Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

G.9980

(11/2012)

СЕРИЯ G: СИСТЕМЫ И СРЕДА ПЕРЕДАЧИ, ЦИФРОВЫЕ СИСТЕМЫ И СЕТИ

Сети доступа – Сети внутри помещений

Дистанционное управление оборудованием на площадях абонента по широкополосным сетям – протокол управления оборудованием на площадях абонента через WAN

Рекомендация МСЭ-Т G.9980

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ G

СИСТЕМЫ И СРЕДА ПЕРЕДАЧИ, ЦИФРОВЫЕ СИСТЕМЫ И СЕТИ

МЕЖДУНАРОДНЫЕ ТЕЛЕФОННЫЕ СОЕДИНЕНИЯ И ЦЕПИ	G.100–G.199
ОСНОВНЫЕ ХАРАКТЕРИСТИКИ, ОБЩИЕ ДЛЯ ВСЕХ АНАЛОГОВЫХ СИСТЕМ ПЕРЕДАЧИ	G.200–G.299
ИНДИВИДУАЛЬНЫЕ ХАРАКТЕРИСТИКИ МЕЖДУНАРОДНЫХ ВЧ-СИСТЕМ ТЕЛЕФОННОЙ СВЯЗИ ПО МЕТАЛЛИЧЕСКИМ ЛИНИЯМ	G.300–G.399
ОБЩИЕ ХАРАКТЕРИСТИКИ МЕЖДУНАРОДНЫХ СИСТЕМ ТЕЛЕФОННОЙ СВЯЗИ НА ОСНОВЕ РАДИОРЕЛЕЙНЫХ ИЛИ СПУТНИКОВЫХ ЛИНИЙ И ИХ СОЕДИНЕНИЕ С МЕТАЛЛИЧЕСКИМИ ПРОВОДНЫМИ ЛИНИЯМИ	G.400–G.449
КООРДИНАЦИЯ РАДИОТЕЛЕФОНИИ И ПРОВОДНОЙ ТЕЛЕФОНИИ	G.450–G.499
ХАРАКТЕРИСТИКИ СРЕДЫ ПЕРЕДАЧИ И ОПТИЧЕСКИХ СИСТЕМ	G.600–G.699
ЦИФРОВОЕ ОКОНЕЧНОЕ ОБОРУДОВАНИЕ	G.700–G.799
ЦИФРОВЫЕ СЕТИ	G.800–G.899
ЦИФРОВЫЕ УЧАСТКИ И СИСТЕМА ЦИФРОВЫХ ЛИНИЙ	G.900–G.999
КАЧЕСТВО ОБСЛУЖИВАНИЯ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ – ОБЩИЕ И СВЯЗАННЫЕ С ПОЛЬЗОВАТЕЛЕМ АСПЕКТЫ	G.1000–G.1999
ХАРАКТЕРИСТИКИ СРЕДЫ ПЕРЕДАЧИ TRANSMISSION	G.6000–G.6999
ПЕРЕДАЧА ДАННЫХ ПО ТРАНСПОРТНЫМ СЕТЯМ – ОБЩИЕ ПОЛОЖЕНИЯ	G.7000–G.7999
АСПЕКТЫ ПЕРЕДАЧИ ПАКЕТОВ ПО ТРАНСПОРТНЫМ СЕТЯМ	G.8000–G.8999
СЕТИ ДОСТУПА	G.9000–G.9999
Сети внутри помещений	**G.9900–G.9999**

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

Рекомендация МСЭ-T G.9980

Дистанционное управление оборудованием на площадях абонента по широкополосным сетям – протокол управления оборудованием на площадях абонента через WAN

Резюме

В Рекомендации МСЭ-T G.9980 определяются требования к дистанционному управлению поставщиком услуг сетевыми устройствами, расположенными дома у потребителя. Представлен обзор и необходимые нормативные ссылки на серию технических спецификаций. Описано, как соотносятся различные технические спецификации этой серии. В разделах 3 и 4 представлен глоссарий терминов и определений, используемых в технических спецификациях.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-T G.9980	23.11.2012 г.	15-я

Ключевые слова

CWMP, TR-069.

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 извещения 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

Основой данной Рекомендации является разработанный организацией Broadband Forum протокол управления CPE WAN (CWMP), называемый TR-069.

Протокол предназначается для взаимодействия между CPE и сервером автоконфигурации (ACS). Протокол управления CPE WAN определяет механизм, объединяющий защищенную автоконфигурацию CPE, а также включает другие функции управления CPE в общую структуру.

В TR-069 приводятся общие требования протокола управления и методы, применимые к любому CPE спецификации TR-069. Другие технические отчеты организации Broadband Forum (TR) описывают управляемые объекты или модели данных для конкретных типов устройств или услуг.

Протокол может использоваться для управления различными типами CPE, включая автономные маршрутизаторы и абонентские устройства на стороне LAN. Он не зависит от конкретной среды доступа, используемой поставщиком услуг, однако зависит от IP-уровня связи, установленной устройством вначале.

Рекомендация МСЭ-Т G.9980

Дистанционное управление оборудованием на площадях абонента по широкополосным сетям – протокол управления оборудованием на площадях абонента через WAN

1 Сфера применения

В настоящей Рекомендации определяются требования к дистанционному управлению поставщиком услуг сетевыми устройствами, расположенными дома у потребителя. Представлен краткий обзор и необходимые нормативные ссылки на серию технических спецификаций (см. рисунок 1). Описано, как соотносятся различные технические спецификации этой серии.

Согласно [b-ITU-T G.988], CPE, такое как G-PON ONU, может частично управляться OMCI. В [b-ITU-T G.988]определяются варианты общего управления такими устройствами. Эти варианты и управление CPE посредством OMCI не входят в сферу применения настоящей Рекомендации.

Протокол предназначен для обеспечения гибкости модели возможности установления соединений.

- Протоколом разрешено устанавливать соединения, инициированные как CPE, так и ACS, при этом необходимость в постоянном соединении каждого CPE и ACS отсутствует.
- Функциональное взаимодействие ACS и CPE не должно зависеть от того, какая из сторон инициировала установление соединения. В частности, даже там, где инициированная ACS возможность установления соединения не поддерживается, все транзакции, инициированные ACS, должны совершиться при помощи соединения, установленного CPE.
- Протокол позволяет одному или более ACS обслуживать несколько CPE. Каждое CPE может быть связано только с одним ACS, в то время как каждый ACS может быть связан с одним или более поставщиком услуг. Однако одно физическое устройство может представлять более одного логического устройства CPE, каждое из которых может быть связано с различным ACS.
- Протокол обеспечивает CPE механизмами, позволяющими обнаружить надлежащий ACS для данного поставщика услуг.
- Протокол обеспечивает ACS механизмами, позволяющими безопасно идентифицировать CPE и соотнести его с пользователем/абонентом.

Процессы, обеспечивающие такое соотнесение, поддерживают как модели, требующие взаимодействия пользователя, так и полностью автоматические модели.

