

Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

J.179

(11/2005)

КАБЕЛЬНЫЕ СЕТИ И ПЕРЕДАЧА СИГНАЛОВ
ТЕЛЕВИЗИОННЫХ И ЗВУКОВЫХ ПРОГРАММ И
ДРУГИХ МУЛЬТИМЕДИЙНЫХ СИГНАЛОВ
IPCablecom

**Обеспечение мультимедийной связи в
IPCablecom**

МСЭ-Т Рекомендация J.179



Рекомендация МСЭ-Т J.179

Поддержка IP-Cablecom для мультимедийной связи

Аннотация

В настоящей Рекомендации описывается развертывание общих мультимедийных услуг при помощи предоставления технического определения нескольких интерфейсов передачи IP сигналов, которые максимально используют основные возможности управления на основе качества обслуживания (QoS) и заданных правил, присущие кабельным модемам. Мультимедийные услуги определяются как услуги на IP (например, онлайн-игры, видеоконференции, передача мультимедийных потоков и т. д.), требующие сетевых ресурсов с гарантированным QoS (в отличие от таких услуг, как просмотр веб-узлов, электронная почта, мгновенный обмен сообщениями и обмен файлами, которые обычно предоставляются с применением потоков с негарантированным обслуживанием). В то время как телефония и услуги по передаче голоса из этого определения не исключаются, набор Рекомендаций IP-Cablecom-T специально рассматривает этот тип доставки услуг и, следовательно, при необходимости следует обращаться к этим Рекомендациям.

Источник

была одобрена 29 ноября 2005 года 9-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, определенной Рекомендацией МСЭ-Т А.8

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. 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 I 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 носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это 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/>.

© ITU 2008

Все права сохранены. Никакая часть данной публикации не может быть воспроизведена с помощью каких-либо средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1	Сфера применения 1
2	Справочные документы 1
2.1	Нормативные справочные документы..... 1
2.2	Информативные справочные документы 1
3	Термины и определения 2
4	Сокращения, акронимы и условные обозначения..... 2
4.1	Сокращения и акронимы 2
4.2	Условные обозначения..... 4
5	Технический обзор..... 4
5.1	Общие сведения о качестве обслуживания (QoS) 4
5.2	Архитектура 8
6	Описание интерфейса авторизации 16
6.1	Шлюзы: Правила управления QoS..... 17
6.2	Смена состояний шлюза 23
6.3	Профиль COPS для передачи мультимедийной информации в IPCablecom 29
6.4	Форматы сообщений протокола управления шлюзом..... 31
6.5	Операции протокола контроля шлюза..... 55
7	Описание интерфейса передачи сообщений о событиях 64
7.1	Введение 64
7.2	Требования к серверу регистрации..... 66
7.3	Общие требования к элементу мультимедийной сети IPCablecom 66
7.4	Сообщения о событиях при передаче мультимедийной информации в IPCablecom 68
7.5	Атрибуты сообщений о событиях для мультимедийной сети IPCablecom..... 73
7.6	Протокол отчета RADIUS (Службы дистанционной аутентификации пользователей) 81
8	Требования безопасности..... 83
8.1	CMTS – CM QoS интерфейс (pkt-mm-1) 83
8.2	Policy Server – CMTS COPS интерфейс (Услуги с общими открытыми правилами предоставления) (pkt-mm-2) 83
8.3	Application Manager – Policy Server COPS интерфейс (Услуги с общими открытыми правилами предоставления) (pkt-mm-3) 84
8.4	Policy Server – RKS интерфейс сообщения о событии (pkt-mm-4) 84
8.5	CMTS – RKS интерфейс сообщения о событии (pkt-mm-5)..... 85
9	Соответствие профиля трафика FlowSpec (Спецификации потока) с DOCSIS 85
9.1	Соответствие FlowSpecs с типами расписаний DOCSIS 85
9.2	Преобразование FlowSpecs в параметры трафика DOCSIS..... 86
9.3	Параметры восходящих потоков данных DOCSIS 88
9.4	Параметры нисходящих потоков данных DOCSIS 91

	Стр.
10	Потоки сообщений 93
10.1	Общая последовательность сообщений 94
10.2	Подробная последовательность сообщений 96
11	Выводы для последующего изучения 115
Приложение I – Основная информация..... 116	
I.1	Введение 116
I.2	Объекты и рамки мультимедийной сети IPCablecom 117
I.3	Структура мультимедийной сети IPCablecom 119
I.4	Управляемые удаленно QoS с правилом активного опроса (Сценарий 1)..... 124
I.5	Запрошенное клиентом QoS с правилом активного опроса (Сценарий 2)..... 132
I.6	Запрашиваемое клиентом QoS с получением правила (Сценарий 3)..... 139
I.7	Сравнение сети IPCablecom-T и мультимедийной сети IPCablecom..... 141
Приложение II – Рекомендации для назначения номера версии 145	

Поддержка IP-Cablecom для мультимедийной связи

1 Сфера применения

В настоящей Рекомендации описывается развертывание общих мультимедийных услуг при помощи описания предоставления технического определения интерфейсов передачи IP сигналов, которые максимально используют присущие кабельным модемам основные возможности управления на основе QoS и заданных правил. Мультимедийные услуги определяются как услуги на базе IP (например, онлайн-игры, видеоконференции, передача мультимедийных потоков, и т. д.), требующие сетевых ресурсов с гарантированным QoS (в отличие от таких услуг, как просмотр веб-узлов, электронная почта, мгновенный обмен сообщениями и обмен файлами, которые обычно предоставляются с применением потоков с негарантированным обслуживанием). В то время как телефония и услуги по передаче голоса из этого определения не исключаются, набор Рекомендаций IP-Cablecom-Т специально рассматривает этот тип доставки услуг и, следовательно, при необходимости следует обращаться к этим Рекомендациям.

2 Справочные документы

2.1 Нормативные справочные документы

В нижеследующих рекомендациях МСЭ-Т и в других документах содержатся положения, которые, с помощью ссылки в настоящем тексте, составляют положения настоящей рекомендации. На время публикации указанные здесь издания были действительными. Все рекомендации и другие документы постоянно пересматриваются; поэтому всем пользователям данной рекомендации настоятельно рекомендуется по возможности использовать последние издания перечисленных ниже рекомендаций и других документов. Список действующих рекомендаций МСЭ-Т регулярно публикуется. Ссылка в настоящей рекомендации на какой-либо документ не придает этому отдельному документу статуса рекомендации.

- [1] Рекомендация МСЭ-Т J.112 Дополнение В (2004 г.), *Спецификации услуг передачи по кабелю: Спецификация радиочастотного интерфейса.*
- [2] IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis.*
- [3] IETF RFC 2210 (1997), *The Use of RSVP with IETF Integrated Services.*
- [4] IETF RFC 2211 (1997), *Specification of the Controlled-Load Network Element Service.*
- [5] IETF RFC 2212 (1997), *Specification of Guaranteed Quality of Service.*
- [6] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.*
- [7] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol.*
- [8] IETF RFC 2866 (2000), *RADIUS Accounting.*
- [9] Рекомендация МСЭ-Т J.163 (2005 г.), *Динамичное качество обслуживания для обеспечения услуг реального времени по сетям кабельного телевидения с использованием кабельных модемов.*
- [10] Рекомендация МСЭ-Т J.164 (2005 г.), *Требования к сообщению о событии для поддержки услуг реального времени по сетям кабельного телевидения с использованием кабельных модемов.*
- [11] Рекомендация МСЭ-Т J.170 (2005 г.), *Спецификация безопасности IP-Cablecom.*
- [12] Рекомендации МСЭ-Т J.125 (2004 г.), *Конфиденциальность канала связи для реализаций кабельного модема.*

2.2 Информативные справочные документы

- [13] IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: An Overview.*

- [14] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.
- [15] IETF RFC 2216 (1997), *Network Element Service Specification Template*.
- [16] IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.
- [17] IETF RFC 2670 (1999), *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS Compliant RF Interfaces*.
- [18] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control*.
- [19] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR)*.
- [20] IETF RFC 3175 (2001), *Aggregation of RSVP for IPv4 and IPv6 Reservations*.
- [21] CableLabs (<http://www.cablemodem.com/specifications>).
- [22] IETF RFC 2751 (2000), *Signaled Preemption Priority Policy Element*.

3 Термины и определения

В настоящей Рекомендации определяются следующие термины:

3.1 клиент типа 1: Клиент типа 1 представляет собой существующие оконечные точки "прошлых поколений" (например, компьютерные приложения, игровые консоли), которым не достает информированности о конкретных параметрах QoS или возможностей передачи сигналов. Такой клиент ничего не знает о передаче сообщений в средах CableModem, IPCable2Home или IPCablecom, и, следовательно, к нему не могут быть применены никакие связанные с этим требования. Такие Клиенты могут быть различными – от простых аналоговых устройств воспроизведения звука и изображения до сложных сетевых периферийных устройств и бытовых электронных приборов, таких как многофункциональные блоки или игровые консоли. Для запроса услуги такой Клиент связывается с Администратором приложений, и не запрашивает ресурсы QoS непосредственно из сети доступа оператора. Настоящая Рекомендация касается только клиента типа 1.

3.2 клиент типа 2: Клиент типа 2 аналогичен адаптеру мультимедийного телефонного терминала (МТА) в IPCablecom-T в том, что касается поддержки передачи сигналов QoS на основе IPCablecom. Такой клиент знает о IPCablecom Multimedia QoS, и связывается с Администратором приложений для запроса услуги и получения метки для ресурсов сети доступа оператора. Клиент затем представляет эту метку, когда запрашивает ресурсы QoS от сети доступа оператора (pkt-mm-1, pkt-mm-6). Информация для настоящей Рекомендации по клиенту типа 2 будет получена в ходе дальнейших исследований.

3.3 клиент типа 3: Клиент типа 3 запрашивает QoS, основываясь на RSVP без взаимодействия с Администратором приложений. Такой клиент знает о RSVP, основанном на стандарте IETF, и использует этот протокол для запроса ресурсов QoS сети доступа непосредственно из CMTS. Информация для настоящей Рекомендации по клиенту типа 3 будет получена в ходе дальнейших исследований.

3.4 DOCSIS: Описывает определенную технологию CableModem, разработанную Лабораторией кабельного телевидения ("CableLabs"), размещенную по адресу: <http://www.cablemodem.com/specifications/>. Международная версия определена в Дополнении В Рекомендации J.112.

3.5 IPCablecom-T: Комплект Рекомендаций MCЭ-T по IPCablecom, который поддерживает услуги телефонной связи.

4 Сокращения, акронимы и условные обозначения

4.1 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения:

AM	Application Manager (a system that interfaces to Policy Server(s) for requesting QoS-based service on behalf of an end-user or network management system)	Администратор приложений (система, которая связана с сервером(ами), обеспечивающими выполнение правил, для запроса услуги с гарантированным качеством от лица конечного пользователя или системы управления сетью)
----	---	--

BCID	Billing Correlation ID (defined in the IPcablecom Event Messaging Recommendation)		Идентификатор корреляции биллинга (определен в Рекомендации по передаче сообщений в IPcablecom)
CM	Cable Modem		Кабельный модем
CMS	Call Management Server		Сервер управления вызовами
CMTS	Cable Modem Termination System		Система завершения вызова для кабельного модема
COPS	Common Open Policy Service (defined in RFC 2748)		Услуга с общими открытыми правилами предоставления (определена в RFC 2748)
DQoS	Dynamic Quality-of-Service		Динамическое качество обслуживания
DSx (Messaging)	J.112 Annex B QoS signalling mechanism providing Dynamic Service Add, Change and Delete semantics		Механизм сигнализации, соответствующий Дополнению В к Рекомендации J.112, описывающей семантику динамического добавления, изменения и удаления услуг
FQDN	Fully Qualified Domain Name		Полное доменное имя
HFC	Hybrid Fibre/Coax		Гибридное соединение оптоволоконно / коаксиальный кабель
IETF	Internet Engineering Task Force		Рабочая группа по стандартам сети Интернет
IP	Internet Protocol		Интернет- протокол
KDC	Key Distribution Centre		Центр распределения ключей
MG	Media Gateway		Медиа шлюз
MGC	Media Gateway Controller		Контроллер медиашлюза
MTA	Multimedia Terminal Adapter		Адаптер мультимедийного терминала
NAT	Network Address Translation		Трансляция сетевых адресов
PDP	Policy Decision Point (определена в RFC 2753)		Точка принятия решения
PEP	Policy Enforcement Point (определена в RFC 2753)		Точка обязательного выполнения решения
PS	Policy Server		Сервер, обеспечивающий выполнение правил
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая сеть общего пользования
QoS	Quality of Service		Качество обслуживания
RADIUS	Remote Authentication Dial-In User Service (defined in RFC 2138 and RFC 2139)		Служба дистанционной аутентификации пользователей (определена в RFC 2138 и RFC 2139)
RAP	Resource Allocation Protocol (Working Group in the IETF – responsible for the definition and maintenance of the COPS protocol)		Протокол распределения ресурсов (Рабочая группа в IETF, ответственная за определение и поддержание протокола COPS)
RCD	Resource Control Domain		Домен управления ресурсами
RFC	Request for Comments (technical policy documents approved by the IETF which are available at http://www.ietf.org/rfc.html)		Запрос комментариев (документы по технической политике, IETF и доступные по адресу http://www.ietf.org/rfc.html)
RFI	Radio Frequency Interface (specification defining MAC and Physical layer interfaces между CMTS and CM network elements)		Радиочастотный интерфейс (спецификация, определяющая интерфейсы MAC уровня и физического уровня между сетевыми элементами CMTS и CM)
RKS	Record Keeping Server		Сервер регистрации
RSVP	Resource ReSerVation Protocol (defined in RFC 2205)		Протокол резервирования ресурсов (определен в RFC 2205)
RSVP+	IPcablecom profile and extension of RSVP (defined in the IPcablecom DQoS Recommendation)		Профиль для IPcablecom и расширение протокола RSVP (определен в Рекомендации IPcablecom DQoS)
SCD	Session Control Domain		Домен управления сеансом связи
S-MTA	Standalone MTA (a single node that contains an MTA and a non-DOCSIS MAC (e.g., Ethernet))		Отдельно стоящий MTA (отдельный узел, содержащий MTA и MAC, не соответствующий DOCSIS (например, Ethernet))

TCP	Transmission Control Protocol	Протокол управления передачей
TLV	Type-Length-Value (technique used in formatting protocol elements)	Тип-Длина-Значение (метод, используемый в элементах протокола форматирования)
UDP	User Datagram Protocol (a connectionless protocol built upon Internet Protocol (IP))	Протокол датаграмм пользователя (протокол без установления соединений, построенный на базе Интернет-протокола (IP))
UGS	Unsolicited Grant Service (Annex B/J.112 QoS scheduling type used for constant bit rate services (e.g, voice codecs))	Услуга без запроса разрешения (Тип планирования QoS, соответствующий Дополнению B/J.112 и используемый для услуг с постоянной скоростью передачи (например, голосовых коджеков))
UGS/AD	Unsolicited Grant Service with Activity Detection	Услуга без запроса разрешения с определением присутствия сигнала
VoIP	Voice over IP	Передача голоса по каналам IP
VPN	Virtual Private Network	Виртуальная частная сеть

4.2 Условные обозначения

В тексте настоящей Рекомендации слова, которые используются для определения важности определенных требований, напечатаны заглавными буквами. Это следующие слова:

"ДОЛЖЕН"	Это слово или прилагательное "ТРЕБУЕМЫЙ" означает, что этот предмет является безусловным требованием настоящей Рекомендации.
"НЕЛЬЗЯ"	Это слово означает, что этот предмет является безусловно запрещенным в настоящей Рекомендации.
"СЛЕДУЕТ"	Это слово или прилагательное "РЕКОМЕНДОВАННЫЙ" означает, что в определенных условиях могут иметься разумные причины, для того игнорировать этот объект, но, до принятия решения о выборе иного направления, необходимо полностью осознать ситуацию и взвесить последствия.
"НЕ СЛЕДУЕТ"	Эта фраза означает, что в определенных условиях могут иметься разумные причины, для того чтобы перечисленные действия были бы приемлемыми или даже полезными, но прежде, чем выполнять действия, описанные в это метке, необходимо полностью осознать ситуацию и взвесить последствия.
"МОЖЕТ"	Это слово или прилагательное "ДОПОЛНИТЕЛЬНЫЙ", означает, что этот объект действительно необязателен. Один поставщик может принять решение о включении этого объекта, например, потому что этого требует определенный сегмент рынка, или потому, что он улучшает продукт; другой поставщик может этого объекта не использовать.

5 Технический обзор

В настоящем разделе представлен справочный материал, который может оказаться полезным некоторым читателям для понимания Рекомендаций с подробным описанием протокола интерфейса, которые будут разработаны в дальнейшем. Предназначение данного раздела – это высокоуровневый обзор архитектуры мультимедийной передачи по IP и фундаментальных технологий, на которых она строится. Более подробно архитектура мультимедийной передачи описана в Приложении I.

5.1 Общие сведения о качестве обслуживания (QoS)

Как отмечается в настоящей Рекомендации, одна из главных возможностей услуги мультимедийной передачи в IP состоит в том, что она обеспечивает доступ на IP уровне к современным возможностям QoS, определенным в Дополнении B/J.112 и Рекомендациях по IP. Настоящий подраздел содержит краткое описание этих возможностей как подготовительной основы для подробного рассмотрения правил управления QoS и ресурсами, которые изложен далее.

5.1.1 Обзор QoS в соответствии с Дополнением В/J.112

В Дополнении В/J.112 Рекомендации по RFI [1] определяется набор возможностей QoS на основе фундаментальной конструкции управления ресурсами сети, известной как Поток услуг. Поток услуг определяется как "Транспортная услуга MAC уровня, которая:

- 1) обеспечивает однонаправленную транспортировку пакетов от объекта услуги верхнего уровня на RF; и
- 2) формирует трафик, обеспечивает выполнение заданных правил и определяет приоритеты его составляющих в соответствии с параметрами QoS трафика, определенными для данного потока".

В дополнение этим основным свойствам, обеспечивающим резервирование составление расписания использования совместно используемых ресурсов сети доступа для каждого отдельного потока, определяется целый ряд базовых вспомогательных конструкций, которые используются для управления этими ресурсами. Две из них таковы:

- Кодирование Потока услуги: параметры, кодируемые в формате тип-длина-значение (TLV), используемые для определения параметров QoS, связанных с потоком услуги.
- Классификатор: параметры IP, Ethernet и IEEE802.1p/q, кодируемые в формате тип-длина-значение (TLV), используемые для определения и ограничения сферы применения потока в значениях конечных точек его создания и завершения.

В то время как Дополнение В/J.112 описывает постоянные (т. е. статические, длительно существующие потоки услуги, которые формируются в процессе регистрации кабельного модема (CM)) и динамические (т. е. переходные потоки услуги, которые добавляются, изменяются и удаляются по мере необходимости) модели QoS, структура IP-Cablecom Multimedia, главным образом, сосредоточена на динамическом разнообразии, поскольку оно позволяет оптимально управлять ресурсами сети при помощи статистического мультиплексирования в соответствии с требованиями к услуге.

Управление потоком услуги выполняется при помощи передачи команд DOCSIS Динамически добавить/изменить/удалить услугу MAC-уровня (DSA/DSC/DSD), которые могут создаваться либо кабельным модемом, либо системой завершения вызова для кабельного модема (CMTS). Транзакции DSA и DSC принимают форму трехстороннего обмена, в котором после запроса (REQ) следует ответ (RSP), получение которого затем подтверждается (ACK). Сообщения DSD – это простой двусторонний обмен. В каждом ответном сообщении DSx присутствует особый атрибут, известный как Код подтверждения, он обозначает состояние транзакции (успешная или нет).

При рассмотрении возможностей, описанных в Дополнении В/J.112, важно отметить, что восходящий и нисходящий потоки услуги обслуживаются на CMTS совершенно по-разному. Это – результат того, что восходящие РЧ каналы – это конкурирующие среды передачи, совместно использующие общий канал доступа, имеющие топологическую форму взаимоотношений "от многих к одному" между несколькими кабельными модемами и одним CMTS. Наоборот, нисходящий РЧ канал ведет себя очень похоже на традиционный IP маршрутизатор, на который пакеты прибывают (либо из сети доступа, либо по магистральным каналам) выстраиваются в очередь и перенаправляются в одном или нескольких направлениях. Следовательно применяются различные механизмы QoS, в зависимости от того, является ли конкретный однонаправленный Поток услуги восходящим или нисходящим.

Восходящие потоки услуг можно определить при помощи одного из пяти типов планирования потока:

- Наилучший из возможных: стандартная стратегия управления ресурсами на основе конкуренции, в которой возможности передачи даются по схеме "первый пришел – первым обслужен", хотя и под управлением планировщика CMTS. Этот тип планирования может быть дополнен характеристиками QoS, в которых, например, к конкретному потоку услуги применяются пределы максимальной скорости.
- Опрос не в реальном времени: стратегия управления ресурсами на основе резервирования, в которой конкретный CM запрашивает фиксированный интервал для определения того, будут ли данные помещены в очередь на передачу определенного Потока услуги и, если это так, то планировщик предоставляет ему возможность передачи или разрешение для этого Потока услуги.
- Опрос в реальном времени: аналогичен типу Опрос не в реальном времени, за исключением того, что интервал запроса, как правило, очень короток (<500 мс). Типы планирования по опросу наиболее пригодны для трафика с переменной скоростью передачи, которому свойственны негибкие требования к периоду ожидания т пропускной способности.

- Без запроса разрешения: стратегия управления ресурсами на основе резервирования, в которой определенному потоку услуги выделяются слоты фиксированного размера с (приблизительно) фиксированными интервалами без дополнительных запросов или взаимодействия. Этот тип планирования наиболее пригоден для трафика с постоянной скоростью передачи и исключает большое количество данных из заголовка протокола, связанных с типами по опросу.
- Без запроса разрешения с определением присутствия сигнала: стратегия управления ресурсами на основе резервирования, которая представляет собой гибрид типов планирования с опросом и без запроса разрешения, в которой выделяются слоты фиксированного размера через (приблизительно) фиксированные интервалы при условии, что данные для передачи помещаются в очередь. Во время периодов отсутствия передачи, этот тип планирования преобразуется в тип с опросом для сохранения неиспользуемой ширины полосы.

Из-за уникальной природы и специальных характеристик каждого из этих типов планирования, с каждым из них связываются особые параметры QoS. Эти параметры подробно рассмотрены в последующем разделе.

Нисходящие потоки услуг определяются с использованием тех же параметров QoS, которые связаны с типом планирования "Наилучший из возможных" в восходящем потоке.

Вне зависимости от ориентации потока или конкретного запрошенного типа планирования, все динамические потоки услуг логически проходят через три этапа, которые кратко описаны ниже. В то время, как определенный сценарий оптимизации сигнализации позволяют выполнять так называемые "однофазные" операции, при обработке на CMTS, запрос все равно логически проходит через три этапа.

- "Разрешенный": запросы аутентифицируются и к ним применяются правила, принятые в сети, в результате формируется формат авторизации, образующий границу для последующих запросов на резервирование.
- "Принятый" (или "Зарезервированный"): формируется неактивный Поток услуги, который резервируется планировщиком, таким образом, гарантируется успешное выполнение последующих запросов на активирование; зарезервированные ресурсы – пока они остаются активными – могут использоваться для передачи трафика в режиме "Наилучший из возможных" (от того же или от других кабельных модемов).
- "Активный" (или "Исполняемый"): активизируется Поток услуги вместе с соответствующими классификаторами; теперь в потоке могут двигаться пакеты с улучшенными параметрами QoS.

ПРИМЕЧАНИЕ. – В буквальном смысле слова, DOCSIS определяет не "состояния", а, скорее, "атрибуты" потоков услуг, которые полностью замещаются при каждой транзакции динамического изменения службы (DSC). Описанные здесь состояния – это логические конструкции, используемые в концептуальной модели, описывающей процесс управления ресурсами, выполняемый на CMTS. Кроме того, Рекомендация DOCSIS RFI стандартизует термины "принятый" и "активный" при определении атрибутов Потока услуги, тогда как в IPComcast для описания состояния шлюза приняты эквивалентные термины "зарезервированный" и "исполняемый".

В то время как DOCSIS не определяет специальной процедуры авторизации, которая должна применяться к сообщениям DSx, она описывает выполнение протокола при помощи устройства, известного под названием "Блок авторизации" для схем авторизации, относящихся к конкретным услугам. Любые параметры доступа или метки авторизации, которые предоставляются при помощи Блока авторизации, до обработки запроса DSx на CMTS, перенаправляются на соответствующий модуль авторизации. В IPComcast широко используется этот механизм авторизации, так как описано ниже.

5.1.2 Обзор QoS в IPComcast-T

В то время как Дополнение В Рекомендации J.112 RFI определяет фундаментальные механизмы QoS, которые образуют ядро модели IPComcast DQoS, Рекомендация IPComcast DQoS [9] расширяет эти возможности при помощи средств управления выполнением установленных правил на основе COPS. Точно так же, как Поток услуги представляет собой основную конструкцию модели QoS в Дополнении В/J.112, Шлюз играет роль аналогичной важности в схеме IPComcast DQoS. Шлюз определяет формат авторизации использования ресурсов, состоящий из параметров QoS уровня IP, а также классификаторов, определяющих сферу применения потоков услуг, которая может быть установлена для этого Шлюза. В соответствии с описанными ниже механизмами авторизации по Дополнению В/J.112, будут удовлетворены только запросы DSx, по всем параметрам соответствующие следующему общему соотношению:

Разрешенный формат \geq Зарезервированный формат \geq Исполняемый формат

На основе этой модели управления IP-Cablecom-T определяет схему предварительной авторизации, в которой до прихода сообщений DSx, которые запрашивают формирование соответствующего Потока услуги, разрешается использование сетевых ресурсов. Следовательно, интерфейс COPS, используемый для создания и управления Шлюзами, более точно соответствует модели COPS-PR, определенной в RFC 3084 [19], чем стандартной схеме COPS, определенной в RFC 2748 [7]. Кроме того, для того чтобы создать эти Шлюзы и управлять ими, Рекомендация IP-Cablecom DQoS определяет множество клиентских объектов COPS, которые образуют элементарные функции интерфейса сигнализации управления шлюзом между CMS и CMTS.

В частности, CMS может быть логически разделен на Агент вызова, ответственный за поддержание состояния телефонного вызова, и Контроллер шлюза, который принимает запросы на авторизацию от Агента вызова (через внутренний интерфейс) и выполняет установленные правилами решения, образуя Шлюзы на CMTS. В модели IP-Cablecom Multimedia это деление формализовано при помощи двух отдельных элементов сети – Сервера, обеспечивающего выполнение правил (аналогичного Контроллеру шлюза в модели IP-Cablecom-T) и Администратора приложений (определяющего функционирование в соответствии с услугой, аналогично тому, как действует Агент вызова в IP-Cablecom-T).

