнике защищаемого домена в архитектуре защитной коммутации 1+1, для двунаправленной защитной коммутации 1+1 требуется протокол координации APS, с тем чтобы селекторы для обоих направлений выбирали тот же объект. С другой стороны, для однонаправленной защитной коммутации 1+1 не требуется протокол координации APS.

В архитектуре линейной защитной коммутации 1:1 рабочему транспортному объекту выделяется защитный транспортный объект. Однако нормальный трафик транспортируется либо в рабочем транспортном объекте, либо в защитном транспортном объекте с использованием моста селектора в источнике защищаемого домена. Селектор в приемнике защищаемого домена выбирает объект, который несет нормальный трафик. Поскольку источник и приемник необходимо координировать для обеспечения того, чтобы мост селектора в источнике и селектор в приемнике выбирали тот же объект, требуется протокол координации APS.

13.5 Кольцевая защитная коммутация Ethernet

В [ITU-T G.8032] определен протокол автоматической защитной коммутации (APS) и механизмы защитной коммутации для кольцевой топологии Ethernet уровня ETH. Включена подробная информация о характеристиках и архитектуре кольцевой защиты Ethernet, а также кольцевом протоколе APS.

Защитный протокол, определенный в [ITU-T G.8032], поддерживает возможность установления защищаемого соединения пункта и пунктом, пункта со многими пунктами и многих пунктов со многими пунктами в пределах кольца или взаимосоединенных колец, называемых топологией "многокольцевая/многозвенная сеть".

13.6 Линейная защитная коммутация для транспортной MPLS (T-MPLS)

В [ITU-T G.8131] представлены требования и механизмы для сквозной защитной коммутации канала и соединения подсети (SNC) для транспортных сетей MPLS (T-MPLS). В Рекомендации описаны типы архитектуры защиты канала и защиты SNC, однонаправленный и двунаправленный типы коммутации и возвратный и невозвратный типы срабатывания. Определяется протокол автоматической защитной коммутации (APS), используемый для согласования обоих концов защищаемого домена.

В [ITU-T G.8131] определяется архитектура 1+1 и архитектура 1:1. Архитектура 1+1 работает с однонаправленной коммутацией. Архитектура 1:1 работает с двунаправленной коммутацией.

13.7 Защитная коммутация ATM

В [ITU-T I.630] представлены типы архитектуры и механизмы для защитной коммутации на уровне ATM. Архитектура включает расширение защищаемого домена и группировку защищаемого домена. Ресурсы для защитных объектов распределяются заранее. В состав механизма входят триггер защитной коммутации, механизмы удержания и протокол управления защитной коммутацией.

В [ITU-T I.630] описана индивидуальная защита VP/VC и групповая защита. Индивидуальная защита VP/VC – это метод, при котором для рабочего объекта и защитного объекта используется одно соединение сети и/или подсети. Групповая защита – это метод, при котором для рабочего объекта и защитного объекта используется логическое объединение одного или более соединений сети и/или подсети.

В настоящее время в [ITU-T I.630] описана двунаправленная защитная коммутация 1+1 и 1:1, а также однонаправленная защитная коммутация 1+1.

13.8 Защитная коммутация для сетей MPLS

В [ITU-T Y.1720] представлены требования и механизмы для функциональных возможностей защитной коммутации 1+1, 1:1, совместно используемых ячеек и пакетов 1+1 для пользовательской плоскости уровневых сетей MPLS. Описанный ниже механизм предназначен для обеспечения сквозных трактов LSP связи пункта с пунктом.

[ITU-T Y.1720] составлена для определения способов защитной коммутации. В [ITU-T Y.1720] разъясняется разница между защитной коммутацией и повторной маршрутизацией следующим образом:

Защитная коммутация: подразумевается, что и маршрутизация, и ресурсы рассчитаны заранее и распределены выделенному защитному LSP до возникновения отказа. Защитная коммутация, таким образом, надежно обеспечивает возможность повторного получения требуемых сетевых ресурсов после отказа.

Повторная маршрутизация: подразумевается, что выделенный защитный LSP не определен и что ни маршрутизация, ни ресурсы не рассчитаны заранее или не распределены до возникновения отказа. Повторная маршрутизация обычно применяется к случаям, когда используются функции маршрутизации и сигнализации и когда "запрос на восстановление соединения" должен быть подан при отказе (сетью или пользователем), и этот "запрос на восстановление соединения" должен конкурировать с другими аналогичными типами трафика в отношении получения требуемого ресурса. Поэтому изменение маршрута передачи не дает гарантии возможности вновь получить требуемый сетевой ресурс после отказа, и обычно этот метод медленнее, чем защитная коммутация.