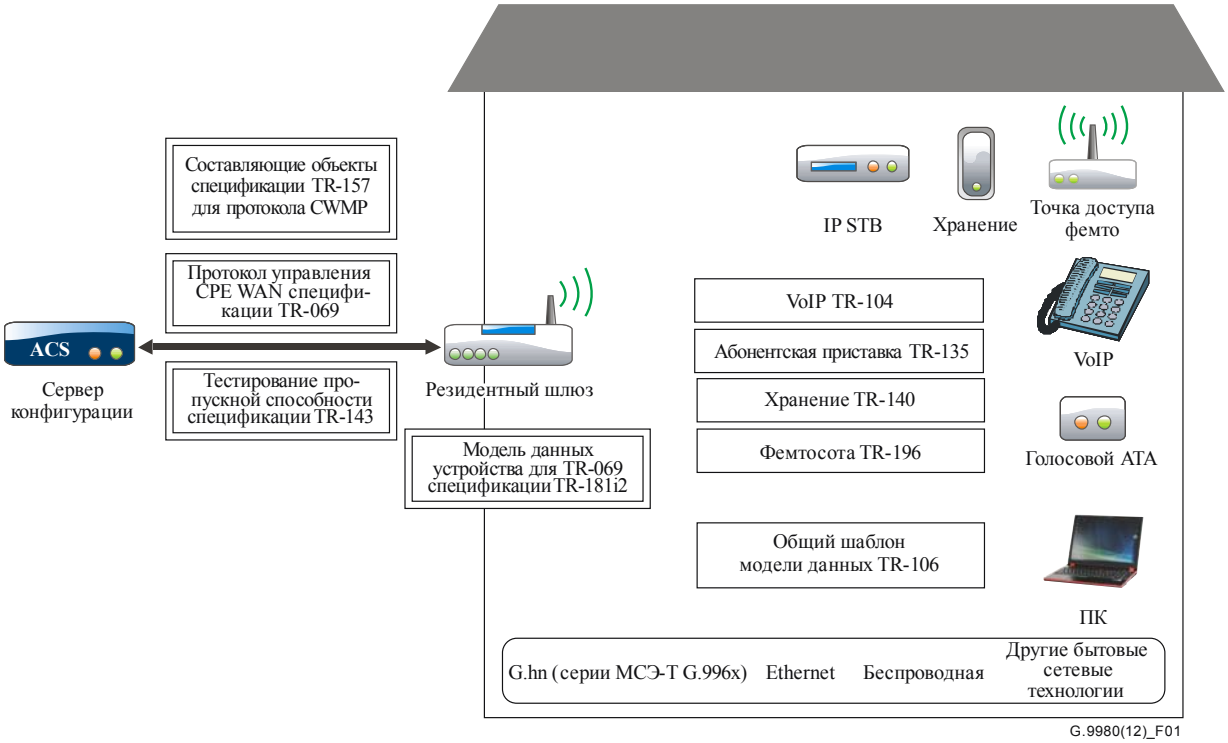
Протокол позволяет ACS контролировать различные параметры, связанные с CPE, и осуществлять их мониторинг. Механизмы, обеспечивающие доступ к данным параметрам, разработаны исходя из следующих предпосылок:

- Различные CPE могут иметь различные уровни возможностей, осуществляя различные подмножества факультативных функций. Кроме того, ACS может управлять рядом различных типов устройств, предоставляющих ряд различных услуг. В результате ACS должен обеспечивать обнаружение возможностей того или иного конкретного CPE.
- ACS должен обеспечивать контроль и мониторинг существующей на данный момент конфигурации CPE.
- Другие объекты, помимо ACS, могут иметь возможность управлять некоторыми параметрами конфигурации CPE (например, посредством автоконфигурации на стороне LAN). В результате протокол должен позволить ACS учитывать внешние изменения в конфигурации CPE. ACS также должен иметь возможность контролировать то, какие параметры конфигурации могут управляться посредством других средств, помимо ACS.
- Протокол должен позволять определять параметры, указанные производителем, и получать к ним доступ.

Протокол предназначен для максимального упрощения реализации и обеспечивает гибкость при соблюдении равновесия между сложностью и функциональностью. Протокол включает определенное количество факультативных компонентов, которые используются, только если требуется конкретная функциональность. В определенных случаях протокол включает существующие стандарты, позволяющие использовать готовые варианты реализации.

Протокол не зависит от базовой сети доступа.

Кроме того, протокол является расширяемым. Он включает механизмы поддержки будущих расширений стандарта, а также четкие механизмы для расширений, указанных производителем.



Технические отчеты для CWMP и моделей данных (см. пп. 6.1 и 6.2) показаны прямоугольниках, обведенных двойной линией.
Технические отчеты, определяющие модели данных служб (см. п. 6.2.1), показаны в прямоугольниках.

Рисунок 1 – Протокол управления CPE WAN и связанные с ним технические спецификации

В любом протоколе, описывающем дистанционную конфигурацию или дистанционное изменение программного обеспечения CPE, должна предусматриваться способность соблюдать все применимые национальные и региональные законы, нормативные акты и политические принципы. Некоторые конкретные национальные и региональные законы, нормативные акты и политические принципы могут требовать введения механизмов обеспечения ясно выраженного подтверждения клиентом своего согласия до начала дистанционного проведения каких-либо процедур в отношении CPE. Пользователи и лица, применяющие описанный CWMP, должны соблюдать все применимые национальные и региональные законы, нормативные акты и политические принципы.

Пользователи и лица, применяющие все Рекомендации МСЭ-Т, включая Рекомендацию МСЭ-Т G.9980 и лежащие в ее основе методы, должны соблюдать все применимые национальные и региональные законы, нормативные акты и политические принципы.

2 Справочные документы

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

[BBF TR-069] Broadband Forum TR-069 Amendment 2 (2007), *CPE WAN Management Protocol v1.1*. <http://www.broadband-forum.org/technical/download/TR-069_Amendment-2.pdf>

[BBF TR-104] Broadband Forum TR-104 (2005), *DSLHome Provisioning Parameters for VOIP CPE*. <http://www.broadband-forum.org/technical/download/TR-104.pdf>

[BBF TR-106] Broadband Forum TR-106 Amendment 4 (2010), *Data Model Template for TR-069-Enabled Devices*. <http://www.broadband-forum.org/technical/download/TR-106_Amendment-4.pdf>

[BBF TR-135] Broadband Forum TR-135 (2007), *Data Model for a TR-069 Enabled STB*. <http://www.broadband-forum.org/technical/download/TR-135.pdf>

[BBF TR-140] Broadband Forum TR-140 (2007), *TR-069 Data Model for Storage Service Enabled Devices*. <http://www.broadband-forum.org/technical/download/TR-140_Issue1.1.pdf>

[BBF TR-143] Broadband Forum TR-143 Corrigendum 1 (2008), *Enabling Network Throughput Performance Tests and Statistical Monitoring*. <http://www.broadband-forum.org/technical/download/TR-143_Corrigendum-1.pdf>

[BBF TR-157] Broadband Forum TR-157 Amendment 1 (2009), *Component Objects for CWMP*. <http://www.broadband-forum.org/technical/download/TR-157_Amendment-1.pdf>

[BBF TR-181 Issue 2] Broadband Forum TR-181 Issue 2 (2010), *Device Data Model for TR-069*. <http://www.broadband-forum.org/technical/download/TR-181_Issue-2.pdf>

[BBF TR-196] Broadband Forum TR-196 (2009), *Femto Access Point Service Data Model*. <http://www.broadband-forum.org/technical/download/TR-196.pdf>

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 оборудование на площадях абонента (customer premises equipment, CPE): Система оконечного пользователя, включающая элементы частной сети, которые соединяют приложения пользователя с линией доступа.

3.1.2 технический отчет (technical report, TR): Одобренная техническая спецификация организации Broadband Forum в соответствии с [b-BBF01].