В качестве иллюстрации этой модели авторизации и использования на CMTS интерфейса Контроллера шлюза, типичный однозоновый (т. е. использующий один Сервер управления вызовами (CMS)) сетевой поток вызовов IP-Cablecom-T обрабатывается следующим образом (как правило, некоторые из этих этапов выполняются параллельно):

- E-MTA_o загружает поток, распределяет его и регистрирует в CMS;
- CMS направляет на E-MTA_o запрос для сообщения о событии подключения и набранных цифрах номера;
- E-MTA_t загружает поток, распределяет его и регистрирует в CMS;
- CMS направляет на E-MTA_t запрос для сообщения о событии подключения и набранных цифрах номера;
- E-MTA_o подключает, уведомляет CMS и сообщает о набранных цифрах номера;
- CMS направляет на E-MTA_o запрос создать новое логическое соединение и вызывает SDP_o;
- CMS направляет запрос на E-MTA_t создать новое логическое соединение и вызывает SDP_t;
- CMS создает шлюз на CMTS_o и вызывает соответствующую метку GateID_o;
- CMS создает шлюз на CMTS_t и вызывает соответствующую метку GateID_t;
- CMS направляет на E-MTA_o запрос (с идентификатором шлюза (GateID_o)) зарезервировать ресурсы выполнить ответный вызов;
- E-MTA_o направляет на CMTS_o запрос DSA-REQ сформировать потоки услуг и зарезервировать ресурсы;
- CMS направляет на E-MTA_t запрос (с GateID_t) зарезервировать ресурсы и передать сигнал тревоги;
- E-MTA_t направляет на CMTS_t запрос DSA-REQ сформировать потоки услуг и зарезервировать ресурсы;
- E-MTA_t подключает и уведомляет CMS;
- CMS направляет на E-MTA_o запрос остановить обратный вызов, использовать ресурсы и установить канал передачи в данной среде;
- E-MTA_o направляет на CMTS_o запрос DSC-REQ использовать ресурсы;
- CMS направляет на E-MTA_t запрос использовать ресурсы установить канал передачи в данной среде;
- E-MTA_t направляет на CMTS_t запрос DSC-REQ использовать ресурсы;
- Обрабатывается вызов.

В отличие от модели IP-Cablecom, в которой клиентское устройство (т. е. E-MTA) инициирует резервирование ресурсов и выполнение процедур активирования, модель управления ресурсами IP-Cablecom Multimedia позволяет выполнять эти этапы от лица конечной точки через расширенный интерфейс управления шлюзом.

Этим завершается данный краткий обзор базовых основ QoS по Дополнению В/Ј.112 и по IPСablecom. Для получения более подробных сведений об этих довольно сложных темах, обратитесь к соответствующим первоисточникам [1] и [9]. В последующем разделе приводится общий обзор архитектуры IPСablecom Multimedia, включая каждый основной элемент сети и соответствующие интерфейсы. Эти данные служат подготовительным этапом для Рекомендации по техническому протоколу, которая приводится далее.

5.2 Архитектура

В Приложении I описана общая архитектура и эталонная модель для IPСablecom Multimedia. В настоящей Рекомендации используется модель, находящаяся в общей архитектуре, и добавляются нормативные требования для нахождения масштабируемого, совместимого решения, пригодного для предоставления мультимедийных услуг в IPСablecom.

5.2.1 Типы клиента

В техническом отчете по IPСablecom определено три вида типов клиента:

- Клиент типа 1, который представляет собой существующие оконечные точки "прошлых поколений" (например, компьютерные приложения, игровые консоли), которым не достаёт информированности о конкретных параметрах QoS или возможностей передачи сигналов. Такой клиент ничего не знает о передаче сообщений в средах CableModem, IPСable2Home или IPСablecom, и, следовательно, к нему не могут быть применены никакие связанные с этим требования. Клиент типа 1 связывается с Администратором приложений для запроса услуги, и не запрашивает (не может запрашивать) ресурсы QoS непосредственно из сети доступа оператора.
- Клиент типа 2 аналогичен адаптеру мультимедийного телефонного терминала (МТА) в IPСablecom-Т в том, что касается его поддержки передачи сигналов QoS на основе Рекомендации IPСablecom DQoS.
- Клиент типа 3 непосредственно запрашивает обработку QoS из сети доступа, без взаимодействия с Администратором приложений. Такой клиент знает о RSVP, основанном на стандарте IETF, и использует этот протокол для запроса ресурсов QoS сети доступа непосредственно из CMTS.

Данная версия настоящей Рекомендации касается только Клиента типа 1. Следовательно, настоящее издание данной Рекомендации описывает только сценарий 1, сценарий, когда "QoS передаются с сервера методом принудительной рассылки", описанный в Приложении I. В рамках этого сценария Администратор приложений несет ответственность за запрос ресурсов QoS от имени клиента, и Сервер, обеспечивающий выполнение правил, принудительно передает запрос на CMTS, который является устройством, действительно ответственным за формирование и управление потоком услуги, требуемым для данного приложения.

5.2.2 Мультимедийные устройства IPСablecom

Кроме клиента (который, как правило, размещается в оборудовании пользователя), для IPСablecom Multimedia требуется, чтобы несколько элементов сети располагались в кабельной сети оператора, или были бы доступными для нее, или были бы доверенными со стороны этой сети. В процессе описания этих элементов сети в тексте настоящей Рекомендации, мы позаимствовали многое из стандартной терминологии и концептуальных решений IETF. Более подробное описание общей архитектуры IPСablecom Multimedia, включая обсуждение внутренних потребностей и задач, можно найти в Приложении I.

Поскольку и COPS [7], и COPS-PR [19] используют термины "Точка обязательного выполнения стратегического решения" (PEP) и "Точка принятия стратегического решения" (PDP) в совершенно различных сценариях взаимодействия, и, поскольку IPСablecom Multimedia добавляет дополнительные нюансы к этим концепциям (в частности, в определение Сервера, обеспечивающего выполнение правил), иногда возникает путаница, если, используя только термины PEP и PDP, пытаться понять зоны ответственности различных компонентов архитектуры IPСablecom Multimedia. В попытках устранить эту путаницу, в разделах настоящей Рекомендации используются обозначения "Домен управления услугой" и "Домен управления ресурсами", для того чтобы обозначить различия в типах правил, которые определяются и выполняются.

Домен управления ресурсами (RCD) можно определить как логическую группу элементов, которые обеспечивают соединение и управление сетевыми ресурсами уровня выполнения правил на маршрутах передачи пакетов от оконечного узла и к нему. RCD состоит из блоков CMTS и Сервера,

обеспечивающего выполнение правил, чьи области ответственности включают управление ресурсами на маршрутах передачи пакета.

Домен управления услугой (SCD) определяется как логическая группа элементов, которая предоставляет пользователям приложения и контент. Администратор приложений располагается в SCD. Отметим, что может существовать один или несколько SCD, связанных с одним RCD. Наоборот, каждый RCD может взаимодействовать с одним или несколькими SCD.



Рисунок 1/J.179 – Домены управления сеансом связи и ресурсами

В архитектуре IP-Cablecom Multimedia, главной задачей Администратора приложений является поддержание состояния приложения на уровне сеанса связи и выполнение все правила Домена управления услугой (SCD) в отношении запросов клиентов на установление связи. Если запрос клиента на установление связи проходит проверку на выполнение правил Администратора приложений SCD, Администратор приложений преобразует запрос на установление связи в запрос ресурсов и передает его на Сервер, обеспечивающий выполнение правил для проверки выполнения правил Домена управления ресурсами (RCD). Если запрос ресурсов не проходит проверку на выполнение правил RCD, то Сервер, обеспечивающий выполнение правил, отклоняет запрос ресурсов, и, следовательно, Администратор приложений отклоняет запрос клиентов на установление связи. Если, однако, запрос ресурсов проходит проверку RCD на Сервере, обеспечивающем выполнение правил, то Сервер, обеспечивающий выполнение правил, перенаправляет запрос на CMTS для контроля над установлением соединения на уровне сети.

В основном, роли различных компонентов IP-Cablecom Multimedia таковы:

- Администратор приложений ответственен за состояние на прикладном уровне и уровне сеанса связи и за применение правил SCD.
- Сервер, обеспечивающий выполнение правил ответственен за применение правил RCD и за управление взаимодействием между Администраторами приложений и CMTS.
- CMTS осуществляет контроль над установлением соединения и управление ресурсами сети при помощи потоков услуг DOCSIS.

Здесь может оказаться полезным разъяснить, как мы употребляем термин "контроль над установлением соединения" и "правила авторизации". В тексте настоящей Рекомендации, контроль над установлением соединения понимается, обычно, как процесс управления ограниченным набором ресурсов уровня сети (например, ширина полосы сети доступа, мини-слоты планировщика DOCSIS или ресурсы CMTS, необходимые для работы шлюзов и таймеров, и т. д.) и выполнение запроса для этого набора. Для целей повышения качества, контроль над установлением соединения обычно выполняется непосредственно на элементе сети, управляющем маршрутом передачи пакета (например, на CMTS), хотя некоторые усложненные варианты сервера, обеспечивающего выполнение правил, могут поддерживать состояние,

связанное с ресурсами сети, таким образом дополняя и внося свой вклад в процесс контроля над установлением соединения.

Наоборот, правила авторизации используются здесь для описания высокоуровневого агрегатного использования правил (например, количество одновременно действующих разрешений для конкретного пользователя или услуги) которые образуют стратегию управления оператором кабельной сети. Правила авторизации почти всегда определяются и выполняются на сервере, обеспечивающем выполнение правил.

В оставшейся части данного раздела более подробно описывается каждый из этих архитектурных компонентов и связанные с ними интерфейсы.

5.2.2.1 Администратор приложений (AM)

Как отмечалось в предшествующем кратком обзоре, Администратор приложений – это сетевой объект, который определяет правила SCD, координирует запросы пользователя на сеансы использования приложений с доступом к ресурсам, необходимым для выполнения этих запросов, и поддерживает состояние на прикладном уровне.

AM может располагаться на кабельной сети оператора или он может располагаться за пределами данного домена и взаимодействовать с кабельной сетью оператора через определенные доверенные соединения (как правило, определяемые и реализуемые на основе Соглашения об уровне обслуживания). Аналогично, AM может находиться под непосредственным управлением оператора или им может управлять третья сторона. Любой данный Администратор приложений может связываться с одним или несколькими серверами, обеспечивающими выполнение правил, в сети оператора; точно также, один или несколько Администраторов приложений могут связываться с любым данным Сервером, обеспечивающим выполнение правил, в сети оператора (пока существует соответствующее доверенное соединение).

В наиболее вероятных сценариях развертывания службы Администратор приложений будет связываться с клиентом посредством протокола сигнализации, который в настоящей Рекомендации не рассматривается. Используя этот нестандартизованный протокол, AM аутентифицирует и авторизует запросы клиента, основываясь на правилах Домена управления услугой (SCD). Для тех запросов клиента, которые проходят эту проверку, AM определяет конкретные параметры QoS, необходимые для доставки услуги клиенту, основываясь на сведениях о запрашиваемой услуге. Затем он направляет запрос этих ресурсов на соответствующий сервер, обеспечивающий выполнение правил, который может отклонить запрос на основании правил сети или RCD, или может переслать этот запрос далее на CMTS для выполнения и контроля установления соединения.

5.2.2.2 Сервер, обеспечивающий выполнение правил (PS)

Как сказано в RFC 2753 [18], управление выполнением правил, предусмотренное в IP-Cablecom Multimedia, основано на работах группы IETF по разработке Протокола распределения ресурсов (RAP). Поскольку Сервер, обеспечивающий выполнение правил, располагается между Администратором приложений и CMTS, он одновременно играет двойную роль "посредника" для запросов на сеанс связи, инициированных Администратором приложений, "часового" для определения и выполнения правил Домена управления ресурсами.

Как сказано в [18] и предусмотрено в модели IP-Cablecom-T DQoS, Сервер, обеспечивающий выполнение правил, работает в качестве Точки принятия стратегических решений (PDP) в отношении CMTS, в том смысле, что Сервер, обеспечивающий выполнение правил, выполняет процедуры авторизации кабельного оператора и управления ресурсами. Наоборот, Сервер, обеспечивающий выполнение правил, принимает на себя роль Точки обязательного выполнения стратегического решения (PEP) в отношении Администратора приложений, поскольку он является посредником при передаче сообщений управления шлюзом от элемента CMTS и к нему.

Для проверки сценария взаимодействия Администратор приложений создает запрос о выполнении правил и передает его на Сервер, обеспечивающий выполнение правил. Сервер, обеспечивающий выполнение правил, действует как "часовой" для этих запросов, и применяет набор правил, которые были заранее определены оператором кабельной сети. После выполнения проверки, Сервер, обеспечивающий выполнение правил, действует как "посредник" в отношении Администратора приложений и CMTS, ретранслируя запрос о выполнении правил и возвращая любой связанный с ним ответ. Каждая транзакция в рамках запроса о выполнении правил должна выполняться по отдельности.

Решения о выполнении правил могут основываться на множестве факторов, например:

- параметры, связанные с запросом, и статус доступных ресурсов;
- идентификатор конкретного клиента и связанная с ним информация о профиле;
- параметры приложения;
- вопросы безопасности;
- время суток.

Основные функции Сервера, обеспечивающего выполнение правил, включают в себя:

- механизм запроса решения о выполнении правил, запускаемый Администраторами приложений;
- механизм проверки правильности запроса решения о выполнении правил, реализующий выполнение установленных правил;
- механизм доставки решения о выполнении правил, используемый для формирования на CMTS решений о выполнении правил;
- механизм, позволяющий ретрансляцию сообщений управления QoS на CMTS от лица Администратора приложений;
- интерфейс регистрации событий с Сервером регистрации, который используется для сохранения запросов о выполнении правил, что, в свою очередь, может коррелироваться с регистрацией использования ресурсов сети.

Поскольку Сервер, обеспечивающий выполнение правил, действует как "посредник" между элементами АМ и CMTS (с дополнительными интерфейсами с клиентом и сервером), некоторые операторы кабельных сетей могут выбрать вариант, при котором формируется несколько уровней Серверов, обеспечивающих выполнение правил, и делегировать этим серверам принятие определенных решений о выполнении правил, для того чтобы выполнить требования, связанные с масштабируемостью и отказоустойчивостью.

5.2.2.2.1 Сервер, обеспечивающий выполнение правил – сохраняющий и не сохраняющий информацию о состоянии

Существует два основных класса Серверов, обеспечивающих выполнение правил; сохраняющий информацию о состоянии (Stateful) и не сохраняющий информацию о состоянии (Stateless). Название "Сервер, обеспечивающий выполнение правил, не сохраняющий информацию о состоянии" несколько некорректно, поскольку он сохраняет информацию о состоянии, достаточную, для того чтобы направить запросы Администратора приложений на правильный CMTS и поддерживать состояние сеанса связи COPS, тогда как действительно не сохраняющий информацию о состоянии Сервер, обеспечивающий выполнение правил, не поддерживает состояния ни для одного сеанса связи. Сервера, обеспечивающие выполнение правил и сохраняющие информацию о состоянии, встречаются в нескольких вариантах: некоторые участвуют в контроле над установлением соединения и, следовательно, управляют атрибутами QoS активных сеансов связи, некоторые оставляют QoS и контроль над установлением соединения на усмотрение CMTS, но контролируют выполнение некоторых критичных по времени или критичных по объему запросов на услуги от Администратора приложений, и некоторые Сервера, обеспечивающие выполнение правил, располагаются где-то посередине между этими двумя крайними вариантами.

Причина наличия разных типов Серверов, обеспечивающих выполнение правил, заключается в том, что существует множество различных условий, в которых работает оператор. Например, некоторые операторы могут пожелать реализовать IP-Cablecom Multimedia на тех же CMTS, которые они используют для передачи сигналов телефонии по IP-Cablecom, и они могут пожелать использовать единственный CMS/Сервер, обеспечивающий выполнение правил, который видит сетевые ресурсы в глобальном масштабе. С другой стороны, некоторые операторы могут предпочесть работу в среде "только IP-Cablecom Multimedia", или они могут применять более простые механизмы, реализованные на CMTS, для разделения ресурсов, используемых для IP-Cablecom Multimedia и для телефонии. Эти упрощенные конфигурации имеют более скромные требования к состоянию, которое поддерживает Сервер, обеспечивающий выполнение правил.

Требования к состоянию Сервера, обеспечивающего выполнение правил, могут также определяться уровнем доверия между Сервером, обеспечивающим выполнение правил, и Администратором приложений; Сохраняющий информацию о состоянии Сервер, обеспечивающий выполнение правил, может проще обеспечивать выполнение Администратором приложений правил управления сеансом связи, чем Не сохраняющий информацию о состоянии Сервер, обеспечивающий выполнение правил.

Таким образом, Сохраняющий информацию о состоянии Сервер, обеспечивающий выполнение правил, может быть более приемлемым для операторов, поддерживающих работу Администраторов приложений, как третьей стороны. Другие операторы могут надеяться на экономические стимулы в их доверенных отношениях с Администраторами приложений, или они могут сами управлять работой Администраторов приложений. В таких случаях более приемлемым будет Не сохраняющий информацию о состоянии Сервер, обеспечивающий выполнение правил.

Поскольку невозможно классифицировать все различные компоненты сеанса связи и состояния QoS сети, которые поддерживает Сервер, обеспечивающий выполнение правил, разработан протокол, не зависящий от этих сложностей. Сохраняющий информацию о состоянии Сервер, обеспечивающий выполнение правил, тщательно собирает информацию о сеансе связи IP-Cablecom Multimedia из запросов Администратора приложений, в отношении которого он является посредником; любая другая информация, которая ему необходима, собирается при помощи механизмов, работа которых в настоящей Рекомендации не рассматривается. CMTS и Администратор приложений не делают различия между типами Серверов, обеспечивающих выполнение правил, к которым они присоединены, и протокол разработан таким образом, что тип Сервера, обеспечивающего выполнение правил, является прозрачным для конечной точки. Тип Сервера, обеспечивающего выполнение правил, имеет значение только для оператора.

Поскольку некоторые типы Серверов, обеспечивающих выполнение правил, пытаются содействовать контролю над установлением соединения и могут знать гораздо больше о сети и ее ресурсах, при проектировании сети, которая содержит несколько таких Серверов, обеспечивающих выполнение правил, могут проявляться дополнительные проблемы синхронизации состояний. Оператор должен нести ответственность за то, чтобы действия этих Серверов обеспечивающих выполнение правил, не были бы запрещены сетью, в которой имеются другие автономные Сервера, обеспечивающие выполнение правил.

5.2.2.2.2 Модификация запросов и ответов Серверами, обеспечивающими выполнение правил

Хотя Сервер, обеспечивающий выполнение правил, номинально является частью Домена управления ресурсами, он может быть посредником между Доменами управления услугой и управления ресурсами, в дополнение к его обычной роли выполнения процедур авторизации оператора и управления ресурсами. В любой из этих возможностей он может изменять приходящие запросы перед их ретрансляцией на CMTS.

Действуя в качестве посредника между SCD и RCD, Сервер, обеспечивающий выполнение правил, может преобразовывать поля из форматов и масштабов, используемых в SCD, в форматы и масштабы, используемые в RCD. Например, Сервер, обеспечивающий выполнение правил, может изменить "приоритет" запроса, пришедшего от Администратора приложений (это особенно важно сделать для АМ, расположенного за пределами сети MSO) так, чтобы это поле приоритетов использовало в RCD оператора соответствующий масштаб. Действуя в качестве посредника, Сервер, обеспечивающий выполнение правил, может использовать двустороннее преобразование – другими словами, он должен преобразовывать запроса, поступающие от АМ на CMTS и "обратно преобразовывать" ответы, поступающие от CMTS на АМ. Эта возможность может обеспечиваться Сохраняющими информацию о состоянии Серверами, обеспечивающими выполнение правил, при помощи запоминания исходного запроса, и она может обеспечиваться Не сохраняющими информацию о состоянии Серверами, обеспечивающими выполнение правил, если функция преобразования обратима.

Модификация определенных объектов, особенно объектов Классификатор и Профиль трафика, может вызвать эксплуатационные проблемы в исходном АМ. Таким образом, эти объекты НЕЛЬЗЯ модифицировать на Сервере, обеспечивающем выполнение правил. Все остальные объекты, кроме этих исключений, могут быть рассмотрены на предмет выполнения правил и модифицированы по усмотрению PS, на основе существующих правил.

5.2.2.3 Система завершения вызова для кабельного модема (CMTS)

При описании роли элемента сети CMTS, важно учитывать связь между функциями кабельного модема, IP-Cablecom-T и IP-Cablecom Multimedia. Хотя каждый из них соответствует Рекомендациям, касающимся определенного набора функциональных требований, каждый также определяется таким образом, чтобы соответствующее исполнение могло быть выполнено по модульному принципу. Поверх основного CMTS, соответствующего Дополнению В/Ј.112, может быть помещено Управление шлюзом либо IP-Cablecom-T, либо IP-Cablecom Multimedia, при этом имеется возможность добавления дополнительных, вспомогательных функций по требованию бизнес-модели. Кроме того, следует подчеркнуть, что очень важным преимуществом архитектуры IP-Cablecom является то, что варианты для телефонии и для мультимедийной передачи потоков имеют много общего по архитектуре, что приводит к возможности повторного использования лежащих в их основе моделей управления шлюзами.

Система завершения вызова для кабельного модема в IP-Cablecom Multimedia – это обобщенная версия CM-TS для IP-Cablecom-T, которая определена для доставки телефонных услуг в сетях IP-Cablecom-T. CM-TS несет ответственность за выполнение запросов на QoS, которые принимаются от одного или нескольких Серверов, обеспечивающих выполнение правил. Он выполняет эту функцию, устанавливая шлюзы, которые аналогичны шлюзам, определенным в [9]; Шлюзы позволяют кабельному модему пользователя запросить у CM-TS ресурсы сети путем создания динамических потоков DOCSIS с гарантированными уровнями QoS. CM-TS передает Сообщения о событиях, в которых подробно сообщает на Сервер регистрации о реальном использовании ресурсов QoS.

5.2.2.4 Сервер регистрации (RKS)

Сервер регистрации в IP-Cablecom Multimedia играет роль, аналогичную роли RKS в IP-Cablecom-T [10]. Он принимает от Сервера, обеспечивающего выполнение правил, Сообщения о событиях, касающиеся принятия решений о выполнении правил, и от CM-TS -Сообщения о событиях, касающиеся использования ресурсов QoS.

В архитектуре IP-Cablecom Multimedia Сервер регистрации не принимает сообщений непосредственно от Администратора приложений. Однако Администратор приложений может ввести скрытые данные в сообщении, которые он передает на Сервер, обеспечивающий выполнение правил, и эти данные затем могут быть включены в Сообщения о событиях, которые впоследствии будут переданы на RKS.

5.2.3 Интерфейсы IP-Cablecom Multimedia

Передача мультимедийных потоков в IP-Cablecom Multimedia основана на комплекте Рекомендаций IP-Cablecom-T. В том случае, когда интерфейс IP-Cablecom Multimedia служит средой передачи в IP-Cablecom-T, в IP-Cablecom Multimedia используется тот же самый протокол, или расширение того же самого протокола.

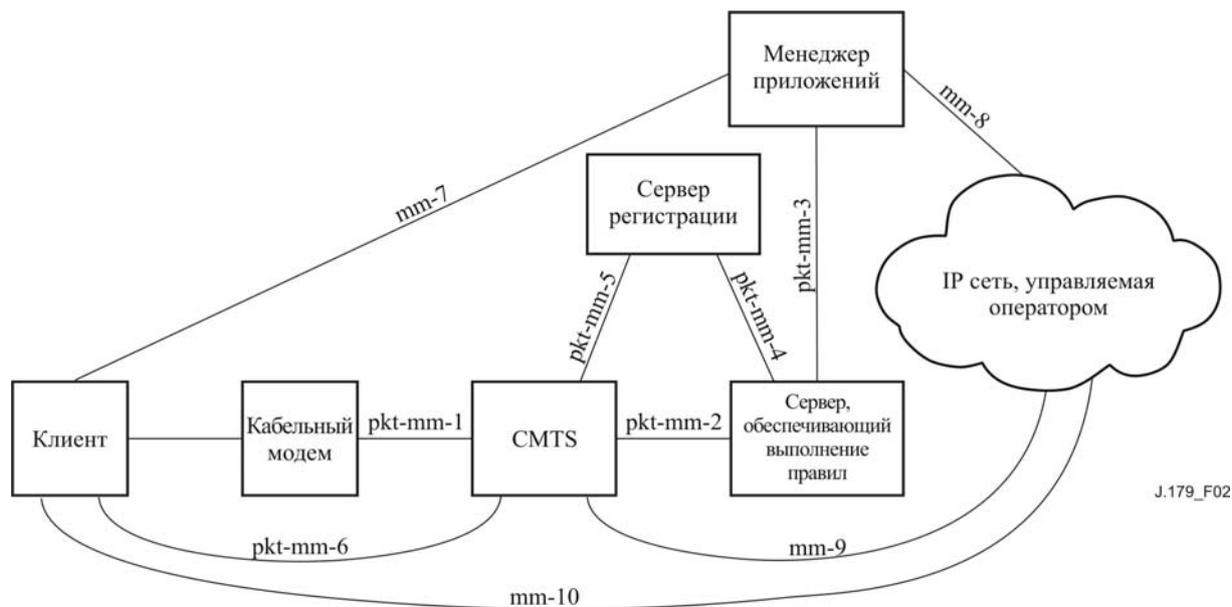


Рисунок 2/J.179 – Архитектура IP-Cablecom Multimedia

Таблица 1/J.179 – Интерфейсы IP Cablecom Multimedia

Интерфейс	Описание	Примечания
pkt-mm-1	CMTS – CM	Кабельный модем (CM) может запросить QoS от CMTS при помощи процедуры сигнализации по Дополнению В/J.112 DSx. В качестве альтернативы, CMTS может приказать CM создать, разрушить или изменить Поток услуги DOCSIS, для того чтобы удовлетворить запрос QoS, опять же при помощи процедуры сигнализации DSx.
pkt-mm-2	PS – CMTS	Этот интерфейс является основным в рамках управления выполнением правил. Он контролирует решения о выполнении правил, которые могут быть: а) навязываемыми CMT Сервером, обеспечивающим выполнение правил, (PS); или б) запрошенными CMTS от PS. Этот интерфейс также позволяет направлять запросы QoS от лица клиента. В ряде сценариев, этот интерфейс может также использоваться для информации PS о том, когда ресурсы QoS становятся не активными
pkt-mm-3	AM – PS	Администратор приложений (AM) может потребовать, чтобы PS принял решение о выполнении правил на CMTS от лица клиента. Этот интерфейс может также использоваться для информации AM об изменениях в состоянии ресурсов QoS.
pkt-mm-4	PS – RKS	PS передает сообщения о событиях на Сервер регистрации (RKS) для отслеживания решений о выполнении правил, связанных с QoS.
pkt-mm-5	CMTS – RKS	CMTS передает на RKS сообщения о событиях для отслеживания запросов QoS и об использовании ресурсов QoS (например, о добавлениях потоков услуг, изменениях, удалениях, и их размерах).
pkt-mm-6	Client – CMTS	Клиент может использовать этот интерфейс для непосредственного запроса в сети и управления ресурсами QoS . Если это разрешено, то запрошенные ресурсы предоставляет ему CMTS.
mm-7	Client – AM	Этот интерфейс может использоваться клиентом для взаимодействия с AM для опосредованного запроса и управления ресурсами QoS . Этот интерфейс в данной версии настоящей Рекомендации не рассматривается.
mm-8	AM – Peer	AM может использовать этот интерфейс для взаимодействия с каким-либо другим объектом, который является частью рассматриваемого приложения. Этот интерфейс в данной версии настоящей Рекомендации не рассматривается.
mm-9	CMTS – оператор кабельной сети – Управляемая IP сеть	Этот интерфейс на CMTS может использоваться для передачи сквозных запросов на QoS за пределами сети доступа. Этот интерфейс в данной версии настоящей Рекомендации не рассматривается.
mm-10	Client – Peer	Клиент может использовать этот интерфейс для взаимодействия с каким-либо другим объектом, который является частью рассматриваемого приложения. Этот интерфейс в данной версии настоящей Рекомендации не рассматривается.

5.2.3.1 Интерфейс между клиентом и Администратором приложений (mm-7)

Интерфейс между клиентом и Администратором приложений в настоящей Рекомендации не рассматривается. Как правило, Администратор приложений, при помощи каких-либо средств, не рассматриваемых в настоящей Рекомендации, аутентифицирует клиента и убедится, что клиенту разрешено пользоваться мультимедийными услугами. Например, клиент может войти на веб-страницу и запросить услугу, введя имя пользователя и пароль. Хотя это выполнено, Администратор приложений должен иметь возможность неоднозначно идентифицировать кабельный(е) модем(ы), на который(е) эта услуга должна быть доставлена, поскольку эта информация должны быть доступной для оператора сети до того, как может быть выполнена доставка QoS.