Защитная коммутация необходима для быстрого восстановления после отказа и, таким образом, повышает показатель надежности и готовности сетей MPLS.

Для защитной коммутации необходимы следующие характеристики:

1) Защитная коммутация должна применяться ко всему LSP.
2) Приоритизированная защита между сигналом отказа и запросами оператора на коммутацию.
3) Необходимо обеспечить возможность защиты на MPLS уровне максимально оперативно (в зависимости от временно́й разрешающей способности детектора обнаружения неисправности).
4) Коэффициент защиты равен 100%, т. е. 100% рабочего трафика, которому может быть причинен ущерб, защищено от отказа в одном работающем LSP.
5) По возможности должна поддерживаться дополнительная пропускная способность.

Дополнение I

Категории электросвязи в чрезвычайных ситуациях

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Электросвязь в чрезвычайных ситуациях между отдельным лицом и органом власти

Инициатором электросвязи между отдельным лицом и органом власти выступает отдельное лицо, использующее обычные возможностей электросвязи в чрезвычайных ситуациях, с целью получения экстренной помощи во время отдельной (относящейся лично к нему) чрезвычайной ситуации либо даже ограниченной чрезвычайной ситуации. Например, вызов от отдельного лица к органу власти может осуществляться с использованием короткого набираемого номера (например, 112, 911 и т. д.), который обеспечивает соединение отдельного пользователя с центром обработки экстренных вызовов. Центр может передать сообщение соответствующей организации-исполнителю (полиции, пожарной службе, службе скорой медицинской помощи) от имени вызывающего абонента. В центр обслуживания вызовов может автоматически передаваться дополнительная информация, например о местонахождении вызывающего абонента. Такая информация может облегчить и даже обеспечить более быстрое реагирование, поскольку иногда вызывающие абоненты не могут либо не имеют времени или возможности предоставить эту информацию самостоятельно. Такой вид связи обычно подразумевает соединение по принципу от одного к одному, при котором инициатор взаимодействует главным образом с ведомством назначения. Подавляющее большинство таких вызовов электросвязи касается небольших по масштабу чрезвычайных ситуаций (например, пожар в отдельном доме), возникших преимущественно вследствие несвязанных событий, в то время как крупномасштабные события (например, землетрясения) могут привести ко многим одновременно связанным последствиям. (Выражение "отдельный" используется в широком смысле и должен распространяться на любое лицо, которому требуется экстренная помощь, включая, например, граждан, приезжих и других, живущих в конкретном месте). Стороны, участвующие в электросвязи в чрезвычайных ситуациях, могут общаться друг с другом с помощью многих видов средств, включая передачу голоса, изображения, текста в реальном времени и мгновенной передачи сообщений.

I.2 Электросвязь в чрезвычайных ситуациях между отдельными лицами

Инициаторами категории электросвязи в чрезвычайных ситуациях между отдельными лицами становятся и отдельные лица (или устройства) из числа граждан, и организации. Например, сразу после того как происходит чрезвычайная ситуация, потребность граждан в общении друг с другом становится высокой. Следовательно, возникает повышенный спрос на электросвязь между отдельными лицами, в то время как ресурсы электросвязи могут быть ограничены в результате повреждений, причиненных чрезвычайными событиями. С учетом всех этих факторов сети электросвязи могут оказаться перегруженными.

I.3 Электросвязь в чрезвычайных ситуациях между органами власти

Электросвязь в чрезвычайных ситуациях между органами власти обычно осуществляется с участием авторизованного пользователя электросвязи в чрезвычайных ситуациях (или его/ее организации), который инициирует взаимодействие с другим авторизованным пользователем, с тем чтобы:

1) содействовать проведению восстановительных работ (например, путем создания центров управления в чрезвычайных ситуациях и соответствующих органов административного управления для получения от правительства или других организаций помощи в виде ресурсов);
2) восстановить основную коммунальную инфраструктуру (например, необходимое водоснабжение, подачу электроэнергии и т. д.); и
3) приступить к выполнению мер по обеспечению долгосрочного полного восстановления (например, восстановления дорог, мостов, зданий и т. д.).

Исторически сложилось, что электросвязь в чрезвычайных ситуациях между органами власти (иногда называемая электросвязью в целях общественной безопасности) с одновременным задействованием сетей общего пользования осуществлялась в случае, когда ресурсы электросвязи оказывались перегруженными в связи с увеличением использования электросвязи между отдельными пользователями.