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 дистанционное управление (remote management): Управление CPE поставщиком услуг по WAN.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ACS	Auto-configuration server	Сервер автоконфигурации
CPE	Customer premises equipment	Оборудование на площадях абонента
CWMP	CPE WAN management protocol	Протокол управления CPE WAN
FAP	Femto Access Point	Фемтосотовая точка доступа
FDD	Frequency-Division Duplexing	Дуплексирование с частотным разделением
IPTV	Internet protocol television	IP-телевидение
NAS	Network attached storage	Запоминающее устройство, подключенное к сети
NAT	Network address translation	Трансляция сетевых адресов
PVR	Personal video recorder	Персональный видеомагнитофон
QoE	Quality of experience	Качество квалификации
QoS	Quality of service	Качество обслуживания
RG	Residential gateway	Резидентный шлюз
RPC	Remote procedure call	Дистанционный вызов процедур
SIP	Session Initiation Protocol	Протокол инициирования сеанса
SSL/TLS	Secure Socket Layer/Transport Layer Security	Безопасность уровня защищенных разъемов/транспортного уровня
STB	Set-top box	Абонентская приставка
TR	Technical report	Технический отчет
UMTS	Universal Mobile Telecommunication System	Универсальная система подвижной электросвязи
VoIP	Voice over internet protocol	Передача голоса по протоколу Интернет
WAN	Wide area network	Территориально-распределенная сеть

5 Условные обозначения

В настоящей Рекомендации не используются какие-либо определенные системы обозначений, стили, представления и т. д.

6 Дистанционное управление CPE по широкополосным сетям

В настоящем разделе перечисляются элементы протокола управления CPE WAN (см. пункт 6.1) и модели данных для конкретных устройств (см. пункт 6.2), которые составляют нормативную часть настоящей Рекомендации.

6.1 Элементы протокола управления CPE WAN

Требования к протоколу управления CPE WAN определены в [BBF TR-069].

Признается, что политика поставщика услуг или местные регуляторные нормы могут ограничивать использование управления CPE WAN и связанных с ним спецификаций из соображений конфиденциальности и безопасности. Такие ограничения могут охватывать один или несколько из следующих пунктов:

- Взаимодействие по протоколу CWMP только посредством взаимно аутентифицированных каналов SSL/TLS.
- Ограничения типа дистанционно управляемого CPE.

- Требование индивидуального подтверждения абонентом в явной форме, которое должно быть получено до установления дистанционного управления с целью получения информации о конфигурации CPE.
- Требование для запроса индивидуального подтверждения абонентом в явной форме, которое должно быть получено до изменения конфигурации CPE.
- Прочее.

6.1.1 TR-069: Протокол управления CPE WAN (CWMP)

Протокол [BBF TR-069] предназначен для связи абонентского устройства (CPE) с сервером автоконфигурации (ACS). Протокол управления CPE WAN определяет механизм, объединяющий защищенную автоконфигурацию CPE и другие функции управления CPE в общую структуру.

С целью обеспечения технического соответствия Рекомендации и [BBF TR-069] остальная часть настоящего раздела (заключенная в рамку) структурирована в соответствии с [BBF TR-069]. Пронумерованные заголовки соответствуют номерам разделов самого [BBF TR-069].

1 Введение

Общие требования методов протокола управления CWMP могут применяться к любому CPE, поддерживающему CWMP.

В чисто функциональном отношении CWMP поддерживает множество функций управления группой CPE, включая следующие основные возможности:

- автоконфигурация и предоставление динамических услуг;
- управление изображениями программного обеспечения;
- мониторинг статуса и показателей работы;
- диагностика.

1.2 Размещение в сквозной архитектуре

Сервер ACS располагается в сети. Он управляет устройствами, расположенными на площадях абонента, посредством протокола управления CPE WAN. CWMP не зависит от конкретной среды доступа, используемой поставщиком услуг, но зависит от IP-уровня связи, установленной устройством.

1.3 Цели безопасности

Возможно масштабирование безопасности CWMP с целью соответствия различным CPE, от очень простых до сложных. Цели безопасности:

- Предотвращение вмешательства в функции управления CPE или ACS, в также в операции, проводимые между CPE и ACS.
- Обеспечение конфиденциальности операций, проводимых между CPE и ACS.
- Предоставление надлежащей аутентификации для каждого типа операций.
- Предотвращение хищения услуг.

2 Архитектура

2.1 Компоненты протокола

Согласно [BBF TR-069], приложения CWMP определяются поверх стека, в который входят соответственно методы RPC, SOAP, HTTP, SSL/TLS, TCP и IP.

2.2 Механизмы обеспечения безопасности

Механизмы, доступные CWMP, включают совместно используемые секреты SSL/TLS и HTTP.

2.3 Компоненты архитектуры

Протокол CWMP разработан на основе фундаментальной идеи дистанционной настройки и извлечения названных переменных, создания и удаления отдаленных объектов и использования малого набора предопределенных методов. На этой основе он поддерживает механизмы автообнаружения, уведомлений и передачи файлов.

Стандартные информационные модели CWMP определены в пункте 6.2 настоящей Рекомендации. Кроме того, информационная модель может расширяться способами, указываемыми производителем.

Сеансы CWMP могут инициироваться как ACS, так и CPE. Когда сеанс инициирует CPE, оно может установить связь с ACS для получения части или практически всей информации об его конфигурации, возможно даже загруженного программного обеспечения.

3 Процедуры и требования

3.1 Обнаружение ACS

В конфигурацию CPE может иметь быть встроен URL ACS по умолчанию. Кроме того, CPE может также установить идентичность ACS посредством локальной конфигурации или варианта DHCP. Также DHCP может предоставить регистрационный код, используемый устройством CPE при дальнейшей идентификации себя для ACS. ACS может самостоятельно менять URL, который будет использоваться CPE для последующей связи с другим ACS.

Если URL ACS указывает HTTPS, для установления сеанса с ACS CPE должно использовать SSL/TLS.

3.2 Установление соединения

CPE может инициировать сеанс взаимодействия с ACS, когда оно начинает работу, когда наступает конфигурированное ACS периодическое или установленное время информирования, когда ему необходимо отправить предусмотренное уведомление об изменении значения или состояния, либо для восстановления преждевременно завершенного предыдущего сеанса. CPE не поддерживает открытый сеанс при отсутствии информации для обмена с ACS.

ACS может косвенно инициировать сеанс с CPE в случае получения от CPE запроса на открытие сеанса, направленного в виде HTTP.

3.3 Использование SSL/TLS и TCP

Использование SSL/TLS для всех сеансов желательно, но не обязательно. При использовании SSL/TLS аутентификация сервера ACS должна осуществляться устройством CPE с использованием сертификата. Желательно также, чтобы ACS аутентифицировал CPE.

В остальных пунктах раздела 3 описываются подробности кодирования сообщений (SOAP), установление сеанса, его проведение и завершение, а также операции по передаче файлов. Определяются дополнительные требования к аутентификации, включая аутентификацию устройства CPE сервером ACS посредством HTTP, в том случае если аутентификация CPE еще не была осуществлена во время согласования SSL/TLS.

Приложение A – Методы RPC

Типы данных и сообщений, определенные для дистанционных вызовов процедур (RPC) CWMP, описаны в Приложении A [BBF TR-069]. Помимо синтаксиса каждого сообщения и ответа на него, в разделе описываются особые поведенческие ограничения, которые могут применяться к ACS либо к CPE.