5.2.3.2 Интерфейс между Администратором приложений и Сервером, обеспечивающим выполнение правил (pkt-mm-3)

Этот интерфейс соответствует интерфейсу IPCablecom-T между Агентом вызова и Контроллером шлюза. В IPCablecom-T – это скрытый, непроверяемый интерфейс, и поэтому для этого интерфейса нет заранее установленных требований к протоколу.

В IPCablecom Multimedia требуется, чтобы на этом интерфейсе использовался протокол COPS [7]. С целью упрощения архитектуры и для того чтобы дать возможность иметь элементы нескольких уровней Сервера, обеспечивающего выполнение правил, между Администратором приложений и CMTS, этот интерфейс максимально копирует интерфейс между Сервером, обеспечивающим выполнение правил, и CMTS. Хотя Администратор приложений является одним из элементов, который разрешает запрос ресурсов от Сервера, обеспечивающего выполнение правил, он, в действительности, формирует этот запрос в Сообщении о принятии решения протокола COPS, а не в Сообщении о запросе протокола COPS. Это дает возможность интерфейсу между Администратором приложений и Сервером, обеспечивающим выполнение правил, выглядеть идентичным интерфейсу между Сервером, обеспечивающим выполнение правил, и CMTS. Администратор приложений – связан с Сервером, обеспечивающим выполнение правил, через PDP, и Сервер, обеспечивающий выполнение правил, связан с Администратором приложений, через PEP.

Когда Администратор приложений соглашается предоставить клиенту услугу, он передает Решение COPS, которое содержит (как минимум) следующую информацию в форме объектов протокола COPS:

- Идентификатор Администратора приложений, делающего запрос;
- Идентификатор клиента(ов), кому должна быть предоставлена услуга;
- Определитель(и) потока(ов) RSVP, определяющий(е) формат(ы) трафика для сеанса связи.

В ответ от Сервера, обеспечивающего выполнение правил, этот сервер включает метку авторизации, ID шлюза, который был им получен от CMTS.

5.2.3.3 Интерфейс между и Сервером, обеспечивающим выполнение правил и CMTS (pkt-mm-2)

Этот интерфейс почти полностью идентичен эквивалентному интерфейсу (между CMTS и Контроллером шлюза) в IPCablecom-T. Как и в IPCablecom-T, COPS используется для передачи информации о выполнении правил между Сервером, обеспечивающим выполнение правил, и CMTS. CMTS действует как PEP протокола COPS, а Сервер, обеспечивающий выполнение правил, действует как PDP протокола COPS. В соответствии с моделью IPCablecom-T, Сервер, обеспечивающий выполнение правил, инициирует установление соединения для сеанса мультимедиа связи путем передачи DQoS сообщения Gate-Set (Создать шлюз) (которое является незапрашиваемым сообщением DECISION протокола COPS) на CMTS.

Это сообщение содержит (как минимум):

- ID Администратора приложений;
- ID пользователя;
- GateSpec – спецификация шлюза;
- FlowSpec(s) – спецификация(и) потока;
- Классификатор.

CMTS отвечает, как и в DQoS, передавая либо сообщение Gate-Set-Ack (Подтверждение создания шлюза) либо сообщение Gate-Set-Err (Ошибка создания шлюза). Оба этих сообщения являются сообщениями REPORT протокола COPS.

Если CMTS отвечает положительно (т.е. сообщением Gate-Set-Ack), он включает в ответ идентификатор шлюза (GateID). Как и в IPCablecom-T, GateID действует как метка авторизации. В отличие от IPCablecom-T, эта метка, в конце концов, не передается клиенту (поскольку окончательным точкам Клиента типа 1 ничего не известно об IPCablecom); вместо этого, она сохраняется Сервером, обеспечивающим выполнение правил, (если это сервер – сохраняющий информацию о состоянии) и Администратором приложений, позволяя им, таким образом, отдавать команды, связанные с данным сеансом связи CMTS, либо непосредственно для Сервера, обеспечивающего выполнение правил, либо – для Администратора приложений – опосредовано через Сервер, обеспечивающий выполнение правил.

5.2.3.4 Интерфейс между и Сервером регистрации и Сервером, обеспечивающим выполнение правил (pkt-mm-4) и интерфейс между Сервером регистрации и CMTS (pkt-mm-5)

Интерфейсы с Сервером регистрации от Сервера, обеспечивающего выполнение правил, и от CMTS идентичны эквивалентным интерфейсам (от CMS и CMTS, соответственно) в IPCablecom-T (см. [10]). Эти интерфейсы используются для передачи в IPCablecom Сообщений о событиях, которые используют

форматы RADIUS. В IP-Cablecom Multimedia Сообщения о событиях содержат подробную информацию, относящуюся к доставляемой услуге, включая точное время создания и удаления этих потоков услуги и (дополнительно объема трафика, переданного в этом потоке услуги за время его существования).

5.2.4 Информация о состоянии

В настоящем разделе мы приводим обзор состояний в системе IP-Cablecom Multimedia. В дополнение к сохраняемой подробной информации о состоянии, устройства передают на Сервер регистрации информацию о смене состояний для таких целей как биллинг, обнаружение и мошенничества, восстановление сеанса связи и т. д.

5.2.4.1 Состояние приложения

Администратор приложений всегда несет ответственность за сохранение подробных сведений о состоянии приложения сеанса связи. Как он это делает, в настоящей Рекомендации подробно не рассматривается, но важно знать, что никакие устройства, отличные от Администратора приложений, не содержат и не должны содержать никаких сведений о состоянии приложения.

Администратор приложений может, однако, сообщить о состоянии сеанса связи путем передачи этой информации через Сервер, обеспечивающий выполнение правил, на Сервер регистрации. Кроме того, некоторая информация о состоянии (например, тот факт, что запрашиваются ресурсы) автоматически передается с Сервера, обеспечивающего выполнение правил, на Сервер регистрации.

5.2.4.2 Состояние ресурсов QoS

Обычно CMTS имеет подробную информацию о состоянии потоков, которыми он управляет. Сервер, обеспечивающий выполнение правил, (если это – сохраняющий информацию о состоянии Сервер, обеспечивающий выполнение правил) может также сохранять данные о состоянии ресурсов QoS на одном CMTS; он может также сопоставлять информацию о состоянии на нескольких CMTS, так что ему (и только ему) известно состояние QoS всей системы. Это может быть важно, например, если оператор установил правила, в соответствии с которыми определенное приложение не должно использовать более чем некоторый процент всех ресурсов системы. В сети, где имеются только не сохраняющие информацию о состоянии Сервера, обеспечивающие выполнение правил, CMTS являются единственными устройствами, которые сохраняют информацию о состоянии QoS. Поскольку не сохраняющие информацию о состоянии Сервера, обеспечивающие выполнение правил, не сохраняют идентификаторы шлюзов (GateID), они не могут даже попросить CMTS получить информацию о конкретном сеансе мультимедиа связи.

Всегда, когда объект Ресурсы QoS переходит из одного состояния в другое, и всегда, когда удаляется объект Ресурсы QoS, от CMTS на Сервер регистрации передается соответствующее Сообщение о событии.

6 Описание интерфейса авторизации

В настоящем разделе описывается интерфейс между Администратором приложений и Сервером, обеспечивающим выполнение правил, и интерфейс между Сервером(ами), обеспечивающим(и) выполнение правил, и CMTS.

Интерфейс между Администратором приложений и Сервером, обеспечивающим выполнение правил, с точки зрения передачи симметричен интерфейсу между Сервером, обеспечивающим выполнение правил, и CMTS. Интерфейсы используются для передачи на CMTS информации авторизации, резервирования и активизации, для предоставления информации о состоянии от CMTS на Сервер, обеспечивающий выполнение правил, и от Сервера, обеспечивающего выполнение правил, на Администратор приложений.

Администратор приложений является точкой принятия стратегического решения (PDP) для Домена управления услугой. Сервер, обеспечивающий выполнение правил, является точкой обязательного выполнения стратегического решения (PEP) по отношению к Администратору приложений и применяет правила Домена управления ресурсами. Сервер, обеспечивающий выполнение правил, является PDP по отношению к CMTS, а CMTS является PEP по отношению к Серверу, обеспечивающему выполнение правил, и располагается на используемом маршруте следования пакетов.

В настоящем разделе описывается использование протокола COPS для транспортировки сообщений QoS в IP-Cablecom между Администратором приложений и Сервером, обеспечивающим выполнение правил, и между Сервером, обеспечивающим выполнение правил, и CMTS.

6.1 Шлюзы: Правила управления QoS

Мультимедийный шлюз в IP-Cablecom – это логическое представление решения о выполнении правил, которое устанавливается на CMTS. Шлюз используется для управления доступом при помощи передачи единственного IP потока на расширенные Услуги QoS, предоставляемые в кабельной сети, соответствующей Дополнению В/J.112. Шлюз всегда однонаправленный; один шлюз управляет доступом к потоку, который имеет либо восходящее, либо нисходящее направление, но не обоими сразу. Для двунаправленного сеанса связи IP требуется два шлюза, один – восходящий и один – нисходящий, каждый из которых идентифицируется своим уникальным GateID. Важно понимать, что это является базовым отличием от IP-Cablecom-T, в котором один GateID может обозначать и восходящий, и нисходящий шлюз.

В IP-Cablecom Multimedia каждый шлюз имеет отдельный GateID. Шлюз определяет форматы авторизации, резервирования и исполнения, которые должен использовать CMTS для выполнения операций авторизации, резервирования и исполнения.

Во всех сценариях при контроле установления соединения CMTS ДОЛЖНА выполнять проверку форматов, для того чтобы гарантировать, что используемый формат меньше или равен зарезервированному формату, и что зарезервированный формат меньше или равен авторизованному формату. Конкретные требования DOCSIS контроля установления соединения приведены в [1].

В модели "QoS, переданное с сервера методом принудительной рассылки" (Сценарий 1), CMTS использует информацию в шлюзе для непосредственного создания Потока услуги по Дополнению В/J.112, затем CMTS выполняет проверки форматов, необходимые для контроля установления соединения. В двух других моделях, описанных в Приложении I, "Запрошенное клиентом QoS, сформированное в соответствии с правилами" (Сценарий 2) и "Запрошенное клиентом QoS переданное с сервера по запросу" (Сценарий 3), CMTS использует информацию шлюза для выполнения контроля установления соединения ресурсов, запрошенных клиентом; CMTS не инициирует создание потоков. Администратор приложений несет ответственность за передачу сообщений шлюза на Сервер, обеспечивающий выполнение правил, а Сервер, обеспечивающий выполнение правил, несет ответственность за применение установленных правил, и за передачу на CMTS сообщений управления шлюзом.

Шлюз состоит из следующих элементов, которые описываются далее в настоящем разделе:

- Идентификатор шлюза (GateID);
- Идентификатор Администратора приложений (AMID);
- Идентификатор пользователя (SubscriberID);
- Спецификация шлюза (GateSpec);
- Классификатор (Classifier)
- Профиль трафика (Traffic Profile);
- Информация о создании сообщений (Event Generation Info) (дополнительно);
- Предел использования по времени (Time-Based Usage Limit) (дополнительно);
- Предел использования по объему (Volume-Based Usage Limit) (дополнительно);
- Скрытые данные (Opaque Data) (дополнительно).

GateID – это метка шлюза. GateID назначается CMTS используется Администратором приложений, Сервером, обеспечивающим выполнение правил, и клиентом для обозначения шлюза.

AMID – это метка, которая идентифицирует Администратора приложений.

SubscriberID однозначно идентифицирует клиента, к которому применяются правила.

GateSpec описывает определенные параметры авторизации, определяющие шлюз (т. е. QoS пределы, время и т. д.)

Классификатор описывает IP поток(и), которые будут поставлены в соответствие Поток(ам) услуги DOCSIS.

Traffic Profile описывает атрибуты QoS Потока услуги, используемого для передачи IP потока.

Информация о создании сообщений содержит информацию, которую использует CMTS с целью выполнения расчетов и сообщения об использовании.

Предел использования по объему определяет предел объема трафика, передаваемого в потоке, связанном со шлюзом.

Предел использования по времени описывает предел времени, ограничивающий продолжительность потока, связанного со шлюзом.

"Opaque Data" представляет собой объект общего назначения, который остается скрытым для элементов CMTS и PS, но который может содержать данные, чрезвычайно важные для АМ. Этот дополнительный объект, если его предоставляет АМ, остается на CMTS и возвращается во всех, связанных с ним ответах (см. 6.4.2.11).

Эти элементы связываются с Сервером, обеспечивающим выполнение правил, и CMTS через объекты COPS и подробно описываются далее в настоящем разделе. Во время создания шлюза, вышеописанная информация передается на CMTS. После того, как создание окончено, может быть создан Поток услуги DOCSIS. После создания Потока услуги DOCSIS, шлюз связывает его с дополнительным элементом – Поток услуги DOCSIS. Существует строгое однозначное соответствие между Поток услуги DOCSIS и шлюзом.

Шлюз проходит через многочисленные состояния. В сценариях 2 и 3, где объект клиент несет ответственность за резервирование и затем активизирование Поточков услуг DOCSIS, Мультимедийный шлюз функционирует аналогично тому, как работает в IP-Cablecom-T шлюз DQoS. Когда Сервер, обеспечивающий выполнение правил, создает шлюз на CMTS, говорят, что шлюз находится в "Авторизованном" состоянии. Он остается в этом состоянии, до тех пор, пока не будет удален Сервером, обеспечивающим выполнение правил, (или, что менее вероятно, пока не будет удален самим CMTS по каким-либо причинам), или до тех пор, пока не будет получен запрос от клиента на динамический поток.

Когда клиент требует, чтобы был добавлен динамический Поток услуги, он предоставляет GateID в качестве метки авторизации. CMTS использует GateID для контроля за установлением соединения на динамическом потоке DOCSIS, сравнивая его с авторизованным форматом, определенным шлюзом. В сценарии 1 Сервер, обеспечивающий выполнение правил, от лица Администратор приложений приказывает CMTS сменить состояние, а CMTS является объектом, ответственным за создание и разрушение Поточков услуги DOCSIS. Эти действия описываются в разделе "Смена состояния" настоящей Рекомендации. Когда CMTS получает команду разрушить Поток услуги DOCSIS, связанный с ним шлюз сохраняется до тех пор, пока он не будет явно удален действиями PS/АМ или пока не истечет время его существования и CMTS не потребует обратно его ресурсы (см. 6.5.8). Однако когда PS/АМ удаляет шлюз, CMTS, наоборот, удалит связанный с ним Поток услуги DOCSIS.

6.1.1 Идентификатор шлюза (GateID)

GateID – это идентификатор, который распределяет на местном уровне CMTS, в зоне действия которого расположен шлюз. GateID ДОЛЖЕН быть связан только с одним шлюзом. В то время как модель управления шлюзом в IP-Cablecom-T DQoS, как правило, предполагает наличие пары однонаправленных шлюзов (один восходящий и один нисходящий) на один GateID для поддержки типового сеанса двусторонней голосовой связи, здесь взаимосвязь шлюз/GateID является абсолютно однозначной, так, чтобы было легче предоставлять широкий спектр мультимедийных услуг.

Когда Администратор приложений передает запрос создать шлюз (Gate-Set), он включает Сервер, обеспечивающий выполнение правил, который передает на CMTS сообщение Gate-Set. Когда CMTS отвечает, передавая подтверждение, содержащее GateID, Сервер, обеспечивающий выполнение правил, ретранслирует этот ответ, включая GateID, обратно Администратору приложений. Отметим, что поскольку между PS и CMTS могут существовать отношения типа "многие-со-многими", невозможно гарантировать, что GateID, назначенный одним CMTS, будет в сети уникальным, поэтому PS могут использовать AMID для АМ, а также SubscriberID и GateID для уникальной идентификации шлюза.

Алгоритм, который может использоваться для присвоения значений GateID, имеет следующий вид. 32-битового слово делится на две части – часть номера и случайную часть. Часть номера идентифицирует шлюз, размещая номера в маленькой табличке, тогда как случайная часть придает величине некоторую скрытость. Вне зависимости от выбранного алгоритма, CMTS СЛЕДУЕТ попытаться минимизировать возможность неоднозначности GateID, обеспечивая такое положение дел, при котором ни одно значение GateID не может быть использовано повторно в течение трех минут после его предыдущего

удаления. В предложенном алгоритме это может быть выполнено путем простого увеличения на единицу части номера для каждого последовательно назначенного GateID, с циклическим возвращением к нулю при достижении максимально возможного целого числа номера.

6.1.2 Идентификатор Администратора приложений (AMID)

Каждому Администратору приложений предварительно назначается AMID, который является уникальным в среде одного провайдера услуг; Администратор приложений вводит этот идентификатор во все сообщения, которые он передает на Сервер, обеспечивающий выполнение правил. Сервер, обеспечивающий выполнение правил, без изменений ретранслирует эту информацию на CMTS при помощи Сообщений управления шлюзом. CMTS ДОЛЖНА вернуть AMID, связанный со шлюзом, на Сервер, обеспечивающий выполнение правил. Сервер, обеспечивающий выполнение правил, использует эту информацию для связи сообщений шлюза с конкретным Администратором приложений.

AMID ДОЛЖЕН представлять собой уникальное – в глобальном масштабе – значение, назначаемым Администратору приложений провайдером услуг. Администратор приложений ДОЛЖЕН использовать назначенный ему AMID при всех своих взаимодействиях Серверами, обеспечивающими выполнение правил. Отметим, что, поскольку Администратор приложений может использоваться третьей стороной, и один Администратор приложений может взаимодействовать с несколькими операторами провайдера услуг, одному физическому Администратору приложений может быть назначено несколько значений AMID.

6.1.3 Идентификация пользователя (SubscriberID)

SubscriberID, состоящий из IP адреса либо клиентского устройства CPE, либо CM, идентифицирует пользователя, запрашивающего услугу. В комплексных сетевых ситуациях этот адрес может использоваться для маршрутизации Сообщений управления шлюзом между несколькими Серверами, обеспечивающими выполнение правил, и для определения, какой CMTS предоставляет услугу для конкретной оконечной точки. Кроме IP адреса, абонент может также быть идентифицирован при помощи FQDN или некоторых скрытых данных (объекта, определенного ниже), относящихся к рассматриваемой услуге.

6.1.4 Спецификация шлюза (GateSpec)

GateSpec описывает некоторые высокоуровневые атрибуты шлюза и содержит и информацию о работе с другими объектами, определенными в сообщении шлюза. Информация, содержащаяся в GateSpec, описана ниже:

- Идентификатор шлюза – GateID;
- Идентификатор сеанса связи – SessionClassID;
- Направление – Direction;
- Таймер авторизации – Authorized Timer;
- Таймер резервирования – Reserved Timer;
- Таймер использования – Committed Timer;
- Таймер восстановления использования – Committed Recovery Timer;
- Замена DSCP/TOS – DSCP/TOS Override.

GateID уникальным образом идентифицирует шлюз, для которого должна быть выполнена данная операция.

SessionClassID позволяет Администратору приложений Серверу, обеспечивающему выполнение правил, разделить Шлюзы Gates на различные классы с различными параметрами авторизации. Например, SessionClassID может использоваться для описания некоторой схемы приоритетов или предпочтений, которая позволяет либо Серверу, обеспечивающему выполнение правил, либо CMTS прервать работы ранее авторизованного шлюза, для того чтобы разрешить работу шлюза с более высоким приоритетом.

Direction указывает для какого потока – нисходящего или восходящего – предназначен данный шлюз. В зависимости от этого указания, CMTS ДОЛЖНА соответствующим образом резервировать и активизировать потоки DOCSIS.

Authorized Timer ограничивает продолжительность времени, в течение которого разрешения остается действительным, пока не будет выполнена процедура резервирования (см. 6.2).

Reserved Timer ограничивает продолжительность времени, в течение которого резервирование остается действительным, пока не начнется использование ресурсов (см. 6.2).

Committed Timer ограничивает продолжительность времени, в течение которого Поток услуги может оставаться пустым.

Committed Recovery Timer ограничивает продолжительность времени, в течение которого используемый Поток услуги может продолжать существовать без получения следующего сообщения об обновлении от PS/AM после того, как PS/AM получил информацию об отсутствии активности (см. 6.2).

Поле DSCP/TOS Override может использоваться для замены поля в пакетах DSCP/TOS, связанных с Потокom услуги DOCSIS, который соответствует данному шлюзу. Это поле МОЖЕТ быть не определено, в этом случае CMTS не переписывает поле DSCP/TOS в пакете. Это поле может использоваться как в нисходящем, так и в восходящем направлениях.

6.1.5 Классификатор

Для шлюза ДОЛЖЕН быть определен Классификатор. Дополнительные Классификаторы могут быть включены в исходное сообщение установки шлюза (Gate-Set). Классификаторы могут добавляться и удаляться в последующих сообщениях Gate-Set. Соответствующие требованиям варианты реализации ДОЛЖНЫ поддерживать, как минимум, четыре Классификатора при обработке сообщения Gate-Set. Классификатор идентифицирует IP поток, который будет поставлен в соответствие Потокom услуги DOCSIS, связанному с данным шлюзом. Классификатор, используемый для создания Потокa услуги, ДОЛЖЕН соответствовать Классификатору, определенному для данного шлюза. В сценарии 1, когда CMTS создает динамический поток, он ДОЛЖЕН использовать Классификатор шлюза в качестве Классификатора Потокa услуги DOCSIS.

Классификатор состоит из восьми значений:

- Протокол – Protocol;
- IP источник – Source IP;
- Порт источника – Source Port;
- IP места назначения – Destination IP;
- Порт места назначения – Destination Port;
- Приоритет – Priority;
- Маска DSCP/TOS – DSCP/TOS Mask.

Поле Protocol идентифицирует тип протокола (например, IP, ICMP, и т. д.).

Source IP – это IP адрес (как его видит CMTS) создателя IP потока, тогда как Destination IP – это точка завершения IP потока.

Source Port и Destination Port определяют порты UDP или TCP для IP потока.

Priority может использоваться, для того чтобы отличить друг от друга различные Классификаторы, которые соответствуют конкретным пакетам. Это поле, как правило, устанавливается в значение "по умолчанию", поскольку Классификаторы, обычно бывают уникальными.

Поле DSCP/TOS идентифицирует поле DSCP/TOS, которое должно быть поставлено в соответствие пакетами, которые вводятся в данный IP поток. Для обеспечения максимальной гибкости при определении стратегии управления сетью, определяется соответствующая маска, которая определяет, какие биты в байте DSCP/TOS должны использоваться в фильтрах при классификации пакетов. Это позволяет использовать обе стратегии DiffServ и TOS (каждая из которых определяет и использует отдельные биты в пределах этого баята).

Классификатор МОЖЕТ содержать поля со знаками подстановки (указанные полями, заполненными нулями), но необходимо проявлять осторожность, чтобы не оказалось так, что нескольким IP потокам будет непреднамеренно соответствовать один и тот же Классификатор, что может привести к неожиданным результатам.

6.1.6 Профиль трафика

Существует три способа определить Профиль трафика для шлюза:

- 1) Спецификация потока – FlowSpec;
- 2) Название класса обслуживания DOCSIS – DOCSIS Service Class Name; или
- 3) Параметры, присущие DOCSIS – DOCSIS-Specific Parameterization.

Сервер, обеспечивающий выполнение правил, и Администратор приложений ДОЛЖНЫ определить Профиль трафика для шлюза, используя одно из следующего:

- 1) Спецификацию потока;
- 2) Названия класса обслуживания DOCSIS; или
- 3) Параметры, присущие DOCSIS.

Форматы, используемые в профиле трафика ДОЛЖНЫ быть одного и того же типа, т. е. это должен быть либо формат Спецификации потока, либо Названий класса услуги DOCSIS, либо Параметров DOCSIS.

ДОЛЖЕН существовать, как минимум один набор параметров профиля трафика, определенный при первичной установке шлюза. Сервер, обеспечивающий выполнение правил, и Администратор приложений МОГУТ определить второй набор для описания резервного формата и третий набор для описания используемого формата. Если CMTS получил указание немедленно создать динамический поток после получения сообщения Gate-Set (при помощи и резервированного или используемого форматов), CMTS ДОЛЖНА использовать параметры профиля трафика резервированного или используемого форматов, для того чтобы выполнить передачу сообщений в соответствии Дополнением В/J.112 с целью формирования потоков направления, указанном в поле Direction сообщения GateSpec (при условии, что запрос авторизован и имеется достаточно ресурсов для его удовлетворения). Когда CMTS получает указание перейти в состояние Committed, CMTS ДОЛЖНА использовать Профиль трафика для активирования Потока услуги DOCSIS. В процессе оптимизации Сервер, обеспечивающий выполнение правил, МОЖЕТ давать указания CMTS о выполнении всех трех действий (авторизовать, зарезервировать и использовать) от лица Администратора приложений при помощи одного сообщения Управления шлюзом (Gate Control). В качестве альтернативы, PS/AM МОГУТ передавать отдельные сообщения Gate-Set, указывая CMTS авторизовать и зарезервировать, а затем использовать при помощи следующего сообщения Gate-Set.

6.1.6.1 Спецификация потока – FlowSpec

Объект FlowSpec содержит объекты FlowSpec протокола RSVP, которые используются для описания профиля трафика IP потока. Объект FlowSpec object может содержать несколько объектов протокола RSVP:

- Объект FlowSpec, который определяет формат авторизации ресурсов, в соответствии с которым будет выполняться резервирование.
- Объект FlowSpec, который определяет формат резервирования, в соответствии с которым будет выполняться запрос на использование ресурсов.
- Объект FlowSpec, который определяет ресурсы. Которые будут использоваться.

Спецификации потока протокола RSVP поддерживают два типа услуг: управляемая нагрузка [4] и гарантированная нагрузка [5]. Основные различия между этими двумя типами услугами рассматриваются Вт разделе 8. Эти два типа услуг основаны на номере услуги FlowSpec, который определен в объекте FlowSpec протокола RSVP. Номер услуги 5 используется для управляемой загрузки, а Номер услуги 2 – для гарантированной. Услуга с управляемой нагрузкой ДОЛЖНА содержать только параметры область памяти для метки TSpec, но не RSpec. Услуга с гарантированной нагрузкой ДОЛЖНА содержать и TSpec, и RSpec.

В разделе 8 содержится информация о том, как явно выполнить преобразование параметров RSVP в параметры DOCSIS. Когда параметры DOCSIS получаются с использованием параметров RSVP FlowSpec, некоторые параметры DOCSIS оказываются в высшей степени приближенными. Если такое приближение не дает Серверу, обеспечивающему выполнение правил, или Администратору приложений желаемой степени контроля, PS/AM могут использовать другие способы определения профиля трафика, который дает возможность определить некоторые параметры DOCSIS. Эти параметры дают возможность Серверу, обеспечивающему выполнение правил, или Администратору приложений то точно отрегулировать стандартное преобразование параметров FlowSpecs в параметры DOCSIS.

6.1.6.2 Название класса обслуживания DOCSIS

Название класса обслуживания DOCSIS указывает класс обслуживания DOCSIS, который должен использоваться для описания атрибутов QoS. CMTS ДОЛЖНА поддерживать названия классов обслуживания DOCSIS.

Название класса обслуживания DOCSIS позволяет использовать на CMTS заранее определенные параметры QoS DOCSIS. На CMTS можно сконфигурировать названия классов обслуживания DOCSIS с различными профилями QoS DOCSIS, затем указать в шлюзе Название класса обслуживания DOCSIS, для того чтобы установить неявное соответствие профиля QoS с конкретным шлюзом. Кроме того, DOCSIS позволяет изменять эти параметры, используя объекты TLV. В рамках IPCablecom Multimedia, НЕЛЬЗЯ модифицировать параметры QoS Названия класса обслуживания DOCSIS при помощи TLV. Если запрашивается изменение параметров QoS для данного Названия класса обслуживания, CMTS ДОЛЖНА вернуть ошибку "Неопределенное Название класса обслуживания, (см. 6.4.2.14).