Учитывая огромные возможности электросвязи в чрезвычайных ситуациях между органами власти для содействия восстановлению нормального состояния и недопущения дальнейших угроз гражданам или имуществу, данной категории электросвязи в чрезвычайных ситуациях может быть предоставлен приоритетный статус над другими категориями электросвязи в чрезвычайных ситуациях во время объявленных чрезвычайных ситуаций или при их обострении.

I.4 Электросвязь в чрезвычайных ситуациях между органом власти и отдельным лицом

В заключение рассмотрим электросвязь в чрезвычайных ситуациях между органом власти и отдельным лицом (относимую иногда к категории систем раннего предупреждения), обычно предполагающую передачу информации, которая предназначена для населения и которая поступает из авторизованного источника. Содержание может нести информацию, которая предназначена для общин, пострадавших в результате бедствия, например меры безопасности, инструкции, руководящие указания, советы и т. д. Обычно инициатором конкретного вызова электросвязи выступает один авторизованный пользователь, при этом получателями информации являются многие отдельные лица.

Связь любого с любым: пример ETS из любого места/от любого устройства для вхождения в контакт с любым другим пользователем (ETS или гражданами) с помощью некоторых мер обеспечения предпочтительного режима со стороны инфраструктуры связи. Хорошим примером является служба GETS в КТСОП, в случае если предпочтительное обслуживание не является повсеместно распространенным и не ограничено выборочным набором оконечных устройств и адресатов.

Связь одного с одним: применительно к электросвязи в чрезвычайных ситуациях данный вид связи является разновидностью случая связи любого с любым. В данном случае число участников ограничено любыми двумя пользователями ETS.

Связь многих с одним: одним из вариантов реализации данной модели является архитектура клиент-сервер для услуги на базе веб, при которой любой из пользователей имеет доступ к одному хорошо известному месту размещения информации. В КТСОП данная модель реализуется с помощью систем 911, 112 и т. д., при которых сеансы в пределах района передаются в единый пункт сообщений общественной безопасности (PSAP).

Связь одного со многими: в данной модели информация передается из одного источника группе приемников (конечных пользователей), избранных для участия в распространении данных. В случае вещательной среды передачи, прекрасными примерами являются телевидение и радио, поскольку приемники лишь получают информацию по выбранному ими каналу. В модели с передачей данных можно провести различие между связью одного со многими и широковещательной передачей, поскольку широковещательная передача подразумевает, что сообщение получают все узлы, независимо от того, выбраны они или нет, в то время как при связи каждого с каждым предполагается непосредственное участие в группе.

Дополнение II

Пример случаев использования систем оповещения для раннего предупреждения

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

II.1 Модель с принудительным оповещением

Системы оповещения на основе модели с принудительным оповещением предлагаются как частным, так и государственным секторами. Однако в настоящей Рекомендации рассматривается только пример общественного сектора. Примером модели с принудительным оповещением для общественного или государственного сектора является веб-сайт центра информации о чрезвычайных ситуациях (http://alert.dc.gov/eic/site/default.asp) органов местного самоуправления г. Вашингтона (округ Колумбия). Пользователи указывают при регистрации контактную информацию, включающую адрес электронной почты, номер пейджера или мобильного телефона (либо текстовое сообщение, либо автоматизированная передача голосовых сообщений). Автоматизированная передача голосовых сообщений эквивалентна передаче сообщений "inverse-911", и все жители округа Колумбия, подключенные с соответствующими станциями проводной телефонной связи, автоматически зарегистрированы в этой службе. Поскольку услуга оповещения предоставляется по электронной почте и пейджеру, она не ограничена только для жителей г. Вашингтон.

II.2 Модель с оповещением по запросу

Наилучшим примером модели по запросу, работающей через Интернет, является японский проект I-AM-Alive (http://www.isoc.org/inet2000/cdproceedings/8l/8l_3.htm, http://www.iaa-alliance.net/en/). Деятельность в рамках проекта I-AM-Alive началась после землетрясения в г. Кобе в 1995 году с целью предоставить населению возможность определения состояния и возможного места нахождения своих близких, пострадавших в результате землетрясения. Эта система работает как центр сбора информации для служб экстренного реагирования и хранит информацию, которую эти службы получили. И наоборот, эта система работает также как центр распространения информации, в котором друзья и родственники могут узнать, не пострадали ли знакомые им люди в результате бедствия.