Общая схема XML является частью этого раздела.

Приложение B – Удалено

(Удалено из этого издания TR-069.)

Приложение C – Подписанные документы

Приложение D – Управление определением идентичности во Всемирной сети

Приложение E – Формат подписанного пакета

Приложение F – Связь устройство-шлюз

CWMP может использоваться для дистанционного управления устройствами CPE, соединенными через LAN посредством шлюза. Когда ACS управляет и устройством, и шлюзом, через который соединено устройство, полезно, чтобы ACS был в состоянии определить идентичность этого конкретного шлюза.

Процедуры, описанные в настоящем приложении, позволяют ACS определить идентичность шлюза, через который соединено данное устройство. Механизм основывается на использовании DHCP и устройством, и шлюзом.

В случае образцового использования DHCP серверу ACS, устанавливающему QoS определенной услуги, возможно, потребуется обеспечить как устройство, так и шлюз, посредством которого соединено это устройство. Чтобы осуществить последнее, ACS должен будет определить идентичность этого шлюза.

Для поддержки данной функции ожидается, что и шлюз, и устройство будут управляться посредством CWMP, а также одним и тем же ACS, либо различными ACS, связанными соответствующим образом.

Приложение G – Запрос соединения посредством шлюза NAT

Трансляция сетевых адресов (NAT) в шлюзе изолирует пространство IP-адресов на стороне LAN от IP-пространства на стороне WAN. CPE за шлюзом NAT может использовать для инициации сеанса ранее определенные методы, но процедуры, определенные в настоящем приложении, необходимы для того, чтобы ACS мог запросить соединение с CPE. Шлюз NAT необязательно должен поддерживать CWMP.

6.1.2 Автоконфигурация и предоставление динамических услуг

CWMP позволяет серверу ACS обеспечивать одно CPE или несколько CPE на основе множества критериев.

Механизм обеспечения предоставляет возможность обеспечивать CPE во время начального соединения с сетью широкополосного доступа, а также возможность повторного обеспечения или повторной конфигурации в любое время. Сюда входит поддержка асинхронного повторного обеспечения CPE, инициированного ACS.

Механизмы идентификации, включенные в протокол, позволяют обеспечивать CPE либо на основе требований каждого отдельного CPE, либо на основе общих критериев, таких как производитель CPE, модель или версия программного обеспечения.

Кроме того, протокол предоставляет факультативные инструменты для управления относящимися к CPE компонентами факультативных приложений или услуг, для которых необходим дополнительный уровень безопасности, например предусматривающих платежи.

Механизм обеспечения дает возможность прямого будущего расширения, позволяющего предоставлять услуги и обеспечивать возможности, еще не включенные в настоящую версию.

6.1.3 Управление изображениями программного обеспечения

CWMP обеспечивает основу для управления загрузкой файлов изображения программного обеспечения CPE. Протокол обеспечивает механизмы идентификации версии, инициации загрузки файла (загрузки, инициированные ACS, и факультативные загрузки, инициированные CPE) и уведомления ACS об успешной загрузке файлов либо о неудаче при загрузке файлов.

6.1.4 Мониторинг статуса и показателей работы

CWMP оказывает поддержку CPE для предоставления доступа к информации, которую сервер ACS может использовать для мониторинга статистики статуса и показателей работы CPE. Кроме того, он определяет набор механизмов, позволяющих CPE активно уведомлять ACS об изменениях в своем статусе. [BBF TR-143] упрощает тестирование пропускной способности, предоставляя возможность анализа опыта абонентов в отношении скорости широкополосного доступа.

6.1.5 Диагностика

CWMP способствует предоставлению устройством CPE информации, используемой ACS для диагностики и решения вопросов, касающихся возможности установления соединения или обслуживания, а также способности выполнения определенных диагностических тестов.

6.1.6 Безопасность

CWMP рассчитан на обеспечение высокой степени безопасности. Кроме того, модель безопасности предусматривает масштабирование. Она обеспечивает базовую безопасность для менее защищенных CPE и более высокую степень безопасности CPE, способным поддерживать более продвинутые механизмы безопасности. Цели безопасности протокола управления CPE WAN:

- предотвращение манипуляций с функциями управления CPE или ACS и с операциями, проводимыми между CPE и ACS;
- обеспечение взаимной жесткой аутентификации CPE и ACS;
- обеспечение конфиденциальности операций между CPE и ACS;
- предоставление надлежащей аутентификации для каждого типа операции;
- предотвращение хищения услуг.

6.2 Модели данных

Модель данных является одним из ключевых понятий для протокола CWMP. Модель данных предоставляет объекты и параметры, в отношении которых могут действовать вызовы общего метода CMWP. Эти объекты и параметры раскрывают данные о конфигурации, диагностике или статусе для различных типов услуг и устройств. Например, модель данных для устройства VoIP наряду с другими возможностями, связанными с VoIP, раскрывает параметры, относящиеся к конфигурации

SIP. Модели данных определяют суперкомплекс функций, которыми можно управлять для конкретного устройства или конкретной услуги; устройства реализуют ту часть моделей данных, которая актуальна для их конкретных функций.

Требования к моделям данных управления CPE WAN определены в [BBF TR-106], [BBF TR-143], [BBF TR-157], [BBF TR-181, Issue 2], [BBF TR-104], [BBF TR-135], [BBF TR-140] и [BBF TR-196].

В [BBF TR-106] представлена общая информация для определения моделей данных протокола CWMP, включая требования к иерархии, правила в отношении морального износа и амортизации, типы данных и схему CWMP-DM XML, которая используется для определения всех моделей данных.

CPE, такие как резидентные шлюзы (RG), абонентские приставки (STB) и сетевые устройства хранения данных (NAS), обеспечиваются и управляются при помощи общего набора параметров, позволяющих распознать устройство из сети ACS и обеспечивающих автоснабжение и непрерывное управление.

Технические отчеты, устанавливающие такие параметры:

- [BBF TR-181, Issue 2]: Device data model for [BBF TR-069].
- [BBF TR-157]: Component objects for CWMP.
- [BBF TR-143]: Enabling network throughput performance tests and statistical monitoring.

Технические отчеты, описывающие модели данных служб:

- [BBF TR-104]: DSLHome provisioning parameters for VOIP CPE.
- [BBF TR-135]: Data model for a [BBF TR-069] enabled STB.
- [BBF TR-140]: [BBF TR-069] data model for storage service enabled devices.
- [BBF TR-196]: Femto access point service data model.

6.2.1 TR-181, Вопрос 2: Модель данных устройства для TR-069

В [BBF TR-181, Issue 2] определяется вторая версия модели данных для устройств, поддерживающих TR-069. Модель данных применяется ко всем типам устройств, поддерживающих TR-069, включая конечные устройства, шлюзы доступа в интернет и другие устройства сетевой инфраструктуры. Она представляет собой явление следующего поколения, заменяющее как [b-BBF TR-181, Issue 1] (не включенный в Рекомендацию), так и [b-BBF TR-098], amendment 2 (не включенный в Рекомендацию). На оборудовании, которое продолжают эксплуатировать, можно и далее использовать модели данных InternetGatewayDevice:1 и Device:1, которые все еще действительны.

ПРИМЕЧАНИЕ. – Переход на Device:2 был необходим для устранения некоторых фундаментальных ограничений модели данных InternetGatewayDevice:1, которая оказалась негибкой и вызывала проблемы при представлении сложных конфигураций устройств. Однако при определении этой модели данных следующего поколения основное внимание уделялось функциям InternetGatewayDevice:1 и Device:1.