Более полная информация о классах обслуживания DOCSIS содержится в В.10.1.3/J.112 [1].

6.1.6.3 Параметры, присущие DOCSIS

Третий способ определения профиля трафика заключается в использовании профиля трафика, присущего DOCSIS; Это дает возможность Администратору приложений явно определить параметры DOCSIS для потока DOCSIS. Если Администратор приложений желает использовать этот третий способ определения профиля трафика, он ДОЛЖЕН включать в себя объект, содержащий параметры, присущие DOCSIS.

Все типы планирования Потока услуги DOCSIS поддерживаются через несколько S-типов профиля трафика. Каждый S-тип имеет собственное кодирование параметров, присущих DOCSIS, относящихся к данному типу планирования Потока услуги DOCSIS. Более подробная информация о параметрах, присущих DOCSIS, содержится в 6.4.2.7.

6.1.7 Информация о создании события

Этот объект содержит информацию, относящуюся к действиям CMTS по выполнению функций расчетов и биллинга. Его атрибуты включают в себя:

- Первичный адрес (Primary Address): Порт первичного Сервера регистрации, на который CMTS ДОЛЖНА передавать записи о событиях.
- Вторичный адрес (Secondary Address): Порт вторичного Сервера регистрации, который CMTS ДОЛЖНА использовать, как определено в [10], если первичный недоступен.
- Флаг, указывающий, ДОЛЖНА ли CMTS передавать Сообщения о событиях на Сервер регистрации в реальном времени, или же CMTS ДОЛЖНА группировать Сообщения о событиях и передавать их периодически с некоторым интервалом.
- Идентификатор BillingCorrelationID, который CMTS ДОЛЖНА передавать на Сервер регистрации с каждой записью о событии.

Отсутствие объекта Информация о создании события указывает, что Системе завершения вызова для кабельного модема НЕЛЬЗЯ создавать Сообщения о событиях для данного шлюза.

6.1.8 Предел использования по времени

Этот объект определяет продолжительность интервала времени, в течение которого шлюз может оставаться используемым до появления временного порога для этого шлюза. Этот объект не виден для CMTS. CMTS не несет ответственности за соблюдение временных пределов, но ДОЛЖНА сохранять этот объект и возвращать его по запросу.

6.1.9 Предел использования по объему

Администратор приложений применяет Предел использования по объему, для того чтобы дать указание CMTS создать Сообщение управления шлюзом, когда через этот шлюз проходит определенное количество данных. CMTS не несет ответственности за соблюдение пределов по объему, но ДОЛЖНА сообщить на PS/AM, когда достигнут определенный предел по объему.

6.1.10 Скрытые данные

Скрытые данные состоят из общей информации, которую Сервер, обеспечивающий выполнение правил, или Администратор приложений могут сохранять в CMTS. Эти данные остаются скрытыми для CMTS, но они содержат полезную информацию для PS или AM. Если это предусмотрено PS/AM, CMTS будет возвращать этот объект во всех ответах (см. 6.4.2.11).

6.1.11 Информация о времени использования шлюза (Gate time info)

Gate Time Info содержит метку времени, указывающую время, когда шлюз использовался. Она может быть запрошена и использована Сервером, обеспечивающим выполнение правил, или Администратором приложений для выполнения правил относительно времени использования сети.

6.1.12 Информация об использовании шлюза (Gate usage info)

Gate Usage Info состоит из счетчика байтов, указывающего количество байтов информации, переданных через этот шлюз (см. 6.4.2.13). Аналогично объекту Информация о времени использования шлюза, эта информация может использоваться Сервером, обеспечивающим выполнение правил, или Администратором приложений для выполнения правил относительно объемов информации, передаваемых в сети.

6.2 Смена состояний шлюза

Как было кратко изложено ранее, шлюз может находиться в следующих логических состояниях:

- Авторизован – Сервер, обеспечивающий выполнение правил, разрешил создание потока с определенными ограничениями по ресурсам;
- Зарезервирован – ресурсы зарезервированы для данного потока;
- Используется – ресурсы активны и используются;
- Восстановление использования – обнаружено отсутствие активности потока; ожидается восстановление ресурсов.

Для состояния, показанного на Рисунке 3, CMTS ДОЛЖНА завершить событие включения с успешным результатом прежде, чем она переведет шлюз из одного состояния в другое. Системе завершения вызова для кабельного модема НЕЛЬЗЯ менять состояние для событий Управления шлюзом до тех пор, пока запрос не будет полностью обработан (включая любые результирующие переходы потока) и пока CMTS не определит, что должно быть передано уведомление об успешном выполнении операции.

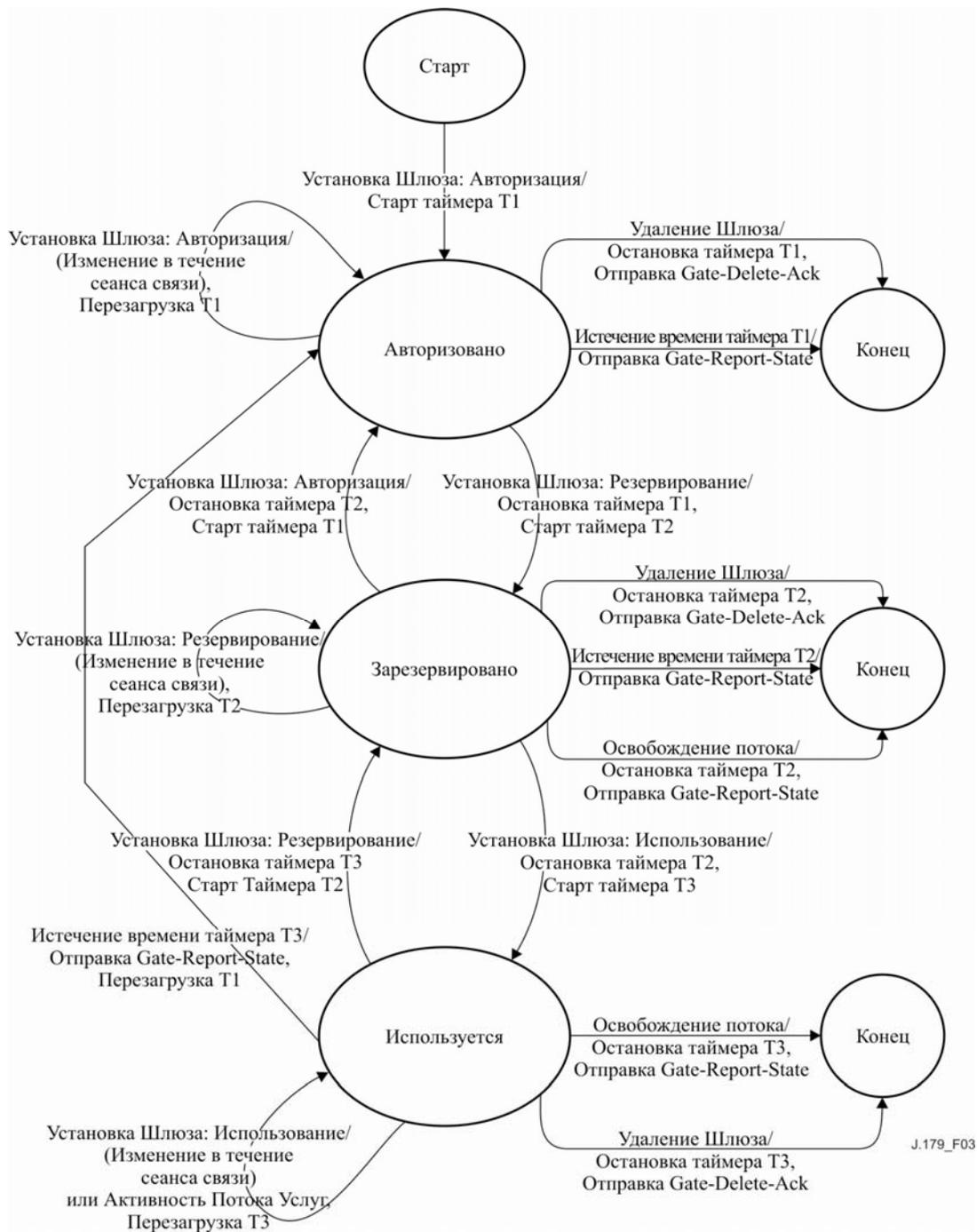


Рисунок 3/J.179 – Смена состояний шлюза

СМТС ДОЛЖНА поддерживать состояния шлюза и их смену, как показано на Рисунке 3 и описано в настоящем разделе. Кроме того, СМТС ДОЛЖНА выполнять переходы для обработки ошибок протокола.

В настоящем разделе мы описываем такие смены состояний шлюза в СМТС, которые вызваны внешними (Сообщениями управления шлюзом от Сервера, обеспечивающего выполнение правил), а также такие смены состояний, которые вызваны внутренними событиями (например, истечением времени, определенным таймером). Отметим, что Сервер, обеспечивающий выполнение правил, не является источником внешних событий; Сервер, обеспечивающий выполнение правил, действует просто как посредник в отношении Администратора приложений, который и генерирует эти события.

6.2.1 Состояние – Авторизован

Шлюз создается на CMTS по команде Gate-Set Сервера, обеспечивающего выполнение правил. CMTS назначает ему уникальные идентификатор, называемый GateID. Теперь говорят, что шлюз находится в состоянии Авторизован, и CMTS ДОЛЖНА включить Таймер T1. Таймер T1 ограничивает продолжительность интервала времени, в течение которого авторизация остается действительной.

Шлюз в состоянии Авторизован ДОЛЖЕН быть удален при приеме сообщения Gate-Delete (Удалит шлюз). Когда это происходит, CMTS ДОЛЖНА ответить, передав уведомление об удалении шлюза Gate-Delete-Ask и ДОЛЖНА остановить Таймер T1.

ТРЕБУЕТСЯ, чтобы CMTS поддерживала следующие смены состояний, пока шлюз находится в состоянии Авторизован:

Смены состояния Авторизован:

- Из состояния Авторизован – обратно в состояние Авторизован: Изменить формата состояния Авторизован;
- Из состояния Авторизован – в состояние Резервирован (определяет формат состояния Резервирован \leq формата состояния Авторизован);
- Из состояния Авторизован – в состояние Конец (удаляет формат состояния Авторизован).

Системе завершения вызова для кабельного модема НЕЛЬЗЯ поддерживать какие-либо иные смены состояний для шлюза находящегося в состоянии Авторизован, но к описанным сменам состояний может привести целый ряд разнообразных побудительных причин.

Когда шлюз создается, говорят, что он находится в состоянии Авторизован. Пока он находится в состоянии Авторизован, Сервер, обеспечивающий выполнение правил, может изменить любой параметр шлюза (например, Профиль трафика, Классификатор, и т. д.). Если в то время, когда шлюз находится в состоянии Авторизован, принимается сообщение Создать шлюз (Gate-Set), которое не переводит шлюз в состояние Резервирован или Используется, то CMTS ДОЛЖНА перезапустить Таймер T1.

Когда шлюз находится в состоянии Авторизован CMTS ДОЛЖНА перевести шлюз в состояние Резервирован после получения успешно обработанного запроса от Сервера, обеспечивающего выполнение правил. CMTS ДОЛЖНА перевести шлюз в состояние Конец после получения сообщения Удалить шлюз (Gate-Delete) от Сервера, обеспечивающего выполнение правил, или после истечения времени, определенного Таймером T1.

6.2.2 Состояние – Резервирован

Шлюз, находящийся в состоянии Авторизован, ожидает, что клиент сделает попытку резервировать ресурсы. В сценарии 1, Сервер, обеспечивающий выполнение правил, резервирует ресурсы от лица клиента. Для того чтобы резервировать ресурсы, Сервер, обеспечивающий выполнение правил, ДОЛЖЕН передать команду Gate-Set с Профилем трафика, содержащим формат состояния Резервирован. После приема такого запроса на резервирование CMTS ДОЛЖНА проверить, находится ли этот запрос в пределах авторизации, установленных для этого шлюза, и выполнить процедуры контроля над установлением соединения.

Если запрос на резервирование не прибывает до истечения времени, определенного Таймером T1, CMTS ДОЛЖНА удалить шлюз, и уведомить Сервер, обеспечивающий выполнение правил, об изменении состояния. Если процедуры контроля над установлением соединения выполнены успешно и было запрошено только резервирование ресурсов, CMTS ДОЛЖНА перевести шлюз в состояние Резервирован. Одновременно, CMTS ДОЛЖНА также остановить Таймер T1 и запустить Таймер T2 (Резервный таймер). Если процедуры контроля над установлением соединения не выполнены, CMTS ДОЛЖНА поддерживать шлюз в состоянии Авторизован и передать на PS ответ Ошибка создания шлюза (Gate-Set-Err).

ТРЕБУЕТСЯ, чтобы CMTS поддерживала следующие смены состояний, пока шлюз находится в состоянии Резервирован:

Смены состояния Резервирован:

- Из состояния Резервирован – обратно в состояние Резервирован: Изменить формата состояния Авторизован (\geq формата состояния Резервирован);
- Из состояния Резервирован – обратно в состояние Авторизован: Изменить формата состояния Резервирован (\leq формата состояния Авторизован);
- Из состояния Резервирован – в состояние Используется (определяет формат состояния Используется \leq формата состояния Резервирован);
- Из состояния Резервирован – в состояние Конец (удаляет форматы состояний Резервирован и Авторизован).

Системе завершения вызова для кабельного модема НЕЛЬЗЯ поддерживать какие-либо иные смены состояний для шлюза находящегося в состоянии Зарезервирован, но к описанным сменам состояний может привести целый ряд разнообразных побудительных причин.

СMTS ДОЛЖНА перевести шлюз из состояния Авторизован в состояние Зарезервирован, если этот переход запрашивается Сервером, обеспечивающим выполнение правил, при условии, что формат состояния Зарезервирован меньше или равен формату состояния Авторизован, запрос проходит контроль за установлением соединения и поток успешно резервируется. Когда шлюз находится в состоянии Зарезервирован, формат состояния Авторизован этого шлюза МОЖЕТ быть изменен при помощи сообщения Gate-Set. Формат состояния Зарезервирован этого шлюза также может быть изменен в состоянии Зарезервирован (см. 6.5.6). Если в то время, когда шлюз находится в состоянии Зарезервирован, принимается сообщение Gate-Set, которое не переводит шлюз в состояние Авторизован или Используется, то СMTS ДОЛЖНА перезапустить Таймер T2.

Если запрос Использовать не поступает до истечения времени, определенного таймером T2, СMTS ДОЛЖНА удалить шлюз и уведомить Сервер, обеспечивающий выполнение правил, об изменении состояния.

Формат состояния Зарезервирован ДОЛЖЕН всегда быть меньше или равен формату состояния Авторизован. Для того чтобы СMTS могла перевести шлюз из состояния Зарезервирован в состояние Используется, формат состояния Используется ДОЛЖЕН быть меньше или равен формату состояния Зарезервирован (см. 6.5.3).

Когда шлюз находится в состоянии Зарезервирован, Сервер, обеспечивающий выполнение правил, может изменить формат состояния Авторизован, определив новый Профиль трафика в сообщении Gate-Set. Этот новый Профиль трафика определит измененный формат состояния Авторизован и тот же самый формат состояния Зарезервирован, который использовался ранее для перевода шлюза в состояние Зарезервирован. Однако все запросы на изменение форматов состояний Авторизован, Зарезервирован или Используется, ДОЛЖНЫ соответствовать общему правилу:

формат состояния Авторизован \geq формат состояния Зарезервирован \geq формат состояния Используется
Сервер, обеспечивающий выполнение правил, МОЖЕТ удалить шлюз, находящийся в состоянии Зарезервирован, передав сообщение Gate-Delete.

6.2.3 Состояние – Используется

Шлюз, находящийся в состоянии Зарезервирован, ожидает, что клиент начнет использовать ресурсы, и таким образом активизирует их. В сценарии 1, Сервер, обеспечивающий выполнение правил, использует ресурсы от лица клиента. Для того чтобы использовать ресурсы, Сервер, обеспечивающий выполнение правил, ДОЛЖЕН передать команду Gate-Set с Профилем трафика, содержащим формат состояния Используется. СMTS ДОЛЖНА снова авторизовать QoS, запрошенные в формате состояния Зарезервирован. Если авторизация прошла успешно, СMTS ДОЛЖНА запустить Таймер T3, и либо остановить Таймер T2, если формат состояния Авторизован равен формату состояния Используется, либо перезапустить Таймер T2, если формат состояния Авторизован больше формата состояния Используется. Если авторизация не выполнена, СMTS ДОЛЖНА перезапустить Таймер T2.

Отметим, что после того, как Поток услуги DOCSIS активизирован, СMTS ДОЛЖНА перезапускать Таймер T3, когда в потоке передаются данные. Если в течение времени, равного T3, в потоке не наблюдается активности, СMTS ДОЛЖНА уведомить Сервер, обеспечивающий выполнение правил, об изменении состояния. Точно также, Сервер, обеспечивающий выполнение правил, ДОЛЖЕН уведомить Администратора приложений об изменении состояния.

Когда шлюз находится в состоянии Используется, Администратор приложений МОЖЕТ удалить шлюз, передав сообщение Gate-Delete на Сервер, обеспечивающий выполнение правил, который, в свою очередь, ДОЛЖЕН ретранслировать это сообщение на СMTS. Если Сервер, обеспечивающий выполнение правил, передает на СMTS сообщение Gate-Delete, СMTS ДОЛЖНА удалить шлюз и соответствующий Поток услуги, и остановить Таймеры T2 и T3, если они работают.

ТРЕБУЕТСЯ, чтобы СMTS поддерживала следующие смены состояний, пока шлюз находится в состоянии Используется:

Смены состояния Используется:

- Из состояния Используется – обратно в состояние Используется: Изменить формат состояния Авторизован (\geq формата состояния Зарезервирован);
- Из состояния Используется – обратно в состояние Используется: Изменить формат состояния Зарезервирован (\geq формата состояния Используется и \leq формата состояния Авторизован);
- Из состояния Используется – обратно в состояние Используется: Изменить формат состояния Используется (\leq формата состояния Зарезервирован);

- Из состояния Используется – в состояние Резервирован (удаляет формат состояния Используется);
- Из состояния Используется – в состояние Восстановление использования: (инициирует процесс восстановления ресурсов);
- Из состояния Используется – в состояние Конец (удаляет форматы состояний Используется, Резервирован и Авторизован).

Системе завершения вызова для кабельного модема НЕЛЬЗЯ поддерживать какие-либо иные смены состояний для шлюза находящегося в состоянии Используется, но к описанным сменам состояний может привести целый ряд разнообразных побудительных причин.

Когда шлюз находится в состоянии Резервирован, CMTS ДОЛЖНА перевести шлюз в состояние Используется, если это запрашивается Сервером, обеспечивающим выполнение правил, при условии, что формат состояния Используется меньше или равен формату состояния Резервирован (см. 6.5.3). Когда шлюз находится в состоянии Используется, Сервер, обеспечивающий выполнение правил, Может изменить формат состояния Используется этого шлюза при помощи сообщения Gate-Set, при условии, что формат состояния Авторизован больше или равен формату состояния Резервирован. В этом состоянии Сервер, обеспечивающий выполнение правил, МОЖЕТ также изменить формат состояния Резервирован, при условии, что формат состояния Резервирован больше или равен формату состояния Используется. В этом состоянии Сервер, обеспечивающий выполнение правил, МОЖЕТ даже изменить формат состояния Используется, при условии, что новый формат состояния будет меньше или равен формату состояния Резервирован. Если, когда шлюз находится в состоянии Используется, принимается запрос прекратить использование всех ресурсов (но сохранить их резервированными), CMTS ДОЛЖНА остановить Таймер T3, (пере-)запустить Таймер T2, и перевести шлюз обратно в состояние Резервирован. В сценарии 1, Сервер, обеспечивающий выполнение правил, Может запросить это действие, передав сообщение Gate-Set с Профилем трафика, который содержит форматы состояний Авторизован и Резервирован, но не содержит формат состояния Используется.

Когда шлюз находится в состоянии Используется, CMTS ДОЛЖНА перевести шлюз в состояние Конец после получения сообщения Gate-Delete от Сервера, обеспечивающего выполнение правил. Когда шлюз находится в состоянии Используется, Сервер, обеспечивающий выполнение правил, Может изменить формат состояния Авторизован или Резервирован, просто определив новый Профиль трафика; этот новый Профиль трафика ДОЛЖЕН содержать измененные форматы состояний Авторизован или Резервирован, и тот же самый формат состояния Используется, который был применен ранее при переводе шлюза в состояние Используется.

При выполнении (повторного) перехода в состояние Используется из-за приема сообщения Gate-Set, CMTS ДОЛЖНА (пере)запустить Таймер T2, если формат состояния Резервирован больше, чем формат состояния Используется, или ДОЛЖНА остановить Таймер T2, если он работал до этого, и формат состояния Резервирован теперь равен формату состояния Используется.

Когда шлюз находится в состоянии Используется:

- 1) Если истекает время, заданное таймером T2, шлюз ДОЛЖЕН оставаться в состоянии Используется, а CMTS ДОЛЖНА передать сообщение о состоянии шлюза Gate-Report-State с кодом причины 9 (Состояние шлюза не изменилось, но истечение времени, заданного таймером T2, привело к уменьшению резервирования) на Сервер, обеспечивающий выполнение правил, указывая на уменьшение резервированных ресурсов;
- 2) Если сообщение Gate-Set возвращает шлюз обратно в состояние Резервирован, то таймер T2 ДОЛЖЕН быть запущен, если он не работал до сих пор и перезапущен, если он работал; и
- 3) Если возникает переход в состояние Конец, оба таймера T2 и T3 ДОЛЖНЫ быть остановлены, если они до сих пор работали.

В качестве оптимизации для сценария 1, Сервер, обеспечивающий выполнение правил, МОЖЕТ Авторизовывать, Резервировать и Использовать одновременно, передавая сообщение Gate-Set с Профилем трафика, который содержит все три формата, так что CMTS получает команду выполнить все три действия последовательно без дополнительного взаимодействия с Сервером, обеспечивающим выполнение правил: то есть, все команды должны быть выполнены успешно (если это так, то CMTS ДОЛЖНА указать это, передав уведомление Gate-Set-Ack) или не успешно (если это так, то CMTS ДОЛЖНА указать это, передав сообщение об ошибке Gate-Set-Err).

Из состояния Используется шлюз переходит в состояние Восстановление использования из-за того, что истекает время, заданное таймером T3. Если CMTS обнаруживает, что в течение времени E3 в соответствующем потоке не наблюдается никакой активности, то CMTS ДОЛЖНА запустить таймер T4, передать сообщение о состоянии шлюза (Gate-Report-State) на Сервер, обеспечивающий выполнение

правил, указывая, что поток не активен в течение времени, заданного таймером T3, и перейти в состояние Восстановление использования, оставляя при этом соответствующий поток в активном состоянии. Сервер, обеспечивающий выполнение правил, ДОЛЖЕН ретранслировать сообщение о состоянии шлюза (Gate-Report-State) Администратору приложений. Администратор приложений ДОЛЖЕН либо обновить правила, передав сообщение Gate-Set, или удалить шлюз, передав сообщение Gate-Delete.

В некоторых приложениях нежелательно получать уведомления о прекращении активности в потоке. В таком случае, Администратор приложений может установить таймер T3 (который соответствует таймеру активного состояния DOCSIS) в 0. Как определено в [1], значение 0 для таймера активного состояния DOCSIS указывает на то, что для данного потока на CMTS отключена функция обнаружения активности. Таким образом, шлюз будет оставаться в состоянии Используется либо до тех пор, пока не будет получено сообщение Gate-Delete, либо пока не отключится CM.

6.2.4 Состояние – Восстановление использования

В состоянии Используется поток, связанный с данным шлюзом, является активным. Если CMTS обнаруживает, что поток не используется в течение времени, которое превышает время, определенное таймером T3, CMTS уведомляет PS (который уведомляет AM) о том, что Поток услуги, связанный с данным шлюзом, не используется, запускает таймер T4 и переводит шлюз в состояние Восстановление использования.

ПРИМЕЧАНИЕ. – Если таймер T2 работает, он продолжает работать. Его НЕЛЬЗЯ перезапускать.

AM должен принять решение о том, изменять ли правила, передавая на PS сообщение Gate-Set, или удалить шлюз, передав на PS сообщение Gate-Delete. Сервер, обеспечивающий выполнение правил, ДОЛЖЕН ретранслировать на CMTS сообщение Gate-Set или сообщение Gate-Delete.

Если, во время нахождения в состоянии Восстановление использования, CMTS принимает Сообщение создать шлюз (Gate-Set) для данного шлюза до истечения времени, определенного таймером T4, то CMTS ДОЛЖНА остановить таймер T4, перезапустить таймер T3, перевести шлюз обратно в состояние Используется и (пере)запустить таймер T2, если формат состояния Зарезервирован больше, чем формат состояния Используется, или остановить таймер T2, если он работает и новый формат состояния Зарезервирован равен формату состояния Используется.

Если, во время нахождения в состоянии Восстановление использования, до истечения времени, определенного таймером T4, то CMTS ДОЛЖНА остановить таймер T4, удалить шлюз и соответствующий Поток услуги, и остановить таймер T2, если он работает.

Если время, определенное таймером T4, истекает во время нахождения в состоянии Восстановление использования, то CMTS ДОЛЖНА передать на PS сообщение о состоянии шлюза (Gate-Report-State), остановить таймер T2, если он работает, остановить передачу Потока услуги, связанного с данным шлюзом и затем удалить шлюз. Далее, Сервер, обеспечивающий выполнение правил, ДОЛЖЕН уведомить Администратора приложений об изменении состояния.

Если время, определенное таймером T2, истекает во время нахождения в состоянии Восстановление использования, то шлюз ДОЛЖЕН оставаться в состоянии Восстановление использования, и CMTS ДОЛЖНА передать сообщение Gate-Report-State с кодом причины 9 (Состояние шлюза не изменилось, но истечение времени, определенного таймером T2, привело к уменьшению зарезервированных ресурсов) на Сервер, обеспечивающий выполнение правил, указывающим на уменьшение зарезервированных ресурсов.

Во время нахождения шлюза в состоянии Восстановление использования, CMTS ДОЛЖНА поддерживать следующие смены состояний:

Смены состояния Восстановление использования:

- Из состояния Восстановление использования – в состояние Восстановление использования: (обновлены правила);
- Из состояния Восстановление использования – в состояние Конец (удаляет форматы состояний Используется, Зарезервирован и Авторизован);
- Из состояния Восстановление использования – в состояние Восстановление использования (Истекло время, определенное таймером T2; передается сообщение Gate-Report-State).

Системе завершения вызова для кабельного модема НЕЛЬЗЯ поддерживать какие-либо иные смены состояний для шлюза находящегося в состоянии Восстановление использования, но к описанным сменам состояний может привести целый ряд разнообразных побудительных причин.

Могут существовать приложения, в которых нежелательно поддерживать шлюз после обнаружения его не активности. В такой ситуации AM может установить таймер T4 в 0. когда T4 установлен в ноль, шлюз ни одного мгновения не находится в состоянии Восстановление использования, и по истечении времени, определенного таймером T3, этот шлюз (и поток) ДОЛЖНЫ быть удалены.

6.3 Профиль COPS для передачи мультимедийной информации в IPcablecom

Как было определено раньше, контроль за установлением соединения включает в себя процесс управления запросами ресурсов QoS, основанный на выполнении административных правил и доступных ресурсах. Высокоуровневые операционные модули, связанные с этим процессом, описаны в Приложении I. В этой модели административные правила хранятся в специальной базе данных и управляются Сервером, обеспечивающим выполнение правил.