В системе I-AM-Alive используется сочетание входных данных, получаемых по факсу, по телефону и из веб-сети, для накопления информации, размещенной отдельными лицами или службами экстренного реагирования. Последующее распространение информации осуществляется, в основном, в виде веб-страниц, однако некоторую информацию можно получить по хорошо известным телефонным номерам, относящимся к этой системе.

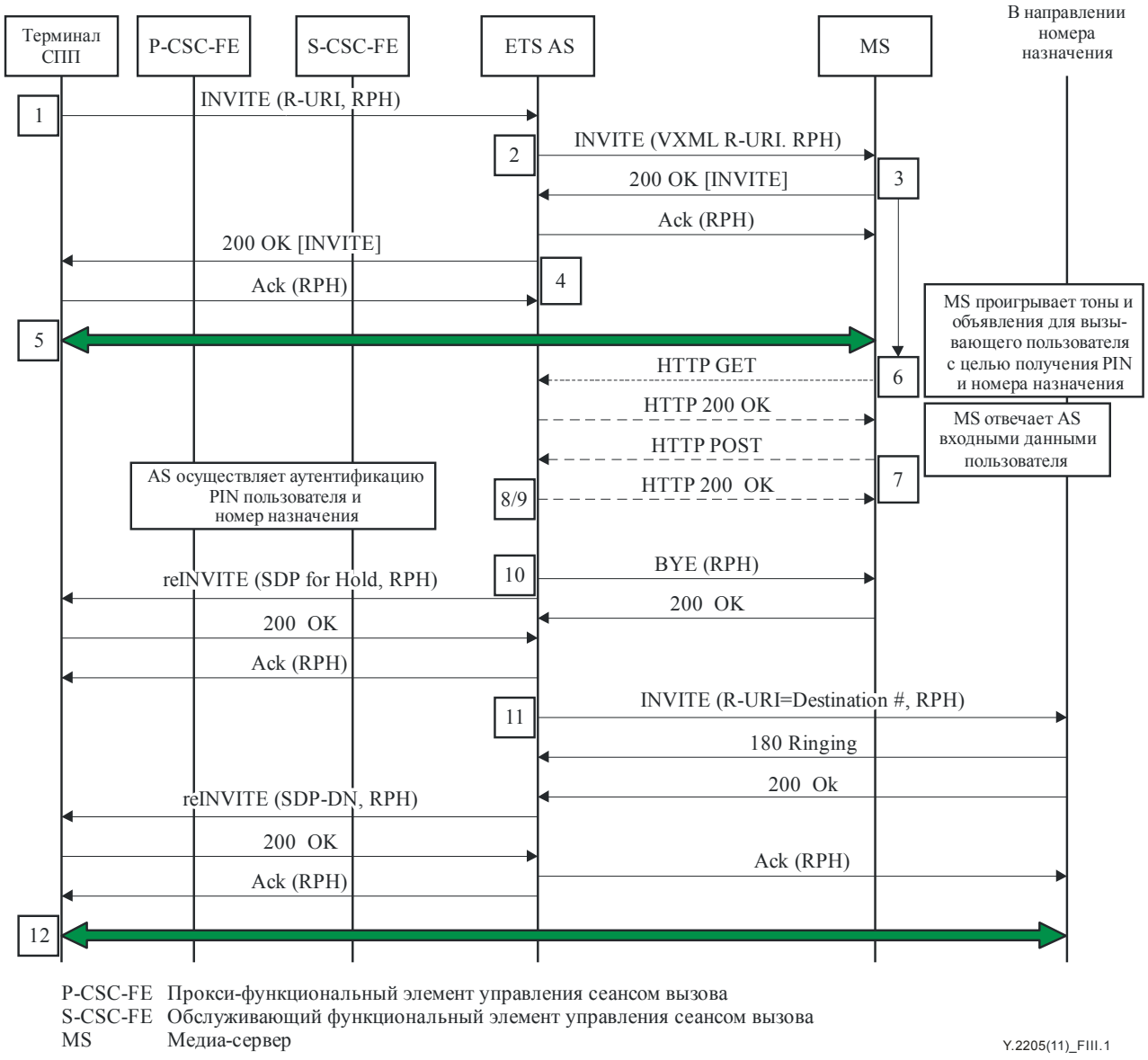
Дополнение III

Примеры потоков вызовов/сеансов ETS для СПП

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В данном Дополнении представлен пример потоков вызова или сеанса ETS из [ITU-T Q-Sup.57], применимый к СПП. Этот поток вызова иллюстрирует успешную установку вызова или сеанса ETS, в котором для аутентификации и авторизации пользователя используется PIN.