Модель данных Device:2, определенная в [BBF TR-181 Issue 2], объединяет ряд объектов данных, включающих такие аспекты, как базовая информация об устройстве, конфигурация времени суток, сетевой интерфейс и конфигурация стека протоколов, управление маршрутизацией и сопряжениями, а также диагностические тесты. Кроме того, в ней определяется базовый профиль, характеризующий минимальный уровень поддержки модели данных.

Основой модели данных Device:2 является механизм засылки интерфейсов в стек. Интерфейсы сети и уровни протокола смоделированы как независимые объекты данных, которые могут засылаться в стек, один поверх другого, в любую конфигурацию, поддерживаемую устройством.

С целью обеспечения технического соответствия Рекомендации и [BBF TR-181 Issue 2], остальная часть настоящего раздела (заключенная в рамку) структурирована в соответствии с [BBF TR-181 Issue 2]. Пронумерованные заголовки соответствуют номерам разделов в [BBF TR-181 Issue 2].

4 Архитектура

4.1 Уровни интерфейса

В настоящем Техническом отчете сетевые интерфейсы и уровни протокола моделируются как независимые объекты данных, обычно именуемые объектами интерфейса (или интерфейсами). Объекты интерфейса могут засылаться в стек один поверх другого, используя эталонные значения трассы для динамического определения отношения между интерфейсами.

Объект интерфейса и стек интерфейсов – понятия, восходящие к [b-IETF RFC 2863].

В рамках модели данных Device:2 объекты интерфейса произвольно ограничены определениями, используемыми на уровне IP-сети или ниже (т. е. уровни 1–3 модели OSI). Однако объекты интерфейса, указанные производителем, МОГУТ быть определены, что выходит за рамки данной ограниченной сферы применения.

4.2 Объекты интерфейса

Объект интерфейса – это вид сетевого интерфейса или уровня протокола. Каждый вид интерфейса смоделирован в таблице модели данных Device:2, одна строка на один экземпляр интерфейса (например, IP.Interface.{i} для IP-интерфейсов).

Каждый объект интерфейса содержит базовый набор параметров и объектов, служащих шаблоном для определения объектов интерфейса в модели данных. Объекты интерфейса также могут содержать другие параметры и подобъекты, характерные для данного типа интерфейса.

4.3 Таблица InterfaceStack

Несмотря на то что стек интерфейсов можно пересечь по параметрам LowerLayers (согласно разделу 4.2.1 *Нижние уровни*), для помощи в визуализации общих отношений засылки в стек и для получения быстрого доступа к объектам в пределах стека предоставляется альтернативный механизм.

Таблица InterfaceStack является объектом модели данных Device:2, а именно *Device.InterfaceStack.{i}*. Эта таблица предназначена только для чтения, ее строки автоматически производятся устройством CPE на основе текущих отношений, сконфигурированных между объектами интерфейса (через параметр LowerLayers каждого экземпляра интерфейса). Каждая строка таблицы представляет "связь" между объектом интерфейса более высокого уровня (на который указывает его параметр HigherLayer) и объектом интерфейса более низкого уровня (на который ссылается его параметр LowerLayer). Это означает, что строки параметров HigherLayer и LowerLayer таблицы InterfaceStack всегда будут заполнены.

ПРИМЕЧАНИЕ. – Как следствие, созданные экземпляры интерфейса не будут отображаться в таблице InterfaceStack. Также вероятно, что множественные, несвязные группы засылаемых в стек объектов интерфейса будут сосуществовать в пределах таблицы (например, каждый IP-интерфейс будет являться корнем несвязной группы; неиспользованные "фрагменты", например вторичный канал DSL с конфигурируемым ATM PVC, не прикрепленным ни к чему выше, останутся, если они по-прежнему будут соединенными между собой; и наконец, частично конфигурируемые "фрагменты" могут присутствовать при создании стека интерфейсов).

5 Определения параметров

Нормативное определение модели данных Device:2 дается в нескольких документах DM Instance (см. [BBF TR-069] Приложение A). В таблице 3 перечислены версии модели данных Device:2 и DM Instances, которые были определены на момент создания документа. Кроме того, там указываются соответствующие Технические отчеты и даются ссылки на связанные файлы XML и HTML. Документ XML спецификации TR-181i2 определяет саму модель Device:2 и импортирует дополнительные компоненты из других перечисленных документов XML. Документ HTML спецификации TR-181i2 представляет собой отчет, сформированный из файлов XML, и представляет модель данных Device:2 в удобочитаемом формате.

Приложение A – Сопряжение и очередь

В настоящем приложении определяется модель очереди и сопряжения (классификация пакетов, очередь и диспетчеризация, а также сопряжение), отображение уровня 2/3 QoS по умолчанию, определения URN для таблиц app и flow (App ProtocolIdentifier, Flow Type и Flow TypeParameters).

6.2.2 TR-157: Составляющие объекты для CWMP

В [BBF TR-157] определяются составляющие объекты для использования в устройствах, управляемых CWMP, для всех корневых моделей данных. Составляющий объект определен как объект, а входящие в него параметры могут использоваться в любой применимой корневой модели данных CWMP. Объект (объекты) может (могут) находиться на верхнем уровне или на уровне соответствующего подобъекта.

Для поддержки функций, определенных в [BBF TR-157], в таблице 1 [BBF TR-157] определено расширение к модели данных Device и модели данных InternetGatewayDevice. Для модели данных Device это расширение считается частью Device:1.4 (версия 1.4 модели данных Device), которая расширяет версию 1.3 модели данных Device, определенной в TR-157, Issue 1. Для модели данных InternetGatewayDevice это расширение считается частью InternetGatewayDevice:1.6 (версия 1.6 модели данных InternetGatewayDevice), которая расширяет версию 1.5 модели данных InternetGatewayDevice, определенную в TR-157, Issue 1.

6.2.3 TR-143: Обеспечение возможности проведения тестов показателей качества и статистического мониторинга пропускной способности сети

В [BBF TR-143] определяется тестовый набор для активного мониторинга, который может использоваться поставщиками сетевых услуг для мониторинга и/или диагностирования состояния трасс их широкополосных сетей, обслуживающих группы абонентов, имеющих CPE, которое соответствует TR-069. Активный мониторинг поддерживает как диагностику, начатую сетью, так и диагностику, начатую CPE, для мониторинга и характеристики служебных трактов постоянно или по запросу. Эти общие инструменты обеспечивают платформу для подтверждения целей QoS и соглашений об уровне обслуживания.

С целью обеспечения технического соответствия требований Рекомендации и [BBF TR-143] остальная часть настоящего раздела (заключенная в рамку) структурирована в соответствии с [BBF TR-143]. Пронумерованные заголовки соответствуют номерам разделов в [BBF TR-143].

4 Активный мониторинг

Активный мониторинг – это концепция внедрения фиктивного трафика TCP или UDP в сеть, в данном случае в сеть широкополосного доступа, куда входит устройство CPE, работающее на основе TR-069, с целью оценки QoS. Пробный трафик может исходить из сети или из устройства CPE, поддерживающего [BBF TR-143].

5 Определения параметров

В разделе 5 определяются особый синтаксис и семантика параметров услуги VoIP. Параметры сгруппированы в пакеты, которые затем далее объединяются в профили для различных приложений в разделе 7.