Рисунок 4/J.179 – Алгоритм контроля за QoS установления соединения

О решениях, связанных с контролем за установлением соединения, принятые Сервером, обеспечивающим выполнение правил, ДОЛЖНО быть сообщено на CMTS или Администратору приложений с использованием протокола COPS. CMTS МОЖЕТ передавать на сервер COPS запросы Контроля за QoS установления соединения, основанные на событиях в сети, инициированных либо протоколом сигнализации QoS, оили при помощи механизмов обнаружения потоков данных. Событию в сети может также требоваться регулирование ширины полосы QoS, например, когда вводится в действие новый интерфейс с возможностями QoS.

Решения о выполнении правил QoS, принимаемые Сервером, обеспечивающим выполнение правил, МОГУТ быть принудительно переданы на CMTS по требованию Администратора приложений. CMTS МОЖЕТ получить доступ к этой информации о решении для принятия решений об обязательном выполнении правил для входящих запросов на сеансы связи, принимаемых данной CMTS. В IPcablecom Multimedia Система завершения вызова для кабельного модема НЕЛЬЗЯ поддерживать инициированные кабельным модемом (CM) DSx сообщения. CMTS ДОЛЖНА рассматривать инициированное кабельным модемом (CM) DSx сообщение как запрос с неправильным идентификатором шлюза (GateID).

Конфигурация клиент/сервер протокола COPS, поддерживающая Контроль за QoS установления соединения, определена в документе IETF по протоколу COPS [7]. Этот протокол предусматривает следующие действия:

- Открыть клиента (OPN)/ Принять клиента (CAT)/ Закрыть клиента (CC). Клиент протокола COPS (PEP) передает сообщение OPN для установления соединения с сервером COPS (PDP), и этот сервер отвечает, передавая сообщение CAT, о создании соединения. Для завершения соединения, этот сервер или клиент передает сообщение CC.
- Запрос (REQ). Клиент передает на сервер сообщение REQ для запроса информации о решении контроля за установлением соединения или информации о конфигурации устройства. Сообщение REQ может содержать информацию о клиенте, используемую сервером, а также данные из базы данных о правилах установления сеансов связи, необходимые для принятия решений, основанных на выполнении правил.
- Решение (DEC). Сервер отвечает на полученные сообщения REQ, передавая сообщение DEC обратно клиенту, создавшему исходный запрос. Сообщения DEC могут быть переданы сразу

же в ответ на REQ (т. е. a solicited DEC) или в любой время после изменения или обновления ранее принятого решения (т. е. an unsolicited DEC).

- Сообщение о состоянии (Report-State (RPT)). Клиент передает на сервер сообщение RPT, указывая изменения в состоянии запроса клиента. Клиент передает это сообщение, для того чтобы проинформировать сервер о реальном объеме зарезервированных ресурсов после того, как сервер разрешил соединение. Клиент может также использовать сообщение, для того чтобы периодически сообщать серверу о текущем состоянии клиента.
- Удалить запрос о состоянии (Delete-Request-State (DRQ)). Клиент передает на сервер сообщение DEL, запрашивая удаление текущего состояния. Это может быть результатом освобождения клиентом ресурсов QoS.
- Сохранить действующим (Keep-Alive (KA)). Передается и клиентом, и сервером для обнаружения срыва связи.
- Запрос о состоянии синхронизации/Завершение синхронизации (Synchronize-State-Request (SSQ)/Synchronize-State-Complete (SSC)). Сервер передает сообщение SSQ клиенту, запрашивая информацию о текущем состоянии. Клиент повторно передает запрошенные данные на сервер для выполнения синхронизации, затем передает сообщение SSC для уведомления о завершении события синхронизации. Сервер, обеспечивающий выполнение правил, МОЖЕТ, при необходимости поддерживать функции синхронизации SSQ/SSC для Сервера, обеспечивающего выполнение правил, для получения данных или модификации состояния от CMTS. CMTS ДОЛЖНА поддерживать функции синхронизации.

В архитектуре IP-Cablecom Multimedia существуют следующие связи PDP-PEP:

- Администратор приложений – это Точка принятия решения (PDP) в протоколе COPS по отношению к Серверу, обеспечивающему выполнение правил.
- Сервер, обеспечивающий выполнение правил, – это PEP по отношению к Администратору приложений.
- Сервер, обеспечивающий выполнение правил, – это PDP по отношению к CMTS.
- CMTS – это PEP по отношению к Серверу, обеспечивающему выполнение правил.

Несмотря на то, что содержание сообщений протокола COPS, требуемых для работы IP-Cablecom Multimedia, соответствует протоколу COPS, существует некоторое различие в том, как начинается сеанс связи COPS, и некоторое ослабление требований относительно порядка ответа. В документе RFC 2748 [7] сказано:

"Протокол COPS использует единственное устойчивое соединение TCP между PEP и удаленной PDP. Единственная реализация PDP на сервере ДОЛЖНА вести контрольное подслушивание хорошо известного номера порта TCP (COPS=3288 [IANA]). PEP несет ответственность за инициацию TCP соединения с PDP."

Последняя строчка в этом утверждении говорит о том, что PEP несет ответственность за инициацию TCP соединения. В модели IP-Cablecom, наоборот именно CMTS (PEP) отвечающая за назначенный порт 3918, и именно Сервер, обеспечивающий выполнение правил, ДОЛЖЕН инициировать TCP соединение с CMTS. Это – различие в моделях, описанное в RFC. Однако когда TCP соединение установлено, CMTS работает так, как это требуется клиенту, или PEP, в протоколе COPS. Аналогично, Сервер, обеспечивающий выполнение правил, (PEP) ведет контрольное подслушивание назначенного порта 3918, а Администратор приложений ДОЛЖЕН инициировать TCP соединение с Сервером, обеспечивающим выполнение правил.

Отметим, что DQoS в IP-Cablecom Multimedia и в IP-Cablecom-T DQoS ведет контрольное подслушивание различных портов, так чтобы CMTS мог бы инициировать сеанс связи COPS с правильным типом клиента.

В RFC 2748 также сказано:

"RPT сообщения, запрошенные решениями для данного Client Handle ДОЛЖНЫ устанавливать флаг Solicited Message (запрошенное сообщение) и ДОЛЖНЫ передаваться в том же порядке, в котором были приняты соответствующие им сообщения Решение".

Протокол COPS использует порядок передачи сообщений RPT и Решение для преобразования запросов в ответы. Наоборот, реализации архитектуры PacketCable Multimedia для преобразования запросов в ответы ДОЛЖНЫ использовать объект TransactionID, и им СЛЕДУЕТ передавать сообщения RPT сразу после их создания.

Подробные данные о протоколе COPS приводятся в RFC 2748. В этом документе IETF RFC содержится описание базового протокола COPS, не зависящего от типа клиента. Архитектура IP-Cablecom также соответствует IETF RFC 3084 [19]. В COPS-PR сказано:

"В COPS-PR, запросы о выполнении правил описывают PEP и ее переменные параметры (а не эксплуатационное событие). Если эти базовые параметры меняются, передается обновленный запрос. Следовательно, запросы передаются не часто. Решения не обязательно преобразуются непосредственно в запросы, и они передаются, в большинстве случаев, когда PDP отвечает на внешние события или на события PDP (обновления правил)".

Когда эта концепция переносится в архитектуру IP-Cablecom Multimedia, PEP передает на PDP запрос, определяющий Client-Handle. Эта Client-Handle затем используется во всех будущих сообщениях Decision, передаваемых от PDP на PEP. Эти сообщения Decision содержат сообщения управления шлюзом (т. е. Gate-Set, Gate-Info и Gate-Delete), определенные для типов клиента DQoS и Multimedia. Client-Handle используется для уникальной идентификации связи PDP-PEP.

В архитектуре IP-Cablecom Multimedia может существовать несколько Администраторов приложений, взаимодействующих с одним или несколькими Серверами, обеспечивающими выполнение правил. В IP-Cablecom Multimedia существует один-единственный экземпляр сеанса связи протокола COPS на одно соединение TCP; в котором сеанс связи IP-Cablecom Multimedia протокола COPS указывает на шлюз сообщения между PDP и PEP, связанный с единственным Client-Handle. Это означает, что существует одно соединение с COPS-TCP между Администратором приложений и Сервером, обеспечивающим выполнение правил. Аналогично, может существовать один или несколько Серверов, обеспечивающих выполнение правил, общающихся с одной или несколькими CMTS. Когда PEP соединена с несколькими PDP, она ДОЛЖНА обеспечить, чтобы для каждой связи использовался уникальный Client-Handle.

6.4 Форматы сообщений протокола управления шлюзом

Сообщения протокола для управления шлюзом ДОЛЖНЫ передаваться внутри сообщений протокола COPS. PDP и PEP для связи между собой ДОЛЖНЫ установить и использовать TCP соединение, а также применять механизмы, описанные в [11], для защиты маршрута передачи.

6.4.1 Общий формат сообщений протокола COPS

Каждое сообщение COPS состоит из заголовка COPS, за которым следует несколько типовых объектов. Администратор приложений, Сервер, обеспечивающий выполнение правил и CMTS ДОЛЖНЫ использовать определенный ниже Общий формат сообщений протокола COPS в качестве формата сообщений для всех обменов сообщениями. В приведенной далее спецификации объекта, каждый ряд представляет собой 4-байтовое слово, поскольку все объекты лежат внутри 4-байтовой границы.

0		1		2		3	
Версия	Флаги	Op-Code		Тип клиента			
Длина сообщения							

Версия – это 4-битовое поле, содержащее номер текущей версии COPS. Это поле ДОЛЖНО быть установлено в 1.

Флаги – это 4-битовое поле. Младший бит – это флаг запрошенного сообщения. Когда сообщение COPS передается в ответ на другое сообщение (например, запрошенное решение, переданное в ответ на запрос) этот флаг ДОЛЖЕН быть установлен в 1. В других случаях (например, незапрошенное решение) этот флаг устанавливать НЕЛЬЗЯ (значение = 0). Сохраняя соответствие с моделью DQoS, первое сообщение Decision, переданное в ответ на сообщение запроса, является запрошенным ответом и его флаг запрошенного сообщения ДОЛЖЕН быть установлен. Все остальные сообщения Decision являются незапрошенными, и их флаг запрошенного сообщения ДОЛЖЕН быть очищен. Все остальные флаги ДОЛЖНЫ быть установлены в ноль.

Op-code – это 1-байтовое целочисленное поле, которое позволяет выполнить операцию COPS. В настоящей Рекомендации по IP-Cablecom используются следующие операции COPS:

- 1 = Запрос (REQ);
- 2 = Решение (DEC);
- 3 = Отчет о состоянии (RPT);

- 4 = Удалить Отчет о состоянии (DRQ);
- 5 = Запрос о состоянии синхронизации (SSQ);
- 6 = Открыть клиента (OPN);
- 7 = Принять клиента (CAT);
- 8 = Закрывать клиента (CC);
- 9 = Сохранить действующим (KA);
- 10 = Завершение синхронизации (SSC).

Тип клиента – это 1-байтовый целочисленный (без знака) идентификатор. Для использования в IPCablecom Multimedia, Тип клиента ДОЛЖЕН быть установлен в значение клиента IPCablecom Multimedia (0x800A). Для сообщений Сохранить действующим (Op-code = 9), Тип клиента ДОЛЖЕН быть установлен в ноль, так как здесь КА используется для проверки соединения, а не для проверки сеанса связи с клиентом.

Длина сообщения – это 4-байтовая целочисленная (без знака) величина, определяющая общую длину сообщения в байтах. Сообщения ДОЛЖНЫ быть внутри 4-байтовой границы, поэтому их длина ДОЛЖНА быть кратной четырем.

После общего заголовка COPS следует один или несколько объектов. Все объекты ДОЛЖНЫ соответствовать одному и тому же формату объектов, в котором каждый объект состоит из одного или нескольких 4-байтовых слов с четырехбайтовым заголовком, следующего формата.

0	1	2	3
Длина		C-Num	C-Type
Содержание объекта			

Длина – это 2-байтовая целочисленная (без знака) величина, которая ДОЛЖНА определять число байтов (включая заголовок), составляющих объект. Если исходная длина в байтах не кратна четырем, в конец объекта ДОЛЖНО быть добавлено заполнение, так чтобы объект соответствовал границе следующих 4-байтов.

C-Num идентифицирует класс информации, содержащейся в объекте, а C-Type идентифицирует подтип или версию информации, содержащейся в объекте. В настоящей Рекомендации используются следующие стандартные объекты COPS (определенные в [7]) и их стандартные значения C-Num:

- 1 = Handle – Заголовок;
- 2 = Context – Контекст;
- 6 = Decision – Решение;
- 8 = Error – Ошибка;
- 9 = Client Specific Info – Информации о клиенте;
- 10 = Keep-Alive-Timer – Таймер сохранения действующим;
- 11 = PEP Identification – Идентификация PEP;
- 12 = Report Type – Тип отчета.

Каждый из этих объектов ДОЛЖЕН соответствовать формату и правилам, связанным с конкретным объектом, определенным в RFC 2748.

6.4.2 Дополнительные объекты COPS для контроля шлюза

Так же, как в случае с профилями COPS-PR и COPS-RSVP, Тип Клиента IPCablecom определяет некоторое количество дополнительных форматов объектов. Эти объекты ДОЛЖНЫ быть размещены внутри объекта Принятия, C-Num (Номер Клиента) = 6, C-Type (Тип Клиента) = 4 (Данные принятия, особые для Клиента) при переносе от PDP к PEP в сообщении Принятия. Они ДОЛЖНЫ быть также размещены в объекте ClientSI object, C-Num = 9, C-Type = 1 (Сигнальный ClientSI) при переносе от PEP к PDP в сообщении Отчета о Состоянии или сообщении Открытия Клиента.

Данные объекты закодированы схожим образом с объектами, особыми для клиента, для профиля COPS-PR, и так же, как в профиле COPS-PR данные объекты пронумерованы с помощью особой для клиента цифровой области, которая независима от цифровой области объекта высшего уровня COPS. По этой причине, номера и типы клиентов даются как S-Num и S-Type, соответственно. S-Num и S-Type ДОЛЖНЫ быть равны одному байту. Поле Длины COPS ДОЛЖНО быть равно двум байтам.

Дополнительные объекты COPS определены для использования мультимедийной сетью IP-Cablecom в последующих разделах.

6.4.2.1 Идентификатор Передачи

Идентификатор Передачи является 2-байтовым целым числом без знака, которое содержит метку, которую используют Менеджер приложений для согласования ответов от Сервера, обеспечивающего выполнение правил, и Сервер, обеспечивающий выполнение правил, для согласования ответов от CMTS на предыдущие запросы. Идентификатор Передачи ДОЛЖЕН содержать тип команды, который указывает на то, чтобы действие принималось или на него был получен ответ. Объект Идентификатора передачи ДОЛЖЕН соответствовать следующему формату.

Длина = 8	S-Num = 1	S-Type = 1
Идентификатор передачи		Тип команды шлюза

Идентификатор Передачи ДОЛЖЕН быть установлен равным 0, когда включается в сообщение Отчета о состоянии шлюза.

Тип Команды Шлюза является 2-байтовым целым значением без знака, которое определяют тип сообщения Контроля Шлюза и ДОЛЖНО иметь один из следующих видов:

<Reserved>	1–3
Gate-Set	4
Gate-Set-Ack	5
Gate-Set-Err	6
Gate-Info	7
Gate-Info-Ack	8
Gate-Info-Err	9
Gate-Delete	10
Gate-Delete-Ack	11
Gate-Delete-Err	12
<Reserved>	13
<Reserved>	14
Gate-Report-State	15

6.4.2.2 AMID

AMID, Идентификатор Менеджера приложений, является 4-байтовым целым значением без знака, которое назначает Менеджер приложений, ответственный за управление сеансом связи. Менеджер приложений ДОЛЖЕН включать этот объект во все сообщения, которые он направляет на Сервер, обеспечивающий выполнение правил. Сервер, обеспечивающий выполнение правил, ДОЛЖЕН включать полученный AMID во все сообщения, которые он отправляет на CMTS в ответ на сообщения, получаемые им от Менеджера приложений. CMTS ДОЛЖНА включать полученный объект AMID во все сообщения, которые она отправляет на Сервер, обеспечивающий выполнение правил, а Сервер, обеспечивающий выполнение правил, так же ДОЛЖЕН включать полученный AMID в сообщения для Менеджера приложений. Сервер, обеспечивающий выполнение правил, может использовать AMID в сообщениях от CMTS для помощи Менеджеру приложений, которому он может понадобиться для создания сообщений. Объект AMID ДОЛЖЕН соответствовать следующему формату.

Длина = 8	S-Num = 2	S-Type = 1
AMID		

6.4.2.3 Идентификатор абонента

Идентификатор абонента является 4-байтовым значением без знака, представляющим IPv4 адрес (имеющим вид 4 соединенных байтовых значений) абонента для этого запроса услуги. Данный адрес может быть фактическим IP адресом CPE устройства абонента, которое запрашивает услугу (если этот адрес является маршрутизируемым и видимым с центрального блока управления), или этот адрес может быть IP адресом Кабельного Модема, обслуживающего данного абонента (если NAT осуществляется после CM). Данный объект используется для маршрутизации сообщений Контроля Шлюза в пределах целой сети из элементов PS и CMTS. Также он может использоваться при определении и ужесточении правил для конкретных абонентов. Объект Идентификатора абонента ДОЛЖЕН соответствовать следующему формату.

Длина = 8	S-Num = 3	S-Type = 1
Идентификатор абонента (4-байтовый IPv4 адрес)		

6.4.2.4 Идентификатор шлюза

Идентификатор шлюза является 4-байтовым значением без знака, которое определяет Шлюз в соответствии с сообщениями команд, или соотносится CMTS для ответного сообщения. CMTS ДОЛЖНА гарантировать, что Идентификатор шлюза уникален. Если CMTS также поддерживает IP-Cablecom-T, НЕЛЬЗЯ, чтобы Идентификатор шлюза повторял Идентификатор шлюза, находящийся в использовании в данное время. Объект Идентификатора Шлюза ДОЛЖЕН соответствовать следующему формату.

Длина = 8	S-Num = 4	S-Type = 1
Идентификатор шлюза		

6.4.2.5 GateSpec (Спецификация Шлюза)

Спецификация Шлюза (GateSpec) назначает определенный набор признаков, относящихся к Шлюзу. Объект GateSpec ДОЛЖЕН соответствовать следующему формату.

Длина = 16		S-Num = 5	S-Type = 1
Метки	Поле DSCP/TOS	Маска DSCP/TOS	ID Класса сеанса связи
Таймер T1		Таймер T2	
Таймер T3		Таймер T4	

Метки – это однобайтовые значения битового поля, определенные следующим образом:

- Бит 0: бит направления, ДОЛЖЕН быть равным либо нулю для Шлюза нисходящего потока, либо единице для Шлюза восходящего потока.
- Бит 1: бит разрешения DSCP/TOS, ДОЛЖЕН быть равным либо нулю для запрета перезаписывания DSCP, либо единице для разрешения.
- Биты 2–7: зарезервированы, ДОЛЖНЫ быть равными нулю.

Идентификатор Класса сеанса связи является 1-байтовым целым значением без знака, которое определяет надлежащее допущение контроля правил, или параметры, которые должны быть приняты для этого Шлюза. Идентификатор Класса сеанса связи – это битовое поле, определенное следующим образом:

- Бит 0–2: Приоритет, число от 0 до 7, где 0 – это низкий приоритет, а 7 – высокий.
- Бит 3: Внеочередное занятие линии, установлено для разрешения внеочередного занятия полосы частот, назначенной для сеансов связи низкого приоритета, если необходимо (если поддерживается).
- Бит 4–7: Настраиваемый, по умолчанию равен 0.

Поле приоритета описывает относительную важность сеанса связи в сравнении с другими сеансами, созданными одной и той же PDP. PEP МОЖЕТ использовать это значение как для инструмента допущения на основе приоритета (в соединении с битом внеочередного занятия линии), так и для защиты получившегося в результате потока от перехвата линии (смотри RFC 2751 [22] "защита приоритета"). Степень детализации приоритета CMIS может быть меньше 8 доступных значений. В таком случае CMIS СЛЕДУЕТ распределить его уровни между всем спектром приоритета. К примеру, если CMIS назначает 2 уровня приоритета, тогда ей следует рассматривать значения с 0 по 3 как низкий приоритет, а значения с 4 по 7 – как высокий приоритет. Серверу, обеспечивающему выполнение правил, СЛЕДУЕТ нормализовать, или иначе трансформировать данное значение, для того чтобы обеспечить логически последовательную систему приоритетов среди Систем завершения вызова для кабельного модема (CMIS) оператора, но отвечать на любой запрос AM исходным значением приоритета.

Бит внеочередного занятия линии используется PDP для указания PEP регулировать доступ на основе приоритета. Поддержка внеочередного занятия линии является дополнительной; PEP МОЖЕТ игнорировать этот бит. Если внеочередное занятие линии не запрашивается PDP или не осуществляется PEP, тогда правило регулирования доступа будет осуществляться в порядке очереди. Если PEP решает занять линию вне очереди, она ДОЛЖНА занять емкость канала сеансов связи, чей приоритет ниже, чем приоритет данного сеанса связи, начиная с сеанса(ов) связи с самым низким приоритетом. Данный бит не используется для контроля того, какой сеанс связи допускает вытеснение; наоборот, сеанс связи, не допускающий вытеснение, запрашивается с помощью самого высокого приоритета. Если сеанс связи с более низким приоритетом прерван в результате внеочередного занятия линии, PEP ДОЛЖНА отправить сообщение Отчета о состоянии шлюза PDP вместе с объектом GateState поля Причины 1 "Закрытие инициировано CMIS вследствие переназначения резервирования" и перемещением шлюза в состояние "конца".

Менеджеры приложений, которые обеспечивают новые услуги, МОГУТ использовать Настраиваемое поле для назначения новых классов сеанса связи. Сервер, обеспечивающий выполнение правил, МОЖЕТ поддерживать настраиваемые правила на основе данного значения и МОЖЕТ перезаписывать это поле перед переадресацией данного сообщения на CMIS. CMIS МОЖЕТ обеспечивать метрику нового класса связи, используя эти биты, но значение 0 ДОЛЖНО соответствовать разумному значению по умолчанию для PDP, которое безразлично к данной метрике.

Поле DSCP/TOS – это 1-байтовое поле, определяемое следующими переменными структурами, зависящими от стратегии управления сетью. Данное поле, объединенное с 1-байтовой Маской DSCP/TOS, используется для идентификации отдельных битов в пределах байта IPv4 DSCP/TOS.

0	1	2	3	4	5	6	7
Кодовая точка дифференцированного обслуживания (DSCP)						Не используется	Не используется

0	1	2	3	4	5	6	7
Приоритет IP			IP TOS			Не используется	

Если в поле метки GateSpec установлен бит "Разрешено", тогда CMIS ДОЛЖНА пометить пакеты, пересекающиеся со значением CMIS DSCP/TOS. Если бит "Разрешено" чист, тогда НЕЛЬЗЯ, чтобы CMIS осуществляла какую-либо маркировку.

Таймеры T1, T2, T3 и T4 являются 2-байтовыми целыми числами без знака, определяемые в секундах, и ДОЛЖНЫ использоваться так, как изображено на Диаграмме Переключения Шлюза, как описывается в разделе 6.2. Значение нуля для T1 указывает на то, что обеспечиваемое значение CMIS для таймера ДОЛЖНО использоваться. T2 совпадает с Допустимым таймером DOCSIS, а T3 совпадает с Активным таймером DOCSIS. Все совпадающие требования DOCSIS применимы к данным таймерам. Особенно значение нуля для любого из этих таймеров указывает на то, что соответствующий таймер ДОЛЖЕН быть отключен.

6.4.2.6 Классификатор

Объект Классификатора определяет правила согласования пакета, связанные со Шлюзом. Как определено в разделах 6.4.3.1 и 6.4.3.2, множественные объекты Классификатора могут быть включены в сообщение Gate-Set, для того чтобы позволить общие правила классификатора. Объект Классификатора ДОЛЖЕН соответствовать следующему формату.

Длина = 24		S-Num = 6	S-Type = 1
Идентификатор Протокола		Поле DSCP/TOS	Маска DSCP/TOS
IP адрес источника (4-байтовый)			
IP адрес Точки назначения (4-байтовый)			
Порт источника		Порт точки назначения	
Приоритет	Зарезервировано		

IP адрес источника и IP адрес точки назначения ДОЛЖНЫ быть парой 4-байтовых IPv4 адресов, со значением нуля при несовпадении (т.е. определение специального символа, которое подойдет для любого пакета).

Порт источника и Порт точки назначения ДОЛЖНЫ быть парой 2-байтовых целых значений без знака, или нулем при несовпадении.

Идентификатор Протокола ДОЛЖЕН соответствовать разделу В.С.2.1.5.2 [1], или нулю при несовпадении.

Поле DSCP/TOS является 1-байтовым полем, которое ДОЛЖНО соответствовать следующим переменным структурам:

0	1	2	3	4	5	6	7
Кодовая точка дифференцированного обслуживания (DSCP)						Не используется	Разрешено

0	1	2	3	4	5	6	7
Приоритет IP			IP TOS			Разрешено	

Маска DSCP/ТО является 1-байтовым битовым полем, предоставляющим битовую маску, используемую для выбора значимых битов из сопровождающего значения поля DSCP/ТО.

Если установлен бит "Разрешено", то CMTS ДОЛЖНА использовать эти значения для создания Спектра IP TOS и поля Маски, определяемого в обмене сообщениями DSx. Если бит "Разрешено" чист, тогда CMTS ДОЛЖНА пропускать Спектр IP TOS и значение Маски в обмене сообщениями DSx и удалить байт IP TOS из процесса классификации пакета.

Приоритет является 1-байтовым полем, которое позволяет установить различия между классификаторами, которые могут перекрываться. Значение по умолчанию, равное 64, СЛЕДУЕТ использовать, если специальное значение приоритета не требуется. Для дальнейшего рассмотрения поля Приоритета, обратитесь к разделу В.С.2.1.3.5 [1].

6.4.2.7 Профили трафика

Существует три разных способа выражения профиля трафика. Профиль трафика может быть выражен через Спецификацию потока, Название Класса услуги DOCSIS или особых для DOCSIS параметров. Данные три метода различаются по разному значению S-Туре в объекте Профиля трафика (S-Num = 7). S-Туре 1-го способа указывает на то, что объект содержит Профиль трафика, определенный в формате RSVP FlowSpec. S-Туре 2-го способа указывает на то, что объект содержит Профиль трафика, определенный в формате Имени Класса Услуги DOCSIS. S-Туре 3-го способа, или больше, указывает на то, что объект содержит Профиль трафика, который определен с помощью параметров, особых для DOCSIS.

Все Профили трафика используют семантику "замещения", то есть, форматы, представленные в этом Профиле трафика, замещают все существующие оболочки, связанные со Шлюзом и соответственные с Потокном Услуг. Таким образом, все параметры профиля трафика, связанные с данным Шлюзом, ДОЛЖНЫ включаться в каждое сообщение, которое включает Профиль трафика.

Все Профили трафика имеют общее поле, известное, как Поле формата. Это поле является битовым полем, которое сообщает типы формата (т.е. Авторизовано, Зарезервировано и использования), которые присутствуют в этом объекте. Значение 1 в данном битовом поле указывает на то, что тип формата присутствует в Профиле трафика.

- Бит 0: Авторизованный формат.
- Бит 1: Зарезервированный формат.
- Бит 2: Формат использования.