На рисунке III.1 показан метод аутентификации пользователя ETS, при котором используется вводимый пользователем PIN в IP-сети. Медиасервер (MS) является комбинацией функционального объекта управления медиаресурсом/функциональным объектом обработки медиаресурса (MRC-FE/MRP-FE). Все запросы SIP включают заголовок приоритета ресурса (RPH) [IETF RFC 4412] для указания того, что требуется приоритетный режим.



P-CSC-FE Прокси-функциональный элемент управления сеансом вызова
S-CSC-FE Обслуживающий функциональный элемент управления сеансом вызова
MS Медиа-сервер

Y.2205(11)_FIII.1

Рисунок III.1 – Установление вызова или сеанса ETS с использованием аутентификации на основании PIN

1) Вызов или сеанс направляет по маршруту на сервер приложений ETS (AS), на котором инициируется обработка аутентификации пользователя.

2) Сервер AS ETS направляет приглашающее сообщение INVITE выбранному медиасерверу (MS) вместе с SDP, связанным с отправителем. Сообщение INVITE содержит URL сценария VoiceXML, хранимого на сервере приложений ETS. В сценарии описывается, как MS должен взаимодействовать с отправителем (какие воспроизводить оповещения, как собирать цифры, как много цифр собирать, межцифровые таймеры и т. д.).

3) По получении приглашающего сообщения INVITE сервер MS:

- может направить сообщение о попытке 100 Trying серверу приложений ETS;
- осуществить выборку сценария VoiceXML непосредственно с сервера приложений ETS, используя HTTP и URL из сообщения INVITE (MS направляет сообщение HTTP GET (Получить HTTP) серверу приложений ETS, сценарий VoiceXML возвращается от сервера приложений ETS в сообщении HTTP 200 OK);
- осуществляет валидацию сценария;
- составляет и отправляет сообщение 200 OK, содержащее его собственный SDP на сервер приложений ETS.

4) AS ETS отправляет сообщение 200 OK вызывающей стороне (терминал СПП), включив в него информацию о сеансе, поученную от MS.

5) В этой точке доступно медиа-соединение между MS и вызывающей стороной.

6) По получении подтверждения ACK и сценария VXML в сообщении HTTP 200 OK сервер MS выполняет сценарий VoiceXML. Она проигрывает сигнал и собирает цифры (PIN), введенный вызывающей стороной.

7) Далее MS отправляет набранные цифры непосредственно серверу приложений ETS, используя для этого сообщение HTTP POST.

8) Получив собранные цифры, сервер приложений ETS осуществляет верификацию действительности полученных цифр (PIN).

- Если полученные цифры недействительны (количество полученных цифр или неверный номер), сервер приложений ETS определяет, что требуется дальнейшее взаимодействие с отправителем. Сервер приложений ETS возвращает сообщение HTTP 200 OK сервер MS с новым сценарием VoiceXML. Сервер приложений ETS передаст инструкцию для окончательного обслуживания обработки.
- Если полученные цифры действительны, сервер приложений ETS даст секции MS инструкцию воспроизвести оповещение для набора цифр (номер назначения).

9) Сервер приложений ETS определяет действительность введенных вызывающей стороной цифр номера назначения.

10) Сервер приложений ETS освобождает MS от вызова или сеанса посредством сообщения SIP BYE, и направляет сообщение повторного приглашения reINVITE вызывающей стороне с SDP для удержания медиаканала.

11) Сервер приложений ETS направляет приглашающее сообщение INVITE стороне назначения. Получив сообщение 200 OK (отчет), сервер приложений ETS отправляет сообщение повторного приглашения reINVITE вместе с SDP, связанным с пунктом назначения, вызывающей стороне.

12) Устанавливается медиатракт между вызывающей стороной и номером назначения с аутентификацией AS ETS на маршруте управления вызовом.

Библиография

[b-ITU-T Q-Sup.62] ITU-T Q-series Recommendations – Supplement 62 (2011), *Overview of the work of standards development organizations and other organizations on emergency telecommunications service*.

[b-UN Global Survey] Организация Объединенных Наций/Международная стратегия уменьшения опасности бедствий (2006 г.), *Заключительный отчет о Глобальном обзоре систем раннего предупреждения.* <http://www.unisdr.org/ppew/info-resources/ewc3/Global-Survey-of-Early-Warning-Systems.pdf>

[b-ATIS 1000010] ATIS-1000010.2006, *Support of Emergency Telecommunications Service (ETS) in IP Networks*.