6 Требования к уведомлению

7 Определения профилей

7.1 Обозначения

7.2 Профиль загрузки

Профиль загрузки конфигурирует CPE для выполнения тестовой загрузки и записи результатов. В качестве части профиля могут конфигурироваться поля приоритета Ethernet и DSCP.

7.3 Профиль загрузки TCP

Профиль загрузки TCP расширяет профиль загрузки для записи времени запроса и ответа TCP, если загрузка использует TCP.

7.4 Профиль закачки

Профиль закачки конфигурирует CPE для выполнения тестовой закачки и фиксирования результатов. В качестве части профиля могут конфигурироваться поля приоритета Ethernet и DSCP.

7.5 Профиль закачки TCP

Профиль закачки TCP расширяет профиль закачки для записи времени запроса и ответа TCP, если закачка использует TCP.

7.6 Профиль эхо-UDP

Профиль эхо-UDP конфигурирует CPE для осуществления тестирования эхо-UDP.

7.7 Профиль эхо-плюс-UDP

Профиль эхо-плюс-UDP расширяет профиль эхо-UDP путем добавления параметра эхо-плюс.

Дополнение A – Теория работы

A.1 Эхо-плюс-UDP

Функция эхо-плюс-UDP является расширением обычной функции эхо-ICMP. Она позволяет произвести как одностороннее, так и двустороннее измерение показателей работы пакета. Она обрабатывается согласно меткам приоритета DSCP или Ethernet, что позволяет точнее измерить показатели работы с позиций абонента.

A.2 Диагностика загрузки при использовании транспорта FTP

Этот тест представляет собой передачу посредством FTP тестового файла устройству CPE от испытательного сервера. Он фиксирует количество полученных байтов и несколько временны*х* меток, позволяющих оценить качество загрузки.

A.3 Диагностика закачки при использовании транспорта FTP

Данные тесты подобны тесту загрузки.

A.4 Диагностика загрузки при использовании транспорта HTTP

Данные тесты подобны соответствующему тесту загрузки FTP.

A.5 Диагностика закачки при использовании транспорта HTTP

Эти тесты подобны соответствующим тестам загрузки FTP.

6.2.4 TR-104: Параметры обеспечения DSLHome для CPE с VoIP

В [BBF TR-104] определяется модель данных для обеспечения устройства CPE с передачей голоса по IP (VoIP) сервером автоконфигурации (ACS), использующим механизм, определенный в [BBF TR-069].

С целью обеспечения технического соответствия требований Рекомендации и [BBF TR-104] остальная часть настоящего раздела (заключенная в рамку) структурирована в соответствии с [BBF TR-104]. Пронумерованные заголовки соответствуют номерам разделов в [BBF TR-104].

1 Введение

TR-104:

- Относится к устройствам VoIP, которые либо встроены в шлюзы доступа в интернет, либо являются независимыми устройствами.
- Относится к устройствам VoIP, поддерживающим несколько различных услуг VoIP, каждая из которых потенциально имеет несколько различных линий.
- Поддерживает использование протоколов сигнализации SIP и MGCP.
- Поддерживает различные типы CPE, работающих по протоколу VoIP, включая конечные точки VoIP, исходящие прокси-серверы SIP и двусторонние агенты пользователя SIP.

2 Архитектура

В [BBF TR-104] VoiceService определяется как контейнер, связанный с обеспечивающими объектами для CPE, работающими по VoIP. В контексте [BBF TR-106] объект VoiceService, определенный в [BBF TR-104], представляет собой служебный объект. Отдельные устройства CPE могут содержать ноль или более экземпляров объекта VoiceService. Присутствие более чем одного объекта VoiceService могло бы быть уместным, например, в случае, когда устройство CPE служит прокси-сервером управления для другого CPE, работающего по VoIP, но не поддерживающего TR-069. К примеру, шлюз доступа в интернет мог бы служить прокси-сервером управления для одного или более телефонов VoIP, не поддерживающих TR-069.

Каждый объект VoiceService содержит один или более объектов VoiceProfile. VoiceProfile соответствует одной или более телефонным линиям, имеющим одну и ту же базовую конфигурацию. Каждый объект VoiceProfile содержит один или более объектов линии, каждый из которых представляет одну отдельную телефонную линию.

Объект VoiceProfile позволяет голосовому устройству с несколькими линиями группировать в одном профиле линии, имеющие общие характеристики. Разрешая более чем один VoiceProfile, модель позволяет одному голосовому устройству с несколькими линиями иметь группы линий, конфигурируемые способом, отличным от других. Одним из возможных способов использования этой структуры может оказаться отнесение отдельных групп линий к совершенно отдельным поставщикам услуг, с отдельными серверами VoIP и требованиями конфигурации. Еще одно возможное применение – проведение различия между уровнями обслуживания у одного поставщика услуг. Например, одно устройство может обеспечить несколько потребительских линий плюс несколько бизнес линий, каждая из которых связана с отдельным VoiceProfile и отличается по характеристикам качества.

3 Модель данных VoiceService версия 1.0

В разделе 3 определяются особый синтаксис и семантика параметров услуги VoIP. Параметры сгруппированы в пакеты, которые затем далее объединяются в профили для различных приложений в разделе 4.

4 Определения профилей

4.1 Обозначения

4.2 Профиль конечной точки

Профиль конечной точки объединяет в несколько групп параметры, соответствующие той или иной конечной точке VoIP. Группа возможностей включает границы выбора кодека и скорости передачи, количество одновременных сеансов, доступные протоколы сигнализации, обнаружение и прохождение факса и модема, план нумерации, настройка тонального сигнала, сигнала вызова и размещения клавиш. Группа голосовых профилей подразделена на несколько меньших групп, относящихся к RTP, статусу линии, параметрам используемого кодека, таймерам сеанса, адресам дальнего конца и счетчикам PM.

Следующие три профиля содержат схожую информацию, но в формах, адаптированных к их отдельным протоколам сигнализации.

4.3 Профиль SIPEndpoint

Профиль конечной точки SIP расширяет профиль конечной точки определенными параметрами, необходимыми для передачи сигналов SIP, в частности включая информацию о прокси-сервере SIP, регистрации и аутентификации абонента.

4.4 Профиль MGCPEndpoint

Профиль конечной точки MGCP расширяет профиль конечной точки параметрами, необходимыми для передачи сигналов MGCP. В частности, в их число входит информация об идентичности и регистрации агента и местного пользователя.

4.5 Профиль H323Endpoint

Профиль конечной точки H323 расширяет профиль конечной точки параметрами, необходимыми для передачи сигналов МСЭ-Т H323. В частности, в их число входит информация об идентичности и регистрации контроллера шлюза и местного пользователя.

4.6 Профиль TAEndpoint

Профиль конечной точки TA предназначен для использования конечной точкой терминала. Он расширяет основной профиль конечной точки списками связанных физических портов и их идентификаторов, имеющих те же параметры.

Приложение A – Работа оборудования

Приложение A определяет различные действия VoIP по сигнализации, которые могут вызываться префиксами плана набора номеров абонента или клавишами телефонного аппарата. Примеры включают активацию или дезактивацию таких функций, как переадресация вызова, идентификация линии вызывающего абонента, избирательный вызов и т. п. К другим действиям относятся, к примеру, переключение между множественными удерживаемыми вызовами.

Приложение B – Загрузка файлов тонового сигнала и сигнала вызова

В Приложении B описываются подробности использования функции загрузки файлов [BBF TR-069] с конкретной целью загрузки файлов тонового сигнала и сигнала вызова VoIP.