Таким образом, модель бита 001 (или 0x01) указывает на присутствие только одного Авторизованного формата, в то время как значение 111 (или 0x7) указывает на присутствие всех трех форматов. Только следующие значения являются легальными: 001, 011 и 111; Поле формата ДОЛЖНО быть установлено равным одному из этих трех легальных значений. Дальнейшие ограничения в значении поля Формата могут быть функцией текущего состояния шлюза. За дальнейшей информацией обратитесь к разделу 6.2.

Для форматов Профиля трафика, которые позволяют множественные группы параметров формата, соответствие групп параметра формата проводится одним из следующих методов:

Если все типы форматов, которые указаны в Поле формата, имеют общий набор параметров формата, тогда PDP СЛЕДУЕТ удостовериться в том, что именно один набор параметров формата присутствует в этом профиле трафика. Это допускается для большинства эффективных передач и процессов Профиля трафика по всей системе.

В других обстоятельствах PDP ДОЛЖНА удостовериться, что только один набор параметров форматов включен для каждого типа формата, который указывается в Поле формата. Надлежащий порядок наборов параметров формата показан в диаграмме соответствующего сообщения в разделах 6.4.2.7.1 и с 6.4.2.7.3 по 6.4.2.7.8.

В то время как все Профили трафика заканчиваются, предоставляя QoS для сети доступа, необходимо отметить несколько тонких различий в механизмах сигнализации. Как отмечалось ранее, перевод CMTS Спецификации потока (FlowSpec) (S-Type 1) в параметры DOCSIS в целом менее эффективен, чем определение самих параметров DOCSIS. Как было сказано, определение параметров DOCSIS явно (S-Types 3-7) однако не является панацеей, QoS MIB только регистрирует информацию QoS о названных Потоках Услуг в своей Таблице Регистрации Потока услуг (ServiceFlowLogTable). Таким образом, только потоки, созданные с помощью S-Type 2, будут иметь зарегистрированную информацию в данной таблице. Иногда на это можно не обращать внимания, но при наладке аппаратуры и просто при общем оперативном отслеживании, этот нюанс будет принят во внимание операторами и поставщиками Менеджера приложений, при оценке сигнализации переменных Профиля трафика, предоставляемых в данной Рекомендации.

6.4.2.7.1 Спецификация потока

Объект Спецификации потока определяет Профиль трафика, относящийся к Шлюзу, с помощью подобной RSVP схемы. Соответствие данных параметров с параметрами DOCSIS проводится в разделе 8. Объект Спецификации потока ДОЛЖЕН отвечать следующему описанию:

Длина = 36 или 64 или 92		S-Num = 7	S-Type = 1
Формат	Номер услуги	Зарезервировано	Зарезервировано
Авторизованный Формат			
Скорость права доступа в сегменте памяти [r] (IEEE номер плавающей точки)			
Размер права доступа в сегменте памяти [b] (IEEE номер плавающей точки)			
Пиковая скорость данных (p) (IEEE номер плавающей точки)			
Минимальная управляемая единица [m] (целое число)			
Максимальный размер пакета [M] (целое число)			
Скорость [R] (IEEE номер плавающей точки)			
Ненапряженный период [S] (целое число)			
Зарезервированный формат (дополнительный)			
Скорость права доступа в сегменте памяти [r] (IEEE номер плавающей точки)			
Размер права доступа в сегменте памяти [b] (IEEE номер плавающей точки)			
Пиковая скорость данных (p) (IEEE номер плавающей точки)			
Минимальная управляемая единица [m] (целое число)			
Максимальный размер пакета [M] (целое число)			
Скорость [R] (IEEE номер плавающей точки)			
Ненапряженный период [S] (целое число)			
Формат использования (дополнительный)			
Скорость права доступа в сегменте памяти[r] (IEEE номер плавающей точки)			
Размер права доступа в сегменте памяти [b] (IEEE номер плавающей точки)			
Пиковая скорость данных (p) (IEEE номер плавающей точки)			
Минимальная управляемая единица [m] (целое число)			
Максимальный размер пакета [M] (целое число)			
Скорость [R] (IEEE номер плавающей точки)			
Ненапряженный период [S] (целое число)			

Поле Номера услуги соответствует сервисному номеру RSVP Спецификации потока как определено в [3]. Если Номер услуги установлен равным пяти, это означает услугу Управления нагрузкой, и CMTS ДОЛЖНА использовать только значения TSpec (т. е. параметры права доступа в сегменте памяти) для выполнения необходимой авторизации, резервирования и операций использования. При услуге Управления нагрузкой CMTS ДОЛЖНА игнорировать поля RSpec R и S.

Если Номер Услуги установлен равным двум, это означает Гарантированную услугу, и CMTS ДОЛЖНА использовать значения как TSpec, так и RSpec для выполнения необходимой авторизации, резервирования и операций использования.

Значения r, b, p, m, M, R, и s определяются и описываются в разделе 9.

6.4.2.7.2 Название класса услуги DOCSIS

Объект Имени Класса Услуги DOCSIS определяет Название Класса услуги с заданной конфигурацией, относящегося к Шлюзу. Объект Имени Класса Услуги DOCSIS ДОЛЖЕН отвечать следующему описанию:

Длина = 12 или 16 или 20 или 24		S-Num = 7	S-Type = 2
Формат	Зарезервировано	Зарезервировано	Зарезервировано
----- Название Класса Услуги ----- ----- -----			

Название Класса услуги ДОЛЖНО быть 2-16 байтовой строкой ASCII с завершающим нулем. (Смотри В.С.2.2.3.4 [1]). Это Название ДОЛЖНО быть заполнено нулевыми байтами для выравнивания с 4-байтовой границей.

Следует заметить, что в отличие от трафика Профиля FlowSpec, который позволяет разным параметрам соответствовать каждому формату, Трафик Профиля Имени Класса Услуги DOCSIS поддерживает различные состояния Шлюза, как указывается в Поле формата, но каждый формат определяется тем же связанным Именем Класса Услуги DOCSIS. Это позволяет проводить двухфазные операции использования, используя Имена Класса Услуг DOCSIS, но каждый Формат должен быть идентичным. Также следует заметить, что возможно изменить Название Класса Услуг DOCSIS, связанного со Шлюзом, но такое изменение применяется ко всем Форматам, связанным с данным Шлюзом.

6.4.2.7.3 Услуга "Наилучший из возможных"

Объект "Наилучший из возможных" определяет Профиль трафика, связанного со Шлюзом, с помощью схемы параметризации особого для DOCSIS восходящего потока. Объект "Наилучший из возможных" ДОЛЖЕН отвечать следующему описанию:

Длина = 32, 56 или 80		S-Num = 7	S-Type = 3
Формат	Зарезервировано	Зарезервировано	Зарезервировано
Авторизованный Формат			
Приоритет трафика	Зарезервировано		
Правило запроса передачи			
Максимальная скорость непрерывной передачи трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика		Зарезервировано	
Зарезервированный формат (дополнительно)			
Приоритет трафика	Зарезервировано		
Правило запроса передачи			
Максимальная скорость непрерывной передачи трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика		Зарезервировано	
Формат использования (дополнительно)			
Приоритет трафика	Зарезервировано		
Правило запроса передачи			
Максимальная скорость непрерывной передачи трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика		Зарезервировано	

Приоритет трафика является 1-байтовым полем, содержащим целое число без знака, определяющее относительный приоритет, заданный для Потока услуг, в сравнении с другими потоками. Данное поле полностью определено в В.С.2.2.5.1 [1]. Значение Приоритета трафика по умолчанию, равное 0, СЛЕДУЕТ использовать, если не требуется особого значения Приоритета трафика.

Правило Запроса/Передачи является 4-байтовым битовым полем, как определено в В.С.2.2.6.3 [1]. Значение по умолчанию правила Запроса/Передачи, равное 0, СЛЕДУЕТ использовать, если особое значение Правила Запроса/Передачи не требуется.

Максимальная скорость непрерывной передачи трафика является 4-байтовым полем, содержащим целое число без знака, определяющее параметр скорости, в бит/с, для лимита скорости на основе права доступа в сегменте памяти для данного Потока услуг. Это поле полностью определяется в разделе В.С.2.2.5.2 [1]. Значение 0 указывает на то, что не требуется явно усиленная Максимальная скорость непрерывной передачи. Значение по умолчанию Максимальной непрерывной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение Максимальной непрерывной скорости трафика не требуется.

Максимальная импульсная скорость трафика является 4-байтовым полем, содержащим целое число без знака, определяющее размер права доступа в сегменте памяти, в байтах, для лимита скорости на основе права доступа в сегменте памяти для этого Потока услуг. Данное поле полностью определяется в разделе В.С.2.2.5.3 [1]. Значение по умолчанию Максимальной импульсной скорости трафика, равное 3044 байта, СЛЕДУЕТ использовать, если особое значение Максимальной импульсной скорости

трафика не требуется. Значение данного параметра является неэффективным до тех пор, пока не обеспечивается значение, не равное нулю, для параметра Максимальной импульсной скорости трафика. Минимальная зарезервированная скорость трафика является 4-байтовым полем, содержащим целое число без знака, определяющее минимальную скорость, в бит/с, зарезервированную для этого Потока услуг. Данное поле полностью определяется в разделе В.С.2.2.5.4 [1]. Значение по умолчанию минимальной зарезервированной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение минимальной зарезервированной скорости трафика не требуется.

Допустимый размер пакета минимальной зарезервированной скорости трафика является 2-байтовым полем, содержащим целое число без знака, определяющее допустимый минимальный размер пакета, в байтах, для которой будет обеспечиваться Допустимый размер пакета минимальной зарезервированной скорости трафика для этого потока. Данное поле полностью определяется в разделе В.С.2.2.5.5 [1]. Значение по умолчанию Допустимого размера пакета минимальной зарезервированной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение Допустимого размера пакета минимальной зарезервированной скорости трафика не требуется. После получения значения, равного 0, CMTS ДОЛЖНА использовать свое значение по умолчанию размера, особое для инструмента, для этого параметра, не равное 0 байт.

6.4.2.7.4 Услуга опроса не в реальном времени

Объект Опроса не в реальном времени определяет Профиль трафика, связанный со Шлюзом восходящего потока, с помощью схемы параметризации, особой для DOCSIS. Объект Опроса не в реальном времени ДОЛЖЕН отвечать следующему описанию:

Длина = 36, 64 или 92		S-Num = 7	S-Type = 4
Формат	Зарезервировано	Зарезервировано	Зарезервировано
Авторизованный Формат			
Приоритет трафика	Зарезервировано		
Правило запроса передачи			
Максимальная скорость непрерывной передачи трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика	Зарезервировано		
Номинальный интервал опроса			
Зарезервированный формат (дополнительно)			
Приоритет трафика	Зарезервировано		
Правило запроса передачи			
Максимальная скорость непрерывной передачи трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика	Зарезервировано		
Номинальный интервал опроса			
Формат использования (дополнительно)			
Приоритет трафика	Зарезервировано		
Правило запроса передачи			
Максимальная скорость непрерывной передачи трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика	Зарезервировано		
Номинальный интервал опроса			

Приоритет трафика является 1-байтовым полем, содержащим целое число без знака, определяющее относительный приоритет, заданный для Потока услуг, в сравнении с другими потоками. Данное поле полностью определено в В.С.2.2.5.1 [1]. Значение по умолчанию Приоритета трафика, равное 0, СЛЕДУЕТ использовать, если особое значение Приоритета трафика не требуется.

Правило Запроса/Передачи является 4-байтовым битовым полем, как определяется в разделе В.С.2.2.6.3 [1].

ПРИМЕЧАНИЕ. – Для данного Типа планирования потока услуг не существует значения по умолчанию для Правила Запроса/Передачи, и все значения (включая 0) имеют значение в DOCSIS.

Максимальная скорость непрерывной передачи трафика является 4-байтовым полем, содержащим целое число без знака, определяющее параметр скорости, в бит/с, для ограничения скорости на основе права доступа в сегменте памяти для данного Потока услуг. Это поле полностью определяется в разделе В.С.2.2.5.2 [1]. Значение 0 указывает на то, что не требуется явно усиленная Максимальная скорость непрерывной передачи. Значение по умолчанию Максимальной непрерывной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение Максимальной непрерывной скорости трафика не требуется.

Максимальная импульсная скорость трафика является 4-байтовым полем, содержащим целое число без знака, определяющее размер права доступа в сегменте памяти, в байтах, для лимита скорости на основе права доступа в сегменте памяти для этого Потока услуг. Данное поле полностью определяется в разделе В.С.2.2.5.3 [1]. Значение по умолчанию Максимальной импульсной скорости трафика, равное 3044 байтов, СЛЕДУЕТ использовать, если особое значение Максимальной импульсной скорости трафика не требуется. Значение данного параметра является неэффективным до тех пор, пока не обеспечивается значение, не равное нулю, для параметра Максимальной импульсной скорости трафика.

Минимальная зарезервированная скорость трафика является 4-байтовым полем, содержащим целое число без знака, определяющее минимальную скорость, в бит/с, зарезервированную для этого Потока услуг. Данное поле полностью определяется в разделе В.С.2.2.5.4 [1]. Значение по умолчанию минимальной зарезервированной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение минимальной зарезервированной скорости трафика не требуется.

Допустимый размер пакета минимальной зарезервированной скорости трафика является 2-байтовым полем, содержащим целое число без знака, определяющее допустимый минимальный размер пакета, в байтах, для которой будет обеспечиваться Допустимый размер пакета минимальной зарезервированной скорости трафика для этого потока. Данное поле полностью определяется в разделе В.С.2.2.5.5 [1]. Значение по умолчанию Допустимого размера пакета минимальной зарезервированной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение Допустимого размера пакета минимальной зарезервированной скорости трафика не требуется. После получения значения, равного 0, CMTS ДОЛЖНА использовать свое значение по умолчанию размера, особое для инструмента, для этого параметра, не равное 0 байт.

Номинальный интервал опроса является 4-байтовым полем, содержащим целое число без знака, определяющее номинальный интервал (в микросекундах) между возможностями запроса успешной однонаправленной передачи для данного Потока услуг на восходящем канале. Это поле полностью определяется в разделе В.С.2.2.6.4 [1]. Значение по умолчанию Номинального Интервала опроса, равное 0, СЛЕДУЕТ использовать, если особое значение Номинального интервала опроса не требуется. После получения значения, равного 0, CMTS ДОЛЖНА использовать свое значение по умолчанию размера, особое для инструмента, для этого параметра, не равное 0 микросекунд.

6.4.2.7.5 Услуга опроса в реальном времени

Объект Опроса в реальном времени определяет Профиль трафика, связанный со Шлюзом восходящего потока, с помощью схемы параметризации, особой для DOCSIS. Объект Опроса в реальном времени ДОЛЖЕН отвечать следующему описанию:

Длина = 36, 64 или 92		S-Num = 7	S-Type = 5
Формат	Зарезервировано	Зарезервировано	Зарезервировано
Авторизованный формат			
Правило запроса передачи			
Максимальная поддерживаемая скорость трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика		Зарезервировано	
Номинальный интервал опроса			
Допустимый уровень неустойчивой синхронизации опроса			
Зарезервированный формат (дополнительно)			
Правило запроса передачи			
Максимальная поддерживаемая скорость трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика		Зарезервировано	
Номинальный интервал опроса			
Допустимый уровень неустойчивой синхронизации опроса			
Формат использования (дополнительно)			
Правило запроса передачи			
Максимальная непрерывная скорость трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика		Зарезервировано	
Номинальный интервал опроса			
Допустимый уровень неустойчивой синхронизации опроса			

Правило Запроса/Передачи является 4-байтовым битовым полем, как определяется в разделе В.С.2.2.6.3 [1].

ПРИМЕЧАНИЕ. – Для данного Типа планирования потока услуг не существует значения по умолчанию для Правила Запроса/Передачи, и все значения (включая 0) имеют значение в DOCSIS.

Максимальная скорость непрерывной передачи трафика является 4-байтовым полем, содержащим целое число без знака, определяющее параметр скорости, в бит/с, для лимита скорости на основе права доступа в сегменте памяти для данного Потока услуг. Это поле полностью определяется в разделе В.С.2.2.5.2 [1]. Значение 0 указывает на то, что не требуется явно усиленная Максимальная скорость непрерывной передачи. Значение по умолчанию Максимальной непрерывной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение Максимальной непрерывной скорости трафика не требуется.

Максимальная импульсная скорость трафика является 4-байтовым полем, содержащим целое число без знака, определяющее размер права доступа в сегменте памяти, в байтах, для лимита скорости на основе права доступа в сегменте памяти для этого Потока услуг. Данное поле полностью определяется в разделе В.С.2.2.5.3 [1]. Значение по умолчанию Максимальной импульсной скорости трафика, равное

3044 байта, СЛЕДУЕТ использовать, если особое значение Максимальной импульсной скорости трафика не требуется. Значение данного параметра является неэффективным до тех пор, пока не обеспечивается значение, не равное нулю, для параметра Максимальной импульсной скорости трафика.

Минимальная зарезервированная скорость трафика является 4-байтовым полем, содержащим целое число без знака, определяющее минимальную скорость, в бит/с, зарезервированную для этого Потока услуг. Данное поле полностью определяется в разделе В.С.2.2.5.4 [1]. Значение по умолчанию минимальной зарезервированной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение минимальной зарезервированной скорости трафика не требуется.

Допустимый размер пакета минимальной зарезервированной скорости трафика является 2-байтовым полем, содержащим целое число без знака, определяющее допустимый минимальный размер пакета, в байтах, для которой будет обеспечиваться Допустимый размер пакета минимальной зарезервированной скорости трафика для этого потока. Данное поле полностью определяется в разделе В.С.2.2.5.5 [1]. Значение по умолчанию Допустимого размера пакета минимальной зарезервированной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение Допустимого размера пакета минимальной зарезервированной скорости трафика не требуется. После получения значения, равного 0, СМТС ДОЛЖНА использовать свое значение по умолчанию размера, особое для инструмента, для этого параметра, не равное 0 байт.

Номинальный интервал опроса является 4-байтовым полем, содержащим целое число без знака, определяющее номинальный интервал (в микросекундах) между возможностями запроса успешной однонаправленной передачи для данного Потока услуг на восходящем канале. Это поле полностью определяется в разделе В.С.2.2.6.4 [1]. Для данного Типа планирования потока услуг не существует значения по умолчанию для Номинального Интервала Опроса.

Допустимый уровень неустойчивой синхронизации опроса является 4-байтовым полем, содержащим целое число без знака, определяющее максимальный промежуток времени, на который интервал запроса однонаправленной передачи может быть отложен от номинального периодического расписания (измеряемого в микросекундах). Это поле полностью определяется в разделе В.С.2.2.6.5 [1]. Значение по умолчанию Допустимого уровня неустойчивой синхронизации опроса, равное 0, СЛЕДУЕТ использовать, если особое значение Допустимого уровня неустойчивой синхронизации опроса не требуется. После получения значения, равного 0, СМТС ДОЛЖНА использовать свое значение по умолчанию размера, особое для инструмента, для этого параметра, не равное 0 микросекунд.

6.4.2.7.6 Услуга Услуги без запроса разрешения

Объект Услуги без запроса разрешения определяет Профиль трафика, связанного со Шлюзом восходящего потока, с помощью схемы параметризации, особой для DOCSIS. Объект Услуги без запроса разрешения ДОЛЖЕН отвечать следующему описанию:

Длина = 24, 40, или 56		S-Num = 7	S-Type = 6
Формат	Зарезервировано	Зарезервировано	Зарезервировано
Авторизованный Формат			
Правило запроса передачи			
Размер Услуги без запроса разрешения		Сигналы/Интервал	Зарезервировано
Номинальный интервал разрешающего сигнала			
Допустимый уровень неустойчивой синхронизации разрешающего сигнала			
Зарезервированный формат (дополнительно)			
Правило запроса передачи			
Размер Услуги без запроса разрешения		Сигналы/Интервал	Зарезервировано
Номинальный Интервал разрешающего сигнала			
Допустимый Уровень неустойчивой синхронизации разрешающего сигнала			
Формат использования (дополнительный)			
Правило запроса передачи			
Размер Услуги без запроса разрешения		Сигналы/Интервал	Зарезервировано
Номинальный Интервал разрешающего сигнала			
Допустимый Уровень неустойчивой синхронизации разрешающего сигнала			

Правило Запроса/Передачи является 4-байтовым битовым полем, как определено в разделе В.С.2.2.6.3 [1].

ПРИМЕЧАНИЕ. – Для данного Типа планирования потока услуг не существует значения по умолчанию для Правила Запроса/Передачи, и все значения (включая 0) имеют значение в DOCSIS.

Размер Услуги без запроса разрешения является 2-байтовым полем, содержащим целое число без знака, определяющее размер непредусмотренного сигнала (в байтах) как определено в разделе В.С.2.2.6.6 [1]. Не существует значения по умолчанию для Размера Услуги без запроса разрешения.

Число Разрешающих сигналов за Интервал является полем, содержащим целое число без знака, определяющее число разрешающих сигналов за Номинальный Интервал разрешающих сигналов как указано в разделе В.С.2.2.6.9 [1]. Не существует значения по умолчанию для Числа Разрешающих сигналов за Интервал, но рекомендуется значение, равное 1.

Номинальный Интервал разрешающих сигналов является 4-байтовым полем, содержащим целое число без знака, определяющее номинальное время между возможностями успешного непредусмотренного сигнала данных для данного Потока услуг (в микросекундах) как определено в разделе В.С.2.2.6.7 [1]. Не существует значения по умолчанию для Номинального интервала разрешающих сигналов.

Допустимый Уровень неустойчивой синхронизации разрешающего сигнала является 4-байтовым полем, содержащим целое число без знака, определяющее максимальный интервал времени, на который возможность передачи может быть отложена от номинального периодического расписания (в микросекундах) как определено в разделе В.С.2.2.6.8 [1]. Не существует значения по умолчанию для Допустимого Уровня неустойчивой синхронизации разрешающего сигнала.

6.4.2.7.7 Услуга Услуги без запроса разрешения с определением активности

Объект Услуги без запроса разрешения с определением активности определяет Профиль трафика, связанного со Шлюзом восходящего потока, с помощью схемы параметризации, особой для DOCSIS. Объект Услуги без запроса разрешения ДОЛЖЕН отвечать следующему описанию:

Длина = 32, 56 or 80		S-Num = 7	S-Type = 7
Формат	Зарезервировано	Зарезервировано	Зарезервировано
Авторизованный Формат			
Правило запроса передачи			
Размер Услуги без запроса разрешения		Сигналы/Интервал	Зарезервировано
Номинальный Интервал разрешающего сигнала			
Допустимый Уровень неустойчивой синхронизации разрешающего сигнала			
Номинальный интервал опроса			
Допустимый Уровень неустойчивой синхронизации опроса			
Зарезервированный формат (дополнительно)			
Правило запроса передачи			
Размер Услуги без запроса разрешения		Сигналы/Интервал	Зарезервировано
Номинальный Интервал разрешающего сигнала			
Допустимый Уровень неустойчивой синхронизации разрешающего сигнала			
Номинальный интервал опроса			
Допустимый Уровень неустойчивой синхронизации опроса			
Формат использования (дополнительно)			
Правило запроса передачи			
Размер Услуги без запроса разрешения		Сигналы/Интервал	Зарезервировано
Номинальный Интервал разрешающего сигнала			
Допустимый Уровень неустойчивой синхронизации разрешающего сигнала			
Номинальный интервал опроса			
Допустимый Уровень неустойчивой синхронизации опроса			

Правило Запроса/Передачи является 4-байтовым битовым полем, как определено в разделе В.С.2.2.6.3 [1].

ПРИМЕЧАНИЕ. – Для данного Типа планирования потока услуг не существует значения по умолчанию для Правила Запроса/Передачи, и все значения (включая 0) имеют значение в DOCSIS.

Размер Услуги без запроса разрешения является 2-байтовым полем, содержащим целое число без знака, определяющее размер непредусмотренного сигнала (в байтах) как определено в разделе В.С.2.2.6.6 [1]. Не существует значения по умолчанию для Размера Услуги без запроса разрешения.

Число Разрешающих сигналов за Интервал является полем, содержащим целое число без знака, определяющее число разрешающих сигналов за Номинальный Интервал разрешающих сигналов как указано в разделе В.С.2.2.6.9 [1]. Не существует значения по умолчанию для Числа Разрешающих сигналов за Интервал, но рекомендуется значение, равное 1.

Номинальный Интервал разрешающих сигналов является 4-байтовым полем, содержащим целое число без знака, определяющее номинальное время между возможностями успешного непредусмотренного сигнала данных для данного Потока услуг (в микросекундах) как определено в разделе В.С.2.2.6.7 [1]. Не существует значения по умолчанию для Номинального интервала разрешающих сигналов.

Допустимый Уровень неустойчивой синхронизации разрешающего сигнала является 4-байтовым полем, содержащим целое число без знака, определяющее максимальный интервал времени, на который возможность передачи может быть отложена от номинального периодического расписания (в микросекундах) как определено в разделе В.С.2.2.6.8 [1]. Не существует значения по умолчанию для Допустимого Уровня неустойчивой синхронизации разрешающего сигнала.

Номинальный интервал опроса является 4-байтовым полем, содержащим целое число без знака, определяющее номинальный интервал (в микросекундах) между возможностями запроса успешной однонаправленной передачи для данного Потока услуг на восходящем канале. Это поле полностью определяется в разделе В.С.2.2.6.4 [1]. Для данного Типа планирования потока услуг не существует значения по умолчанию для Номинального Интервала Опроса.

Допустимый уровень неустойчивой синхронизации опроса является 4-байтовым полем, содержащим целое число без знака, определяющее максимальный промежуток времени, на который интервал запроса однонаправленной передачи может быть отложен от номинального периодического расписания (измеряемого в микросекундах). Это поле полностью определяется в разделе В.С.2.2.6.5 [1]. Значение по умолчанию Допустимого уровня неустойчивой синхронизации опроса, равное 0, СЛЕДУЕТ использовать, если особое значение Допустимого уровня неустойчивой синхронизации опроса не требуется. После получения значения, равного 0, CMTS ДОЛЖНА использовать свое значение по умолчанию размера, особое для инструмента, для этого параметра, не равное 0 микросекунд.

6.4.2.7.8 Услуга нисходящего потока

Объект нисходящего потока определяет Профиль трафика, связанного со Шлюзом нисходящего потока, с помощью схемы параметризации, особой для DOCSIS. Объект нисходящего потока ДОЛЖЕН отвечать следующему описанию:

Длина = 32, 56 или 80		S-Num = 7	S-Type = 8
Формат	Зарезервировано	Зарезервировано	Зарезервировано
Авторизованный Формат			
Приоритет трафика	Зарезервировано		
Максимальная непрерывная скорость трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика		Зарезервировано	
Максимальное время ожидания нисходящего потока данных			
Зарезервированный формат (дополнительно)			
Приоритет трафика	Зарезервировано		
Максимальная непрерывная скорость трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика		Зарезервировано	
Максимальное время ожидания нисходящего потока данных			
Формат использования (дополнительно)			
Приоритет трафика	Зарезервировано		
Максимальная непрерывная скорость трафика			
Максимальная импульсная скорость трафика			
Минимальная зарезервированная скорость трафика			
Допустимый размер пакета минимальной зарезервированной скорости трафика		Зарезервировано	
Максимальное время ожидания нисходящего потока данных			

Приоритет трафика является 1-байтовым полем, содержащим целое число без знака, определяющее относительный приоритет, заданный для Потока услуг, в сравнении с другими потоками. Данное поле полностью определено в В.С.2.2.5.1 [1]. Значение по умолчанию Приоритета трафика, равное 0, СЛЕДУЕТ использовать, если особое значение Приоритета трафика не требуется.