[b-IEEE 802.11] IEEE Std 802.11-2007, *IEEE Standard for Information technology – Telecommunications and information exchange between system – Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

[b-IEEE 802.16] IEEE Std 802.16-2009, *IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems*.

[b-IEEE 802.16m] IEEE Std 802.16m-2011, *IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems, Amendment 3: Advanced Air Interface*.

[b-IEEE 802.1p] IEEE Std 802.1D-2004, *IEEE Standard for Local and metropolitan area networks; Media Access Control (MAC) Bridges*.

[b-3GPP TR 23.854] 3GPP TR 23.854 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Enhancements for Multimedia Priority Service (Release 10)*.

[b-3GPP TS 22.153] 3GPP TS 22.153 (06/2008), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia priority service (Release 8)*.

[b-3GPP TS 23.203] 3GPP TS 23.203 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture (Release 10)*.

[b-3GPP TS 23.272] 3GPP TS 23.272 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Circuit Switched (CS) Fallback in Evolved Packet System (EPS); Stage 2 (Release 10)*.

[b-3GPP TS 23.328] 3GPP TS 23.228 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 10)*.

[b-3GPP TS 23.401] 3GPP TS 23.401 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 10)*.

[b-3GPP TS 29.212] 3GPP TS 29.212, version 9 6.1 (2011-04), *Universal Mobile Telecommunications System (UMTS);* LTE; *Policy and Charging Control over Gx reference point (Release 9)*.

[b-3GPP TS 29.214] 3GPP TS 29.214 (in force), *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Rx reference point (Release 10)*.

[b-3GPP TS 29.229] 3GPP TS 29.229, version 9.3.0 (2010-10), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Cx and Dx interfaces based on the Diameter protocol; Protocol details (Release 9)*.

[b-3GPP TS 29.329] 3GPP TS 29.329 v9.4.0 (2011-01), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Sh interface based on the Diameter protocol; Protocol details (Release 9)*.

[b-3GPP2 S.R0117-0] 3GPP2 S.R0117-0-v1.0 (06/2006), *3rd Generation Partnership Project 2; Multimedia Priority Service (MMPS) for MMD-based Networks – Stage 1 Requirements*.

[b-IETF RFC 2750] IETF RFC 2750 (2000), *RSVP Extensions for Policy Control*.

[b-IETF RFC 3265] IETF RFC 3265 (2002), *Session Initiation Protocol (SIP) – Specific Event Notification*.

[b-IETF RFC 3853] IETF RFC 3853 (2004), *S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)*.

[b-IETF RFC 3936] IETF RFC 3936 (2004), *Procedures for Modifying the Resource reSerVation Protocol (RSVP)*.

[b-IETF RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework*.

[b-IETF RFC 4190] IETF RFC 4190 (2005), *Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony*.

[b-IETF RFC 4320] IETF RFC 4320 (2006), *Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction*.

[b-IETF RFC 4495] IETF RFC 4495 (2006), *A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow*.

[b-IETF RFC 4916] IETF RFC 4916 (2007), *Connected Identity in Session Initiation Protocol (SIP)*.

[b-IETF RFC 5027] IETF RFC 5027 (2007), *Security Preconditions for Session Description Protocol (SDP) Media Streams*.

[b-TM Forum GB917] TM Forum GB917 (in force), *SLA Management Handbook, Release 3.0*.

[b-WFM Stage 1-r1] WiMAX Forum – WFM-T31-122-R016v01 (2009), *Service Provider Working Group (SPWG) ETS Phase 1 Requirements for Release 1.6*.

[b-WFM Stage 1-r2] WiMAX Forum – WFM-T31-122-R020v01 (2009), *SPWG ETS Requirements, Release 2.0*.

[b-WFM Stage 2-a1] WiMAX Forum – WFM-T32-001-R016v01 (2010), *Network Architecture – Architecture Tenets, Reference Model and Reference Points, Base Specification, Release 1.6,) ETS Stage 2 Specification (Section 7.14)*.

[b-WFM Stage 3-a1] WiMAX Forum – WFM-T33-001-R016v01 (2010), *Network Architecture – Detailed Protocols and Procedures, Base Specification, Release 1.6, ETS Stage 3 Specification (Section 4.19)*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб 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 служб
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	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	**Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2012 г.