6.2.5 TR-135: Модель данных для абонентской приставки на основе [BBF TR-069]

В [BBF TR-135] определяются спецификации для дистанционного управления функциональными возможностями цифрового телевидения (IPTV или радиовещание) посредством устройств STB по протоколу CWMP. Доступ к сети и контенту PVR управляется посредством служебной платформы IPTV и не входит в сферу действия ACS. ACS может производить начальную конфигурацию новой установленной STB, однако его основными функциями являются конфигурация параметров STB для устранения неисправностей и сбор статистики для мониторинга QoS/QoE. По этой причине большинство параметров, определенных в [BBF TR-135], доступны серверу ACS только для чтения.

ПРИМЕЧАНИЕ. – [BBF TR-135] определяет модель данных для описания устройства STB, а также правила, касающиеся уведомления об изменении значения параметров. Таким образом, обеспечиваются стандартные профили моделей данных, которые, как правило, будут видны во время дистанционного управления подобным устройством.

С целью обеспечения технического соответствия Рекомендации и [BBF TR-135]остальная часть настоящего раздела (заключенная в рамку) структурирована в соответствии с [BBF TR-135]. Пронумерованные заголовки соответствуют номерам разделов в [BBF TR-135].

5 Архитектура

Абонентская приставка (STB) представляет собой набор функций и возможностей, большинство из которых являются факультативными и могут существовать более чем в одном экземпляре. Наравне с базовой инфраструктурой STB к другим компонентам относятся те, чьи профили приведены в разделе 7, ниже.

6 Определения параметров

В разделе 6 определяются особый синтаксис и семантика параметров STB. Параметры сгруппированы в пакеты, которые затем далее объединяются в профили для различных приложений в разделе 7.

7 Определения профилей

7.1 Обозначения

7.2 Базовый профиль

Базовый профиль предоставляет доступную только для чтения информацию о возможностях STB, включая поддерживаемые ею стандарты и максимальное количество потоков различных типов, которые она может поддерживать одновременно. Записываемые параметры ограничены управлением звуком и выбором языка для потоков звука и субтитров.

7.3 Профиль PVR

Профиль персонального видеомагнитофона возвращает статус возможного приложения PVR. Поддержка памяти PVR осуществляется посредством ссылки на класс storageService, определенный в [BBF TR-140].

7.4 Профиль DTT

Профиль цифрового телевизионного радиовещания предоставляет параметры конфигурации для широковещательного цифрового видео, а также доступные только для чтения параметры обслуживания и PM.

7.5 Основной профиль IPTV

Профиль IPTV предоставляет параметры буферизации QoS для чтения-записи и набор доступных только для чтения параметров, которые отражают возможности STB и текущий статус в отношении характеристик IPTV.

7.6 Профиль RTCP

Профиль протокола управления в реальном времени обеспечивает простое управление конфигурацией (включение, настройка интервала) и статусный отчет.

7.7 Профиль RTP AVPF

Профиль обратной связи в реальном времени протокола RTP задает конфигурацию функции обратной связи в реальном времени протокола RTP и представляет отчет о ее текущем статусе.

7.8 Профиль домашней сети IPTV

Профиль домашней сети IPTV сообщает о статусе и возможностях интерфейсов домашней сети STB, транслируемых потоком на стороне WAN.

7.9 Профиль IGMP

Профиль IGMP позволяет конфигурировать параметры IGMP, такие как установление меток, ошибкоустойчивость и интервал предоставления отчета для VLAN, а также доступные только для чтения статистические данные по статусу и PM.

7.10 Профиль BasicPerfmon

Базовый профиль PM (perfmon) поддерживает конфигурацию параметров PM высокого уровня, например общей активации, эталоны времени и интервалов и т. п. Он предоставляет статистику по STB в целом и статистику высокого уровня для основных компонентов на различных уровнях, например для RTP, MPEG и видеодекодера.

7.11 Профиль ECP

Профиль исправления ошибок PM предоставляет статистику, связанную с возможностью исправления ошибок RTP.

7.12 Профиль VideoPerfmon

Профиль видео PM предоставляет статистику, связанную с качеством воспроизведения видео.

7.13 Профиль AudioPerfmon

Профиль аудио PM предоставляет статистику, связанную с качеством воспроизведения звука.

7.14 Профиль AudienceStats

Профиль статистики по аудитории собирает статистические данные по подсчету каналов и времени.

7.15 Профиль AnalogOutput

Профиль аналогового выхода сообщает о возможностях STB в отношении поддержки внешних устройств, таких как видеодисплеи.

7.16 Профиль DigitalOutput

Профиль цифрового выхода сообщает, используется ли защита цифрового широкополосного контента (HDCP) на выходе конкретного видеоустройства.

7.17 Профиль CA

Профиль условного доступа сообщает о существовании условного доступа, создаваемого посредством устройства для чтения смарт-карт.

7.18 Профиль DRM

Профиль цифрового управления правами предоставляет доступные только для чтения параметры по текущему статусу передаваемых медиа-потоков.

Дополнение I – Теория работы

В настоящем Дополнении описывается большое количество случаев применения и объясняется, как в них используется информационная модель STB.

6.2.6 TR-140: Модель данных [BBF TR-069] для устройств на основе услуги хранения данных

В [BBF TR-140] предусматривается управление базовой услугой по хранению информации со стороны ACS. Ниже приведен примерный список вспомогательных возможностей, которые ACS может обеспечить посредством CWMP:

- базовая конфигурация и настройка во время активации устройства (обеспечивается [BBF TR-140] и [BBF TR-181 Issue 2]);
- установки полномочий пользователя и привилегии доступа к файлам (обеспечивается [BBF TR-140] (доступ к папкам));
- восстановление статуса устройства (обеспечивается [BBF TR-140] (параметры) и [BBF TR-181 Issue 2]);
- настройка беспроводного доступа (например, безопасность протокола WEP) для устройства хранения данных с доступом Wi-Fi.
- Диагностика сети и устранение неисправностей, например возможность подключения сети к устройству интернет-шлюза и к интернету (обеспечивается [TR-181 Issue 2] (параметры соединения)).

ПРИМЕЧАНИЕ. – Не все из этих возможностей могут реализовываться в данной модели данных; некоторые возможности являются частью собственного протокола CWMP, а некоторые реализуются через другие модели данных.

4 Определения параметров

В разделе 4 определяются особый синтаксис и семантика параметров устройства хранения данных. Параметры сгруппированы в пакеты, которые далее объединяются в профили для различных приложений в разделе 6.

5 Уведомления

6 Определения профилей

6.1 Обозначения

6.2 Базовый профиль

Базовый профиль предоставляет доступную только для чтения информацию об услуге хранения данных, в том числе о ее возможностях хранения и доступа, физических устройствах, системах файлов и папках верхнего уровня. Записываемые параметры ограничены конфигурацией идентичности внешней сети услуги хранения данных.

6.3 Профиль доступа пользователей

Профиль доступа пользователей позволяет осуществлять конфигурацию сети и локальных пользователей, а также их прав доступа и полномочий входа в систему.

6.4 Профиль группового доступа

Профиль группового доступа расширяет профиль доступа пользователей для групп пользователей и позволяет определить привилегии доступа на уровне группы.

6.5 Профиль FTP-сервера

Профиль FTP-сервера задает конфигурацию возможного FTP-сервера, связанного с услугой хранения данных, в том числе его готовность обслуживать анонимных пользователей.