Максимальная скорость непрерывной передачи трафика является 4-байтовым полем, содержащим целое число без знака, определяющее параметр скорости, в бит/с, для лимита скорости на основе права доступа в сегменте памяти для данного Потока услуг. Это поле полностью определяется в разделе В.С.2.2.5.2 [1]. Значение 0 указывает на то, что не требуется явно усиленная Максимальная скорость непрерывной передачи. Значение по умолчанию Максимальной непрерывной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение Максимальной непрерывной скорости трафика не требуется.

Максимальная импульсная скорость трафика является 4-байтовым полем, содержащим целое число без знака, определяющее размер права доступа в сегменте памяти, в байтах, для лимита скорости на основе права доступа в сегменте памяти для этого Потока услуг. Данное поле полностью определяется в разделе В.С.2.2.5.3 [1]. Значение по умолчанию Максимальной импульсной скорости трафика, равное 3044 байта, СЛЕДУЕТ использовать, если особое значение Максимальной импульсной скорости трафика не требуется. Значение данного параметра является неэффективным до тех пор, пока не обеспечивается значение, не равное нулю, для параметра Максимальной импульсной скорости трафика.

Минимальная зарезервированная скорость трафика является 4-байтовым полем, содержащим целое число без знака, определяющее минимальную скорость, в бит/с, зарезервированную для этого Потока услуг. Данное поле полностью определяется в разделе В.С.2.2.5.4 [1]. Значение по умолчанию

минимальной зарезервированной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение минимальной зарезервированной скорости трафика не требуется.

Допустимый размер пакета минимальной зарезервированной скорости трафика является 2-байтовым полем, содержащим целое число без знака, определяющее допустимый минимальный размер пакета, в байтах, для которой будет обеспечиваться Допустимый размер пакета минимальной зарезервированной скорости трафика для этого потока. Данное поле полностью определяется в разделе В.С.2.2.5.5 [1]. Значение по умолчанию Допустимого размера пакета минимальной зарезервированной скорости трафика, равное 0, СЛЕДУЕТ использовать, если особое значение Допустимого размера пакета минимальной зарезервированной скорости трафика не требуется. После получения значения, равного 0, СМТS ДОЛЖНА использовать свое значение по умолчанию размера, особое для инструмента, для этого параметра, не равное 0 байт.

Максимальное время ожидания Нисходящего потока данных является 4-байтовым полем, содержащим целое число без знака, определяющее максимальное время ожидания между получением пакета NSI Системой завершения вызова кабельного модема (СМТS) и переадресацией пакета РЧ(RF) интерфейсу как определено в разделе В.С.2.2.7.1 1]. Значение по умолчанию Максимального времени ожидания Нисходящего потока данных, равное 0, СЛЕДУЕТ использовать, если особое значение Максимального времени ожидания Нисходящего потока данных не требуется. После получения значения, равного нулю, НЕЛЬЗЯ чтобы СМТS включала данный параметр в свою сигнализацию DOCSIS для этого Потока услуг.

6.4.2.8 Информация о создании события

Объект Информации о создании события содержит всю информацию, необходимую для поддержки сообщений о событии, как определено и требуется в МСЭ-Т Рек. J.164. Объект Информации о создании события ДОЛЖЕН отвечать следующему описанию:

Длина = 44	S-Num = 8	S-Type = 1
IP адрес первичного Сервера регистрации (4-байтовый)		
Порт первичного Сервера регистрации	Зарезервировано	
IP адрес вторичного Сервера регистрации (4-байтовый)		
Порт вторичного Сервера Регистрации	Зарезервировано	
Идентификатор Корреляции биллинга (24-байтовый)		

IP адрес первичного Сервера регистрации является 4-байтовым полем, которое ДОЛЖНО содержать IPv4 адрес первичного RKS, на который должны отсылаться записи о событии.

Поле Порта первичного Сервера регистрации является 2-байтовым целым числом без знака, которое ДОЛЖНО содержать номер порта на первичном RKS, куда должны отсылаться записи о событии.

IP адрес вторичного Сервера регистрации является 4-байтовым полем, которое ДОЛЖНО содержать IPv4 адрес вторичного RKS, на который должны отправляться записи, если первичный RKS недоступен.

Порт вторичного Сервера регистрации является 2-байтовым целым числом без знака, которое ДОЛЖНО содержать номер порта на вторичном RKS, куда должны отсылаться записи о событии.

Идентификатор Корреляции Биллинга является 24-байтовым полем, которое ДОЛЖНО содержать идентификатор, заданным Менеджером приложений (AM) или PS для всех записей, связанных с данным сеансом связи. Смотри [10] для определения и формата данного признака.

6.4.2.9 Лимит использования по объему

Объект Лимита использования по объему определяет количество данных, которые могут быть переданы через этот Шлюз прежде, чем встретится с ограничением объема. Данный объект является ДОПОЛНИТЕЛЬНЫМ в сообщении Gate-Set и Gate-Info-Ack. Его НЕЛЬЗЯ использовать в любых других сообщениях. Объект Лимита использования по объему ДОЛЖЕН отвечать следующему описанию:

Длина = 12	S-Num = 9	S-Type = 1
Лимит использования		

Лимит использования является 8-байтовым целым числом без знака, определяемым в килобайтах. Значение нуля указывает на то, что предел объема не назначен. Байты, учитываемые в лимите, берутся из байта после DOCSIS MAC заголовка HCS до конца циклического контроля избыточности для всех пакетов, переданных через Поток услуг, связанного с данным Шлюзом.

6.4.2.10 Лимит использования по времени

Объект Лимита использования по времени определяет интервал времени, в который Шлюз может оставаться подключенным прежде, чем встретится с ограничением времени. Объект Лимита использования по времени ДОЛЖЕН отвечать следующему описанию:

Длина = 8	S-Num = 10	S-Type = 1
Лимит Времени		

Лимит Времени является 4-байтовым целым числом без знака, определяемым в секундах. Это – лимит интервала времени, в течение которого Шлюз может находиться в состоянии подключения. Данный объект является ДОПОЛНИТЕЛЬНЫМ в сообщении Gate-Set. Если он включается в сообщение Gate-Set, тогда данный объект ДОЛЖЕН храниться Системой завершения вызова для кабельного модема (CMTS) и предоставляться в ответ на любые последующие запросы Шлюза. Вместе с тем, что от Менеджера приложений ТРЕБУЕТСЯ удалить шлюзы, связанные с сеансами медиа-связи, время которых превысило Лимит использования по времени, CMTS или Сервер, обеспечивающий выполнение правил, МОГУТ также запрашивать этот объект, как часть механизма восстановления при ошибке или другого механизма.

Значение нуля указывает на то, что не существует предела времени для соответствующего Шлюза.

6.4.2.11 Скрытые данные

Объект Скрытых Данных содержит информацию, которую Сервер, обеспечивающий выполнение правил, или Менеджер приложений МОЖЕТ хранить на CMTS, и которая остается скрытой для CMTS. Объект скрытых данных является ДОПОЛНИТЕЛЬНЫМ в сообщении Gate-Set. Его НЕЛЬЗЯ использовать в любых других сообщениях, создаваемых PDP для PER. Если этот объект присутствует, тогда CMTS ДОЛЖНА хранить Скрытые Данные локально и включать их во все сообщения, которые они создают для Сервера, обеспечивающего выполнение правил, соответствующего Шлюзу.

Если объект Скрытых Данных включен в сообщение Gate-Set от Менеджера приложений к Серверу, обеспечивающему выполнение правил, Сервер, выполняющий выполнение правил, ДОЛЖЕН перенаправить данный объект CMTS. Длина Скрытых Данных фиксируется в 8 байтах.

Длина = 12	S-Num = 11	S-Type = 1
Скрытые Данные		

6.4.2.12 Информация о времени использования Шлюза

Объект Информации о времени использования Шлюза содержит весь интервал времени, в который Шлюз был в состоянии использования и Восстановления использования. Данный счетчик ДОЛЖЕН быть остановлен после перехода Шлюза из состояния использования, либо Восстановления использования в состояние либо Резервирования, либо Авторизации. Если Шлюз впоследствии возвращается в состояние использования, данный счетчик ДОЛЖЕН быть запущен заново с места, где он был остановлен, т.е. где перешел из состояния использования или Восстановления использования. Объект Информации о времени использования Шлюза ДОЛЖЕН соответствовать следующему описанию:

Длина = 8	S-Num = 12	S-Type = 1
Время использования		

Время использования является 4-байтовым целым числом без знака, обозначающим количество секунд, в течение которых данный Шлюз был либо в состоянии использования, либо в состоянии Восстановления использования.

ПРИМЕЧАНИЕ. – Предполагается, что это будет идентичным документам QoS Активного времени Потока Информации из раздела MIB [17].

6.4.2.13 Информация об использовании Шлюза

Объект Информации об Использовании Шлюза содержит счетчик, указывающий число килобайтов, переданных через данный Шлюз. Объект Информации об Использовании Шлюза ДОЛЖЕН соответствовать следующему описанию:

Длина = 12	S-Num = 13	S-Type = 1
Счетчик Байтов		

Счетчик Байт является 4-байтовым целым числом без знака, которое представляет собой число байтов (сочтенных от DOCSIS MAC Заголовка HCS до окончания CRC), которые прошли Поток услуг, связанный со Шлюзом, в единицах учета, равных 1024 байтам.

6.4.2.14 Ошибка сети IPCablecom

Объект Ошибки сети The IPCablecom содержит информацию о типе ошибки, которая случилась. Эта ошибка создается в ответ на команду Контроля Шлюза и содержит Gate-Set-Err, Gate-Info-Err и Gate-Delete-Err сообщения. Объект Ошибки сети IPCablecom ДОЛЖЕН соответствовать следующему описанию:

Длина = 8	S-Num = 14	S-Type = 1
Код Ошибки	Внутренний код Ошибки	

Код Ошибки является 2-байтовым целым числом без знака, которое представляет собой особую ошибку и ДОЛЖНА иметь один из следующих видов:

- 1 = Недостаток Ресурсов;
- 2 = Неизвестный идентификатор шлюза;
- 6 = Отсутствующий Объект Запроса;
- 7 = Недопустимый Объект;
- 8 = Достигнут Предел использования по объему;
- 9 = Достигнут Предел использования по времени;
- 10 = Достигнут Предел Класса сеанса связи;
- 11 = Неопределенное Название Класса Услуги;

- 12 = Несовместимый Формат;
- 13 = Недопустимый Идентификатор Абонента;
- 14 = Неавторизованный AMID;
- 15 = Неподдерживаемое Число Классификаторов;
- 127 = Другая, Неопределенная Ошибка.

Внутренний Код Ошибки является 2-байтовым полем, содержащим целое число без знака, используемым для предоставления дальнейшей информации об ошибке. В случае Ошибок с кодом 6 и 7, данное 16-битное поле ДОЛЖНО содержать, как 2 8-битных значения S-Num и S-Type отсутствующего объекта, или объекта с ошибкой. Порядок значений S-Num и S-Type внутри Внутреннего Кода Ошибки ДОЛЖЕН быть таким же, как и в исходном сообщении. В случаях, когда существуют множественные возможные альтернативы для S-Type отсутствующего объекта, эта часть Внутреннего Кода Ошибки ДОЛЖНА быть установлена равной нулю. В случае Ошибки с номером 15, поле Внутреннего Кода Ошибки ДОЛЖНО содержать число Классификаторов, поддерживаемых Шлюзом.

Ошибки с кодом 8,9 и 10 создаются в результате невозможности для Запроса Правила удовлетворить требования авторизации Сервера, обеспечивающего выполнение правил. Когда Менеджер приложений создает сообщение Gate-Set с лимитом по объему или времени для Сервера, обеспечивающего выполнение правил, Сервер, обеспечивающий выполнение правил, ДОЛЖЕН отклонить запрос на основе правил, установленных на Сервере, обеспечивающем выполнение правил. Например, такое правило может утверждать, что если запрос лимита объема достигнет максимального значения, Сервер, обеспечивающий выполнение правил, должен отклонить данный запрос.

6.4.2.15 Состояние Шлюза

Информация в объекте Состояния Шлюза отражает текущее состояние Шлюза. CMTS ДОЛЖНА включать объект Состояния Шлюза во все непредусмотренные сообщения, которые она отправляет на Сервер, обеспечивающий выполнение правил. Сервер, обеспечивающий выполнение правил, может использовать данную информацию для отчета о состоянии Менеджеру приложений, или для усиленных общих правил, которые могут потребовать знания о состоянии Шлюза.

Типично, Сервер, обеспечивающий выполнение правил, знает о переменах состояния, так как он обычно обеспечивает стимул для таких перемен для CMTS, но в некоторых случаях Шлюз может переходить из одного состояния в другое локально на CMTS без привлечения Сервера, обеспечивающего выполнение правил. В таких случаях CMTS ДОЛЖНА отчитываться о смене состояния перед Сервером, обеспечивающим выполнение правил, путем непредусмотренных сообщений Gate-Report-State. При создании сообщений Gate-Report-State PEP ДОЛЖНА удостовериться, что Запрошенная Метка в заголовке COPS сообщения очищена, и Тип Отчета в заголовке установлен как Учитывающий. Объект Состояния Шлюза ДОЛЖЕН соответствовать следующему описанию:

Длина = 8	S-Num = 15	S-Type = 1
Состояние	Причина	

Состояние является 2-байтовым полем, содержащим целое число без знака, которое ДОЛЖНО отражать одно из следующих состояний:

- 1 = Бездействующее/Закрыто;
- 2 = Авторизовано;
- 3 = Зарезервировано;
- 4 = Используется;
- 5 = Восстановление использования.

Причина является 2-байтовым полем, содержащим целое число без знака, которое ДОЛЖНО отражать одну из следующих причин для данного обновления:

- 1 = Закрытие инициировано CMTS вследствие переназначения резервирования;
- 2 = Закрытие инициировано CMTS вследствие отсутствия ответа DOCSIS MAC-слоя;
- 3 = Закрытие инициировано CMTS вследствие окончания времени на таймере T1;

- 4 = Закрытие инициировано CMTS вследствие окончания времени на таймере T2;
- 5 = Время таймера неактивности закончилось вследствие неактивности Потока услуг (окончание таймера T3);
- 6 = Закрытие инициировано CMTS вследствие отсутствия Поддержки Резервирования;
- 7 = Состояние шлюза не изменилось, но лимит объема достигнут;
- 8 = Закрытие инициировано CMTS вследствие окончания времени на таймере T4;
- 9 = Состояние Шлюза не изменилось, но окончание времени на таймере T2 вызвало снижение резервирования;
- 65535 = Другое.

6.4.2.16 Информация о версии

Объект Информации о Версии используется с целью активировать приложения, чтобы применить их взаимодействие с другими устройствами так, что может быть достигнуто взаимодействие между продуктами, поддерживающими разные версии протокола. Как Старшая, так и Младшая Версия являются 2-байтовыми целыми числами без знака. Как PDP, так и PEP должны включать в себя данный объект, как указывается в разделе 6.5.1.

Длина = 8	S-Num = 16	S-Type = 1
Номер Старшей Версии	Номер Младшей Версии	

6.4.3 Сообщения контроля шлюза

Существуют два отдельных профиля для сообщений Контроля Шлюза: один для обмена сообщениями между Менеджером приложений и Сервером, обеспечивающим выполнение правил, и другой для сообщений между Сервером, обеспечивающим выполнение правил, и CMTS. Хотя и похожие друг на друга, эти два профиля имеют несколько мелких различий.

Следующие формулировки описывают форматы сообщений РСММ, захватывая как объекты COPS, так и РСММ. Данные формулировки определяют содержание сообщений, но не содержат в себе точной классификации объектов в пределах каждого сообщения. В частности любое упорядочение объектов РСММ ДОЛЖНО приниматься как действующее (и может создаваться), а порядок объектов COPS ДОЛЖЕН быть таким, как указано в RFC 2748. Следует заметить, что поскольку объекты РСММ существуют только внутри объектов COPS, различие между этими двумя наборами очевидно. Данная модель сдерживания также гарантирует, что не существует выпусков со схожим порядком объектов COPS и РСММ.

6.4.3.1 Профиль для Менеджера приложений для интерфейса сервера, обеспечивающего выполнение правил

Сообщение, которые осуществляют контроль шлюза между Менеджером приложений и Сервером, обеспечивающим выполнение правил, определены и ДОЛЖНЫ форматироваться следующим образом.

Следует заметить, что сообщение от Менеджера приложений к Серверу, обеспечивающему выполнение правил, ДОЛЖНЫ форматироваться как сообщения Решения COPS, а сообщения от Сервера, обеспечивающего выполнение правил, к Менеджеру приложений ДОЛЖНЫ форматироваться как сообщения Отчета о Состоянии COPS.

```

<Client Open> = <COPS Common Header> <COPS PEPID> <ClientSI Info>
( <Открытие Клиента> = <Общий Заголовок COPS> <COPS PEPID> <Информация о ClientSI> )
<ClientSI Info> = <COPS Client SI Header> <MM Version Info>
( <Информация ClientSI> = <Заголовок Клиента SI COPS> <Информация о Версии MM> )
<Gate Control Command> = <COPS Common Header> <Client Handle> <Context>
<Decision Flags> <ClientSI Data>
( <Команда Контроля Шлюза> = <Общий Заголовок COPS> <Описатель клиента> <Контекст>
  <Метки Решения> <Данные ClientSI> )
<ClientSI Data> ( <Данные ClientSI> ) = <Gate-Set> | <Gate-Info> | <Gate-Delete>
<Gate Control Response> = <COPS Common Header> <Client Handle> <Report Type>
<ClientSI Object>
( <Ответ Контроля Шлюза> = <Общий Заголовок COPS> <Описатель клиента> <Тип Отчета>
  <Объект ClientSI> )

```

<ClientSI Object> = <Gate-Set-Ack> | <Gate-Set-Err> | <Gate-Info-Ack> | <Gate-Info-Err> | <Gate-Delete-Ack> | <Gate-Delete-Err> | <Gate-State-Report>

<Gate-Set> = <Decision Header> <TransactionID> <AMID> <SubscriberID> [<GateID>]
 <GateSpec> <Traffic Profile> <Classifier> [<Classifier>]
 [<Event Generation Info>]
 [<Volume-Based Usage Limit>] [<Time-Based Usage Limit>] [<Opaque Data>]

<Gate-Set> = <Заголовок Решения> <Идентификатор Передачи> <AMID> <Идентификатор Абонента> [<Идентификатор шлюза>] <Спецификация Шлюза> <Профиль трафика> <Классификатор> [<Классификатор>] [<Информация о Создании События>]
 [<Лимит использования по объему>] [<Лимит использования по времени>]
 [<Скрытые данные>]

<Gate-Set-Ack> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID> <GateID>
 [<Opaque Data>]

<Gate-Set-Ack> = <Заголовок ClientSI> <Идентификатор Передачи> <AMID> <Идентификатор Абонента> <Идентификатор шлюза>
 [<Скрытые данные>]

<Gate-Set-Err> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID>
 <IPCablecom Error> [<Opaque Data>]

<Gate-Set-Err> = <Заголовок ClientSI> <Идентификатор Передачи> <AMID> <Идентификатор Абонента> <Ошибка сети IPCablecom>
 [<Скрытые данные>]

<Gate-Info> = <Decision Header> <TransactionID> <AMID> <SubscriberID><GateID>

<Gate-Info> = <Заголовок Решения> <Идентификатор Передачи> <AMID> <Идентификатор Абонента> <Идентификатор шлюза>

<Gate-Info-Ack> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID> <GateID>
 [<Event Generation Info>] <GateSpec> <GateState> <Classifier>
 <Classifier> <Traffic Profile> <Gate Time Info>
 <Gate Usage Info> [<Volume-Based Usage Limit>]
 [<Time-Based Usage Limit>] [<Opaque Data>]

<Gate-Info-Ack> = <Заголовок ClientSI> <Идентификатор Передачи> <AMID> <Идентификатор Абонента> <Идентификатор шлюза>
 [<Информация Создания События>] <Спецификация Шлюза>
 <Состояние Шлюза> <Классификатор> <Классификатор> <Профиль трафика>
 <Информация о времени использования Шлюза>
 <Информация об Использовании Шлюза> [<Лимит использования по объему>]
 [<Лимит использования по времени>] [<Скрытые данные>]

<Gate-Info-Err> = <ClientSI Header> <TransactionID> <AMID> <GateID> <IPCablecomErr>
 [<Opaque Data>]

<Gate-Info-Err> = <Заголовок ClientSI> <Идентификатор Передачи> <AMID> <Идентификатор шлюза> <Ошибка сети IPCablecom>
 [<Скрытые данные>]

<Gate-Delete> = <Decision Header> <TransactionID> <AMID> <SubscriberID> <GateID>

<Gate-Delete> = <Заголовок Решения> <Идентификатор Передачи> <AMID> <Идентификатор Абонента> <Идентификатор шлюза>

<Gate-Delete-Ack> = <ClientSI Header> <TransactionID> <AMID> <GateID> [<Opaque Data>]

<Gate-Delete-Ack> = <Заголовок ClientSI> <Идентификатор Передачи> <AMID>
 <Идентификатор шлюза> [<Скрытые Данные>]

<Gate-Delete-Err> = <ClientSI Header> <TransactionID> <AMID> <GateID>
 <IPCablecom Error> [<Opaque Data>]

<Gate-Delete-Err> = <Заголовок ClientSI> <Идентификатор Передачи> <AMID>
 <Идентификатор шлюза> <Ошибка сети IPCablecom> [<Скрытые Данные>]

<Gate-Report-State> = <ClientSI Header> <TransactionID> <AMID> <SubscriberID> <GateID>
 <GateState>
 <Gate Time Info> <Gate Usage Info> [<Opaque Data>]

<Gate-Report-State> = <Заголовок ClientSI> <Идентификатор Передачи> <AMID>
 <Идентификатор Абонента> <Идентификатор шлюза> <Состояние Шлюза>

Данные сообщения встроены в Объект Информации, Особой для Клиента, в сообщении Отчета о Состоянии COPS. Объект Типа Отчета (C-Num = 12, C-Type = 1), включенное в сообщение Отчета о Состоянии COPS для ответов Контроля Шлюза, ДОЛЖНО иметь поле Типа Отчета установленное равным 1 (Удачно) или 2 (Ошибка) в зависимости от исхода команды Контроля Шлюза. Сообщения Отчета о Состоянии в ответе на команду Контроля Шлюза ДОЛЖНЫ иметь бит предусмотренной метки сообщения установленным в заголовке COPS. Поле Типа Команды Шлюза в Идентификаторе Передачи различает тип созданного ответа.

СМТС создает сообщение Отчета о состоянии шлюза когда существует изменение состояния на Шлюзе, происходящее не из-за сообщения Принятия, или когда были достигнуты пределы некоторых правил. Для сообщения Отчета о состоянии шлюза поле Типа Отчета ДОЛЖНО быть установлено равным 3 (Учитывающее), а поле предусмотренной метки в стандартном заголовке ДОЛЖНО быть очищено.

Если объект, который был получен в сообщении Контроля Шлюза, содержит S-Num или S-Type, который не опознается, такой объект ДОЛЖЕН игнорироваться. НЕЛЬЗЯ, чтобы присутствие такого объекта внутри сообщения Контроля Шлюза рассматривалось как ошибка, приводящая к тому, что после удаления такого параметра, все необходимые объекты присутствовали бы в сообщении.

6.5 Операции протокола контроля шлюза

6.5.1 Последовательность инициализации

Когда РЕР (Сервер, обеспечивающий выполнение правил, или СМТС) загружается, она ДОЛЖНА принимать во внимание входящие соединения COPS на номере 3918 TCP порта, назначенном IANA. Любой Менеджер приложений или Сервер, обеспечивающий выполнение правил, (PDP), который нуждается в установлении контакта с РЕР, ДОЛЖЕН инициировать TCP соединение с РЕР на этом порте. Ожидается, что множественные Менеджеры приложений установят COPS соединения со множественными Серверами, обеспечивающими выполнение правил, а множественные Серверы, обеспечивающие выполнение правил, установят COPS соединения со множественными СМТС. Когда TCP соединение между РЕР и PDP установлено, РЕР ДОЛЖНА отправить информацию о себе на PDP в виде сообщения Открытия Клиента. Данное сообщение ДОЛЖНО включать в себя объект Информации о Версии Мультимедиа, который проинформирует PDP о текущей поддерживаемой версии протокола, используемой на РЕР.

После успешного получения сообщения Открытия Клиента, PDP ДОЛЖНА отправить сообщение Принятия Клиента, если версия протокола, указанная в объекте Информации о Версии, поддерживается. Данное сообщение ДОЛЖНО включать в себя объект Keep-Alive-Timer (Таймер сохранения действующим), который сообщает РЕР максимальный интервал между сообщениями Keep-Alive.

Если версия протокола, представляемая РЕР, не поддерживается, PDP ДОЛЖНА отправить сообщение Закрытие Клиента с Объектом Ошибки COP, указывающее на Код Ошибки 4 (Невозможно продолжать). После отправления сообщения Закрытия Клиента, PDP ДОЛЖНА сохранить TCP соединение и безопасную связь с РЕР, с тем чтобы РЕР могла повторить попытку инициализации COPS без повторного установления TCP соединения и безопасной связи. После получения сообщения Закрытия Клиента от PDP, которое включает в себя объект Ошибки COPS, указывающий на Код ошибки 4, РЕР МОЖЕТ попытаться вновь установить инициализацию COPS соединения, отправив другое сообщение Открытия Клиента с другим номером версии в Объекте Информации о Версии. Данный процесс МОЖЕТ продолжаться до тех пор, пока РЕР либо не получит сообщение Принятия Клиента от PDP, либо пока не закончатся все доступные версии протокола. После того, как РЕР испробует все версии протокола, которые она поддерживает, РЕР ДОЛЖНА отправить сообщение Открытие Клиента со Старшей Версией 0 и Младшей Версией 0 для указания, что она успешно завершила процесс согласования версий. PDP ДОЛЖНА тогда отправить сообщение Закрытия Клиента на РЕР для уведомления, что согласование протокола было неудачным. После получения сообщения Закрытия Клиента, РЕР ДОЛЖНА закрыть TCP соединение. С этой точки PDP МОЖЕТ периодически пытаться возобновить соединение.

Устройства, совместимые с этим описанием, ДОЛЖНЫ использовать версию 1.0, т.е. Объект Информации о Версии со Страшим Номером Версии 1 и Младшим Номером Версии 0.

После успешного получения сообщения Принятия Клиента, РЕР ДОЛЖНА отправить сообщение с Запросом, включающим в себя Описатель клиента и Контекстные объекты. Объект Контекста (C-Num = 2, C-Type = 1) ДОЛЖЕН иметь значение R-Type (Метки Типа Запроса) равное 0x08 (Запрос Конфигурации), а M-Type равное нулю. Объект Описателя Клиента содержит значение, которое ДОЛЖНО выбираться РЕР. Единственное требование, применимое к этому значению, – это то, что

НЕЛЬЗЯ, чтобы РЕР использовала одно и то же значение для двух разных Запросов в пределах одного TCP соединения. Это завершает последовательность инициации, которая визуалью отображена ниже.

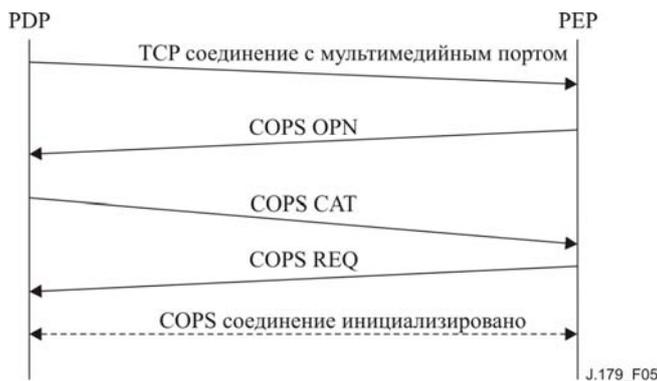


Рисунок 5/J.179 – Установление соединения COPS

Периодически РЕР ДОЛЖНА отправлять сообщения COPS Keep-Alive (КА) на PDP. После получения сообщения COPS КА, PDP ДОЛЖНА отправить сообщение COPS КА обратно РЕР. Данная передача показана ниже и полностью задокументирована в разделе [7]. РЕР ДОЛЖНА отправлять сообщения Keep-Alive по меньшей мере так часто, как указано в Объекте Сохранения Жизни Таймера, возвращенного в сообщении Принятия Клиента. Сообщение Keep-Alive ДОЛЖНО отправляться с Тип Клиентом установленным на ноль и очищенной предусмотренной меткой.