6.6 Профиль SFTP-сервера

Профиль SFTP-сервера дополняет профиль FTP-сервера, позволяя задавать конфигурацию возможного SFTP-сервера, связанного с услугой хранения данных.

6.7 Профиль HTTP-сервера

Профиль HTTP-сервера задает конфигурацию возможного HTTP-сервера, связанного с услугой хранения данных, в том числе его политики безопасности.

6.8 Профиль HTTPS-сервера

Профиль HTTPS-сервера расширяет профиль HTTP-сервера, включая дополнительные параметры HTTPS.

6.9 Профиль конфигурации томов

Профиль конфигурации томов расширяет основной профиль управления конфигурацией логических томов и папок верхнего уровня.

6.10 Профиль RAID

Профиль RAID задает конфигурацию массивов хранения данных и представляет отчет о текущем статусе и размере массива.

6.11 Профиль квоты папок

Профиль квоты папок позволяет осуществлять конфигурацию политики объема папок, включая порог, предупреждающий о превышении объема.

6.12 Профиль порога томов

Профиль порога томов позволяет осуществлять конфигурацию политики в отношении вместимости на уровне логических томов.

6.13 Профиль сетевого сервера

Профиль сетевого сервера задает конфигурацию протоколов доступа к сети, которые могут использоваться для удаленного доступа к услуге хранения данных.

7 Случаи применения

Основной целью услуги хранения, управляемой [BBF TR-069], является снять с подписчика ответственность за управление памятью. В то же время некоторые или все носители данных доступны извне для использования кочевым пользователем или внешними серверами, такими как сам ACS (обновление программного обеспечения) или память персонального видеомагнитофона (PVR) (см. [BBF TR-135]).

Приложение A – Теория работы

В Приложении A приводится подробная информация о работе устройств хранения данных, включая управление съемным устройством, безопасность доступа и подробную информацию о случаях применения.

Приложение B – Описания типа RAID

Приложении B является учебником по способам сочетания дисков под моникером RAID.

6.2.7 TR-196: Модель данных для услуги точки доступа femto (TR-196: Femto access point service data model)

В [BBF TR-196] описывается модель данных для точки доступа femto (FAP) для дистанционного управления с использованием CWMP. Цель [BBF TR-196] – дать оператору возможность предлагать абонентам управляемую услугу точки доступа femto. Ввиду этого большинство аспектов услуги контролируются ACS.

Сферой применения этой модели данных FAP является UMTS FDD архитектуры home nodeB (3G HNB). Вместе с тем структура и организация модели данных может быть расширена с целью охвата другого типа (других типов) устройств FAP на базе других технологий радиоинтерфейса.

С целью обеспечения технического соответствия Рекомендации и [BBF TR-196] остальная часть настоящего раздела (заключенная в рамку) структурирована в соответствии с [BBF TR-196]. Пронумерованные заголовки соответствуют номерам разделов в [BBF TR-196].

4 Определение модели данных

В разделе 4 определяются особый синтаксис и семантика параметров FAP. Параметры сгруппированы по пакетам, которые далее объединяются в профили для различных приложений в разделе 5.

5 Определения профилей

В TR-196 определяется большое количество профилей для группировки характеристик FAP. Базовый профиль указывает детали конфигурации, наличие которых предполагается в любой FAP. Дополнительные профили описывают местную политику доступа, политику безопасности, различные беспроводные протоколы, которые могут поддерживаться, а также возможности PM, аварийной сигнализации и диагностики.

В список профилей входят:

2 Базовый профиль.

3 Профиль ACL.

4 Профиль локального IP-доступа.

5 Профиль REM WCDMA FDD.

6 Профиль REM GSM.

7 Профиль GPS.

8 Профиль транспортного SCTP.

9 Профиль передачи в реальном времени.

10 Профиль туннеля IPSec.

11 Базовый профиль UMTS.

12 Профиль автоматической конфигурации UMTS.

13 Профиль автоматической конфигурации UMTS с NL intra-frequency cell.

14 Профиль автоматической конфигурации UMTS с NL inter-frequency cell.

15 Профиль автоматической конфигурации UMTS с NL inter-RAT cell.

16 Базовый профиль конфигурации соты UMTS.

17 Улучшенный профиль конфигурации соты UMTS.

18 Профиль конфигурации соты UMTS с измерением частоты.

19 Профиль конфигурации соты UMTS с внутренним измерением UE.

20 Профиль конфигурации соты UMTS с NL intra-frequency cell.

21 Профиль конфигурации соты UMTS с NL inter-frequency cell.

22 Профиль конфигурации соты UMTS с NL inter-RAT cell.

23 Профиль защиты от ошибок и неисправностей с поддержкой аварийного сигнала.

24 Профиль защиты от ошибок и неисправностей с активным аварийным сигналом.

25 Профиль защиты от ошибок и неисправностей с историей событий.

26 Профиль защиты от ошибок и неисправностей со срочной доставкой.

27 Профиль защиты от ошибок и неисправностей с доставкой по очередности.

28 Профиль контроля производительности.

Библиография

[b-ITU-T G.988] Recommendation ITU T G.988 (2010), *ONU management and control interface (OMCI) specification*.

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[b-BBF01] Broadband Forum Technical Report Approval Process. <http://www.broadband-forum.org/about/download/trapprovalprocess.pdf>

[b-BBF TR-098] Broadband Forum TR-098 Amendment 2 (2008), *Internet Gateway Device Data Model for TR-069.* <http://www.broadband-forum.org/technical/download/TR-098_Amendment-2.pdf>

[b-BBF TR-181 Issue 1] Broadband Forum TR-181 Issue 1 (2010), *Device Data Model for TR-069.* <http://www.broadband-forum.org/technical/download/TR-181_Issue-1.pdf>

[b-IETF RFC 2863] IETF RFC 2863 (2000), *The Interfaces Group MIB.*

Другие соответствующие документы:

[b-BBF TR-064] Broadband Forum TR-064 (2004), *LAN-side DSL CPE Configuration.* <http://www.broadband-forum.org/technical/download/TR-064.pdf>

[b-BBF TR-68] Broadband Forum TR-68 (2006), *Base Requirements for an ADSL Modem with Routing.* <http://www.broadband-forum.org/technical/download/TR-068_Issue-3.pdf>

[b-BBF TR-122] Broadband Forum TR-122 Amendment 1 (2006), *Base Requirements for Consumer-Oriented Analog Terminal Adapter Functionality.* <http://www.broadband-forum.org/technical/download/TR-122v1.01.pdf>

[b-BBF TR-124] Broadband Forum TR-124 (2006), *Functional Requirements for Broadband Residential Gateway Devices.* <http://www.broadband-forum.org/technical/download/TR-124.pdf>

[b-BBF TR-131] Broadband Forum TR-131 (2009), *ACS Northbound Interface Requirements.* <http://www.broadband-forum.org/technical/download/TR-131.pdf>

[b-BBF TR-133] Broadband Forum TR-133 (2005), *DSLHome TR-064 Extensions for Service Differentiation.* <http://www.broadband-forum.org/technical/download/TR-133.pdf>

[b-BBF TR-142 Issue 2] Broadband Forum TR-142 Issue 2 (2010), *Framework for TR-069 enabled PON Devices.* <http://www.broadband-forum.org/technical/download/TR-142_Issue-2.pdf>

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 протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2014 г.