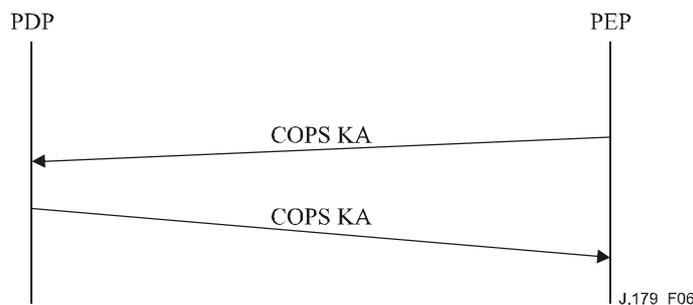


Рисунок 6/J.179 – Обмен сообщениями COPS keep-alive

6.5.2 Последовательность операций

Протокол между PDP и РЕР используется для контролирования ресурсов и правила распределения ресурсов. Менеджер приложений запрашивает принятие правил от Сервера, обеспечивающего выполнение правил, а Сервер, обеспечивающий выполнение правил, авторизует запросы и устанавливает их на CMTS для форсирования во время использования Шлюзов.

Сообщения, которые МОГУТ инициироваться Менеджером приложений и Сервером, обеспечивающим выполнение правил, включают в себя Gate-Set, Gate-Info и Gate-Delete. CMTS МОЖЕТ инициировать сообщения Отчета о состоянии шлюза. Действия для данных сообщений описываются в последующих разделах. Все сообщения от PDP к РЕР ДОЛЖНЫ отправляться с помощью объектов, Особых для Клиента, внутри объекта Принятия COPS сообщения о Принятии. Требуемые ответы от РЕР ДОЛЖНЫ отправляться в виде сообщения Отчета о Состоянии с объектами, Особыми для Клиента, в объекте ClientSI, а требуемая метка ДОЛЖНА быть установлена. Сообщения Отчета о состоянии шлюза от CMTS ДОЛЖНЫ отправляться как непредусмотренные сообщения Отчета о Состоянии через объекты, Особые для Клиента, в объекте ClientSI.

Сообщения Принятия и сообщения Отчета о Состоянии ДОЛЖНЫ содержать одинаковый Описатель клиента, как предусмотрено в начальном Запросе, отправленном Системой завершения вызова для кабельного модема (CMTS) при инициализации COPS соединения.

Сообщение Gate-Set инициирует и модифицирует все параметры правил и трафика для Шлюза и устанавливает информацию биллинга. Сообщение Gate-Set также может использоваться для контроля и обновления состояния Шлюза на CMTS.

Gate-Info является механизмом, с помощью которого Сервер, обеспечивающий выполнение правил, может запрашивать все установки текущего состояния и параметров существующего Шлюза.

Gate-Delete позволяет Серверу, обеспечивающему выполнение правил, удалять определенный Шлюз и любой соответствующий Поток услуг.

Отчет о состоянии шлюза позволяет CMTS информировать Сервер, обеспечивающий выполнение правил, что Шлюз перешел в новое состояние. Сообщения Отчета о состоянии шлюза ДОЛЖНЫ создаваться, когда изменение состояния случается не синхронно (т. е. не в ответ на сообщение Gate-Set message). НЕЛЬЗЯ, чтобы сообщения Отчета о состоянии шлюза создавались, когда изменение состояния происходит синхронно.

PEP ДОЛЖНА периодически отправлять Keep-Alive (KA) сообщение на PDP для содействия обнаружению ошибок в TCP соединении. PDP ДОЛЖНА сохранять отметку о том, когда были получены KA сообщения. Если PEP не получила сообщение KA от PDP во временной интервал, определенный в [7], или PDP не получила уведомления об обнаружении ошибки от TCP соединения, тогда PDP ДОЛЖНА разорвать TCP соединение и попытаться восстановить TCP соединение.

Следующие правила применяются для направления сообщений Контроля Шлюза через структуру мультимедийной сети IP-Cablecom. В частности, обеспечение предоставляется для передачи сообщений Контроля Шлюза туда (т.е. AM-к-PS-к-CMTS) и обратно (т. е. CMTS-к-PS-к-AM) через комплексную многоуровневую сеть, в которой множественные примеры каждого элемента взаимодействуют с элементами в прилегающем(их) слое(ях).

Как описывается в разделе 6.4.3.1, каждый запрос Контроля Шлюза, инициируемый AM (т. е. Gate-Set, Gate-Info, и Gate-Delete) ДОЛЖЕН включать (вдобавок к другим обязательным объектам) объекты как AMID, так и Идентификатора Абонента.

После получения сообщения Контроля Шлюза от AM, PS принимает предоставляемые правила и решает принять или отклонить запрос. Если запрос успешно принят, PS ДОЛЖЕН перенаправить сообщение соответствующей CMTS на основе Идентификатора Абонента, включенного в сообщение. Данное отображение Идентификатор Абонента-на-CMTS может осуществляться динамически, основываясь на запросе к Инфраструктуре OSS, или МОЖЕТ отражать заранее предоставленную информацию о маршрутизации, относящейся к спектру(ам) IP внутренних сетей, которые взаимодействуют с каждой CMTS.

Если запрос Контроля Шлюза отклоняется Сервером, обеспечивающим выполнение правил (PS), ответ на ошибку ДОЛЖЕН возвращаться на производящий AM по поводу того соединения, на которое был отправлен исходный запрос. Если ошибка в соединении замечена между временем, в которое запрос был получен, а ответ предоставлен, PS ДОЛЖЕН уничтожить запрос.

После получения сообщения Контроля Шлюза от PS, CMTS доведет до конца запрошенную операцию. Если данная операция успешно включает в себя либо операцию Gate-Set, либо операцию Gate-Info, CMTS ДОЛЖНА записать AMID и Идентификатор Абонента, включенные в это сообщение и поддерживает связь с соответствующим Шлюзом. Данная информация должна использоваться для гарантий того, что только AM, который изначально создал Шлюз, может запрашивать или модифицировать его. Любые сообщения Контроля Шлюза, которые ссылаются на Шлюз, но которые содержат AMID, отличный от того, который связан со Шлюзом, ДОЛЖНЫ отклоняться CMTS с кодом ошибки "Неавторизованный AMID". Наконец, сообщения Отчета о состоянии шлюза ДОЛЖНЫ доставляться к элементу PS, определенному с помощью IP адреса, который изначально создал Шлюз. Если соединение с данным PS невозможно, тогда CMTS ДОЛЖНА сдерживать сообщения Отчета о состоянии шлюза.

Когда PS получает сообщение Отчета о состоянии шлюза от CMTS, PS ДОЛЖЕН перенаправить данное сообщение Менеджеру приложений (AM), связанному с AMID, включенному в сообщение. С целью поддержать уровень абстракции между неприлегающими слоями и скрыть информацию, связанную с топологией сети, то слоя AM, НЕЛЬЗЯ, чтобы PS включал информацию, непосредственно идентифицирующую определенную CMTS для определенного слоя AM.

6.5.3 Действия для обоснования форматов ресурсов

Набор характеристик Потока услуг данных, которые являются важными для обеспечения усовершенствованного Качества Услуг, известен как формат. Шлюз мультимедийной сети IP-Cablecom может содержать до трех форматов: один, который указывает на Авторизованные ресурсы, один, который указывает на Зарезервированные ресурсы, и один, который указывает на Используемые ресурсы, для Потока услуг, соответствующего Шлюзу. При рассмотрении с любого момента времени, формат использования ДОЛЖЕН находиться внутри Зарезервированного Формата, который ДОЛЖЕН находиться внутри Авторизованного формата.

Когда CMTS получает сообщение Gate-Set, она ДОЛЖНА подтвердить связь между форматом использования, Резервирования и Авторизации Шлюза. Если связь форматов недействительна, CMTS ДОЛЖНА ответить сообщением Gate-Set-Err с кодом ошибки IP-Cablecom "Несовместимый формат".

CMTS ДОЛЖНА также осуществить контроль допуска в любое время, когда запрашивается изменение (включая добавление) зарезервированного формата. Контроль допуска является процессом назначения ресурсов для потока, соответствующего шлюзу. Если ресурсы не могут быть назначены, CMTS ДОЛЖЕН ответить сообщением Gate-Set-Err с кодом ошибки IP-Cablecom "Недостаток Ресурсов".

6.5.3.1 Спецификация Потока (Flow spec)

Вторая колонка в Таблице 2 отображает операцию, которая должна использоваться для сравнения формата А с соответствующим параметром в формате В. Другими словами, формат А соответствует формату В, если каждый из параметров А соответствует критерию, указанному в таблице.

Таблица 2/J.179 – Правила сравнения форматов

Параметр	А {OP} В
Скорость права доступа в сегменте памяти [r]	≤
Размер права доступа в сегменте памяти [b]	≤
Пиковая скорость передачи Данных [p]	≤
Минимальная Управляемая Единица [m]	≥
Максимальный размер пакета [M]	≤
Скорость [R]	≤
Время Простоя [S]	≥

6.5.3.2 Название класса услуг DOCSIS

Для профилей трафика в форме Имени Класса Услуги, цепочка Имени Класса Услуги ДОЛЖНА точно соответствовать ранее существовавшему на CMTS Имени Класса Услуги. Сравнения форматов не требуется, так как все три формата должны иметь одинаковые параметры формата.

6.5.3.3 Параметры Потока услуг DOCSIS

6.5.3.3.1 Кодировка восходящего потока

Вторая колонка Таблицы 3 отображает операцию, которая должна использоваться для сравнения формата А с соответствующим параметром формата В. Другими словами, формат А соответствует формату В, если каждый из параметров А соответствует критерию, указанному в таблице.

Таблица 3/J.179 – Сравнение формата восходящего потока

Параметр	A {OP} B
Приоритет трафика (BE & NRTPS)	≤
Правило запроса передачи (все)	==
Максимальная Скорость Непрерывной передачи трафика (BE, NRTPS, RTPS)	≤
Максимальная импульсная скорость трафика (BE, NRTPS, RTPS)	≤
Минимальная зарезервированная скорость трафика (BE, NRTPS, RTPS)	≤
Допустимый размер пакета минимальной зарезервированной скорости трафика (BE, NRTPS, RTPS)	≥
Номинальный интервал опроса (NRTPS, RTPS, UGS/AD)	Смотри описание интервала ниже
Допустимый уровень неустойчивой синхронизации опроса (RTPS, UGS/AD)	≥
Размер Услуги без запроса разрешения (UGS & UGS/AD)	≤
Число Разрешающих сигналов за Интервал (UGS & UGS/AD)	≤
Номинальный Интервал разрешающих сигналов (UGS & UGS/AD)	Смотри описание интервала ниже
Допустимый уровень неустойчивой синхронизации Разрешающих сигналов (UGS & UGS/AD)	≥

Интервалы – А является внутренним набором В, если параметр в А – целое число множества того же параметра в В.

6.5.3.3.2 Кодировка нисходящего потока Downstream encodings

Вторая колонка Таблицы 4 отображает операцию, которая должна использоваться для сравнения формата А с соответствующим параметром формата В. Другими словами, формат А соответствует формату В, если каждый из параметров А соответствует критерию, указанному в таблице.

Таблица 4/J.179 – Сравнение формата нисходящего потока

Параметр	A {OP} B
Приоритет трафика	≤
Максимальная Скорость Непрерывной передачи трафика	≤
Максимальная импульсная скорость трафика	≤
Минимальная зарезервированная скорость передачи трафика	≤
Допустимый размер пакета Минимальной зарезервированной скорости передачи трафика	≥
Максимальное время задержки нисходящего потока	≥

6.5.4 Действие авторизации ресурсов посредством шлюза

Сообщение Gate-Set МОЖЕТ отправляться от PDP к PEP для инициализации или модификации операционных параметров Шлюзов. Рисунок 7 иллюстрирует пример сигнализации Gate-Set.

ПРИМЕЧАНИЕ. – В качестве примера может использоваться сообщение "Start Session" для уведомления Клиента о том, что ресурсы были авторизованы.



Рисунок 7/J.179 – Пример сигнализации установки шлюза

Если объект Идентификатора Шлюза присутствует в сообщении Gate-Set, тогда это – запрос на модификацию существующего Шлюза. Если объект Идентификатора Шлюза отсутствует в сообщении Gate-Set, тогда это – запрос на создание нового Шлюза. Сообщение Gate-Set ДОЛЖНО содержать только один объект Спецификации Шлюза, описывающий один шлюз либо восходящего, либо нисходящего потока.

Также сообщение Gate-Set содержит Идентификатор Абонента. CMTS ДОЛЖНА использовать данный IP адрес (т.е. Идентификатор Абонента) для определения обслуживающего СМ и ДОЛЖНА использовать MAC адрес Кабельного Модема (СМ) для последующего обмена сообщениями MAC-слоя.

PEP ДОЛЖНА отвечать на сообщение Gate-Set либо сообщением Gate-Set-Ack, указывающим на успех, либо сообщением Gate-Set-Err, указывающим на ошибку. Идентификатор Передачи в ответ ДОЛЖЕН вставить Идентификатор Передачи в запрос. Ошибки в распределяющих или авторизирующих Шлюзах ДОЛЖНЫ фиксироваться в ответе Gate-Set-Err. Обратитесь к разделу 6.4.2.14.

В Сценарии 1, Сервер, Обеспечивающий выполнение правил, МОЖЕТ назначать Форматы Авторизации, Резервирования и использования посредством Профиля трафика, отправляемого в сообщении Gate-Set. Оно МОЖЕТ одновременно давать указание CMTS авторизовывать, резервировать и предоставлять ресурсы.

После получения сообщения Gate-Set CMTS должна сначала привести себя в соответствии с требованиями, указанными в разделе 6.5.3, а затем произвести указанные действия. После успешного завершения действий, запрошенных в сообщении Gate-Set (к примеру, создание Потока услуг DOCSIS), CMTS ДОЛЖНА ответить сообщением Gate-Set-Ack. НЕЛЬЗЯ, чтобы CMTS отвечала сообщением Gate-Set-Ack, пока она не завершит положенные этапы для гарантии того, что любые последующие запросы для Допуска или использования Шлюза не будут неудачны из-за недостатка ресурсов.

CMTS МОЖЕТ осуществлять комплексную авторизацию на основе не только запрошенных QoS и авторизованной Шлюзом Специализации Потока, но также и на основе Идентификатора Класса сеанса связи, определенного при Специализации. CMTS МОЖЕТ иметь обеспеченные правила, которые определяют количество ресурсов, распределенных только для определенного Класса сеанса связи, так же, как и "занятые" правила и правила "приоритетного прерывания обслуживания", которые принимаются для использования ресурсов. Особенности данных типов правил и методик для CMTS находятся вне зоны рассмотрения данной Рекомендации.

После получения сообщений Gate-Set-Ack или Gate-Set-Err от CMTS, Сервер, обеспечивающий выполнение правил, ДОЛЖЕН перенаправить сообщение Менеджеру приложений, соответствующему AMID в сообщении Gate-Set-Ack. Серверу, обеспечивающему выполнение правил, НЕЛЬЗЯ отправлять сообщение Gate-Set-Ack Менеджеру приложений раньше, чем он получит сообщение Gate-Set-Ack от CMTS. Если Менеджер приложений запрашивает услугу, которая не проходит проверку правил Сервера, обеспечивающего выполнение правил, НЕЛЬЗЯ, чтобы Сервер, обеспечивающий выполнение правил, отправлял сообщение Gate-Set на CMTS, и он ДОЛЖЕН отправить сообщение Gate-Set-Err Менеджеру приложений с соответствующим набором ошибок.

6.5.5 Действия для запроса шлюза

Когда Сервер, обеспечивающий выполнение правил, или Менеджер приложений хотят запросить текущие установки параметров Шлюза, они отправляют сообщение Gate-Info на CMTS. CMTS ДОЛЖНА ответить на сообщение Gate-Info либо сообщением Gate-Info-Ack, указывающим на успех, либо сообщением Gate-Info-Err, указывающим на ошибку. Сообщение Gate-Info-Ack ДОЛЖНА содержать информацию о Шлюзе, соответствующему Идентификатору шлюза, в сообщении Gate-Info.

Если запрошенный Шлюз имеет Ограничение использования по объему и/или Времени, тогда CMTS ДОЛЖНА включать данные объекты в сообщение Gate-Info-Ack. PS или AM могут использовать эту информацию для восстановления информации о состоянии Шлюза от CMTS для управления, восстановления ошибок или других целей. Идентификатор Передачи в ответе ДОЛЖЕН соответствовать Идентификатору Передачи в запросе.

Ошибки в запрашиваемых шлюзах ДОЛЖНЫ отражаться в ответе Gate-Info-Err. Объект ошибки в сообщении Gate-Info-Err ДОЛЖЕН содержать один из следующих Кодов Ошибки:

2 = Неизвестный идентификатор шлюза;

127 = Другая, Неопределенная Ошибка.

6.5.6 Действия модификации шлюза

Для модификации Профиля трафика, относящегося к существующему Шлюзу, Менеджер приложений МОЖЕТ отправить сообщение Gate-Set с Идентификатором шлюза, который нужно модифицировать и новым Профилем трафика. Если сообщение Gate-Set не проходит проверки Сервера, обеспечивающего выполнение правил, Сервер, обеспечивающий выполнение правил, ДОЛЖЕН отправить сообщение Gate-Set-Err Менеджеру приложений, и ему НЕЛЬЗЯ отправлять сообщение Gate-Set на CMTS. Однако если сообщение Gate-Set проходит проверку правила Сервера, обеспечивающего выполнение правил, Сервер, обеспечивающий выполнение правил, ДОЛЖЕН отправить сообщение Gate-Set на CMTS. Идентификатор Передачи в сообщении Gate-Set Сервера, обеспечивающего выполнение правил, ДОЛЖЕН соответствовать Идентификатору Передачи в сообщении Gate-Set Менеджера приложений.

После получения сообщения Gate-Set, CMTS должна сначала привести себя в соответствии с требованиями, указанными в параграфе 6.5.3, а затем осуществить запрошенные действия. Подобно созданию нового Шлюза, после успешного завершения действий, запрошенных в сообщении Gate-Set (например, модификация Потока услуг DOCSIS), CMTS ДОЛЖНА ответить сообщением Gate-Set-Ack. НЕЛЬЗЯ, чтобы CMTS отвечала сообщением Gate-Set-Ack, пока она не завершит необходимое количество этапов для гарантии того, что любые последующие запросы для Допуска или использования Шлюза не будут неуспешны из-за недостатка ресурсов.

После получения сообщения Gate-Set-Ack или Gate-Set-Err от CMTS Сервер, обеспечивающий выполнение правил, ДОЛЖЕН перенаправить ответ Менеджеру приложений.

Для модификации Лимитов использования, относящихся к существующим Шлюзам, Менеджер приложений МОЖЕТ отправить сообщение Gate-Set с Идентификатором шлюза, который должен быть модифицирован. Если Профиль трафика в сообщении Gate-Set отличается от Профиля трафика, в настоящее время относящегося к Шлюзу, тогда применяются предыдущие правила. В противном случае, если присутствует Лимит использования потока по объему или времени, тогда существующие лимиты, относящиеся к этому(им) параметру(ам) ДОЛЖНЫ быть заменены новым(и) параметром(ами), а все существующие счетчики или таймеры ДОЛЖНЫ быть обнулены. Однако отсутствие данных параметров в сообщении Gate-Set указывает на то, что даже если Профиль трафика для Шлюза изменяется, существующий(е) Лимит(ы) Шлюза по объему или времени все равно должны применяться. Если данные параметры не присутствуют в сообщении Gate-Set, существующие ограничения ДОЛЖНЫ поддерживаться, а связанные с ними счетчики/таймеры ДОЛЖНЫ продолжать работу со своим текущим значением без перезагрузки.

6.5.7 Действия для поддержки лимитов использования

Менеджер приложений, Сервер, обеспечивающий выполнение правил, и CMTS все принимают участие в укреплении Лимитов использования. Существуют тонкие различия между Лимитом по объему и Лимитом по времени, так что каждый из них описывается отдельно.

6.5.7.1 Действия после достижения лимита использования по объему

Поскольку CMTS является единственным доверенным устройством в мультимедийной сети IP-Cablecom на пути пакета, только одно устройство способно аккуратно отслеживать использование отдельных Шлюзов. Поэтому CMTS ДОЛЖНА отслеживать использование всех Шлюзов вне зависимости от того, связаны они или нет с Лимитом использования по объему. CMTS ДОЛЖНА отмечать весь объем данных, переданных через Шлюз, во всех сообщениях Gate-Info-Ack и всех сообщениях Отчета о состоянии шлюза.

Если Шлюз имеет соответствующий Лимит использования по объему, когда объем данных, переданных через Шлюз равен Лимиту использования по времени, CMTS ДОЛЖНА отправить сообщение с Предусмотренным битом, установленным на 0. Сообщение Отчета о состоянии шлюза ДОЛЖНО включать в себя объект Состояния Шлюза с Причиной, установленной на 7 (Состояние Шлюза не изменилось, но лимит объема достигнут). После получения сообщения Отчета о состоянии шлюза,

поведение PDP зависит от ее роли; Сервер, обеспечивающий выполнение правил, ДОЛЖЕН либо перенаправить сообщение Отчета о состоянии шлюза Менеджеру приложений, либо обработать отчет самостоятельно. Серверу, обеспечивающему выполнение правил, СЛЕДУЕТ только обработать отчет, если это приведет к созданию отчета путем модификации исходного набора шлюза. Другими словами, действия Сервера, обеспечивающего выполнение правил, должны быть видны Менеджеру приложений. Менеджер приложений ДОЛЖЕН обрабатывать полученные запросы. PDP обрабатывает сообщение Отчета о состоянии шлюза с Причиной, установленной на 7, выполняя одно из следующих действий:

- Отправить сообщение Gate-Set с новым объектом Лимита использования по объему, которое SMTS должна использовать для "перезапуска" учета для данного Шлюза;
- Отправить сообщение Gate-Set с Лимитом использования по объему, установленным на 0, для предотвращения неудачи и позволить SMTS продолжить предоставлять услугу для сеанса связи;
- Закрыть Шлюз, издав команду Gate-Delete.

6.5.7.2 Действия после достижения лимита использования по времени

В то время как желательной целью является сохранение действий Лимита по объему и времени как можно более одинаковыми, число прерываний SMTS, необходимых для поддержки укрепления Лимитов использования по времени Системой завершения вызова для кабельного модема (SMTS), делает данный подход невозможным. Поэтому, Менеджер приложений ДОЛЖЕН укрепить Лимит использования Шлюза по времени. После Получения сообщения Gate-Set-Ack для Шлюза с Лимитом использования по времени, АМ ДОЛЖЕН запустить таймер приложения. Когда таймер приложения равен Лимиту использования по времени, Менеджер приложений ДОЛЖЕН отвечать, выполняя одно из следующих действий:

- Отправить сообщение Gate-Set с новым объектом Лимита использования по времени и перезапустить свой таймер приложений;
- Отправить сообщение Gate-Set с Лимитом использования по времени, установленным на 0, чтобы исключить неудачу;
- Закрыть Шлюз, издав команду Gate-Delete.

ПРИМЕЧАНИЕ. – Иногда Менеджеру приложений имеет смысл укрепить Лимит использования, так как Лимиты использования по объему и Времени являются отражениями предложенных услуг в зоне ответственности Домена Контроля Услуги. Это действительно является действием Лимита использования по объему, только необычным, но SMTS – единственное устройство, которое может аккуратно усилить данный лимит.

6.5.7.3 Восстановление ресурсов и ошибок

Поскольку требуется, чтобы Менеджер приложений выполнял одно из нескольких действий, когда достигнут Лимит использования Шлюза, всегда существует возможность того, что Менеджер приложений не ответит надлежащим образом. В таком случае RKS продолжит запись использования Шлюза, так что данное действие будет все-таки возможно учесть, но, при некоторых обстоятельствах, будет полезно восстановить ресурсы, которые использовались "нелегально" Менеджером приложений. Сервер, обеспечивающий выполнение правил, МОЖЕТ поучить сведения о том, что Лимит использования по объему или времени был превышен, на основе сообщений, которые он пересылает от АМ к SMTS. Использование техники "собираания фактов" предполагает, что Сервер, обеспечивающий выполнение правил, кумулятивно изменяет параметры своего состояния в процессе исполнения по вызовам клиентов, но Сервер, обеспечивающий выполнение правил, не изменяющий кумулятивно параметры своего состояния в процессе исполнения по вызовам клиентов, может восстановить ресурсы посредством второй техники, описанной ниже.

Наоборот, Сервер, обеспечивающий выполнение правил, Может иногда запрашивать SMTS посредством сообщения Gate-Info. Ответ будет содержать любые связанные Лимит использования по объему и Информацию об Использовании Шлюза (или Лимит использования по времени и Информацию о времени использования Шлюза). Сервер, обеспечивающий выполнение правил, может затем сравнить данные значения. Вне зависимости от того, как Сервер, обеспечивающий выполнение правил, собирает сведения о том, что Шлюз исчерпал лимит, он МОЖЕТ создавать команду Gate-Delete для Шлюза с исчерпанным лимитом. После получения сообщения Gate-Set-Ack (или Gate-Set-Err) от SMTS, Сервер, обеспечивающий выполнение правил, ДОЛЖЕН отправить сообщение Менеджеру приложений.

Схожим образом пока не требуется восстановление ресурсов от Шлюзов с превышением лимита, CMTS МОЖЕТ произвести то же сравнение самостоятельно и МОЖЕТ удалить Шлюзы с превышением лимита. Дополнительные требования для данного сценария описаны в параграфе 6.5.8.

6.5.7.4 Отслеживание лимитов использования по времени и объема

Шлюзы мультимедийной сети IP-Cablecom могут зафиксированы и расфиксированы много раз (для поддержки, например, функции "паузы" в игре или потоковом медиа). Так как абонент не может передавать/получать данные до тех пор, пока Шлюз находится не в состоянии использования, данные периоды следует использовать против них. Для Лимитов по объему данное требование не имеет эффекта – так как не существует пакетов, которые могли бы быть сверх-учтены, поскольку ни один пакет не может быть отослан, если Шлюз не используется. Однако для Лимитов использования по времени CMTS ДОЛЖНА останавливать свой таймер Информации о времени использования Шлюза, когда Шлюз не находится либо в состоянии использования, либо в состоянии Восстановления использования. Если Шлюз переподключен без изменений Лимита по времени, таймер Информации о времени использования Шлюза ДОЛЖЕН быть установлен на 0 и перезапущен, когда Шлюз вновь будет использоваться.

ПРИМЕЧАНИЕ. – Менеджер приложений должен поддерживать таймер независимым от таймера CMTS для укрепления Лимита использования по времени. Поскольку этот таймер отделен от CMTS сам по себе, время задержки обмена сообщениями может спровоцировать противоречия между данными двумя таймерами. Для приложений, которые требуют высшую степень точности времени, АМ МОЖЕТ затребовать у CMTS ее объект Информации о времени использования Шлюза после того, как он перевел Шлюз в или из состояния использования.

6.5.8 Действия для удаления шлюза

Обычно, когда мультимедийный сеанс связи заканчивается, Менеджер приложений говорит Серверу, обеспечивающему выполнение правил, что сеанс связи завершился, а Сервер, обеспечивающий выполнение правил, в свою очередь, указывает CMTS удалить Шлюз посредством Gate-Delete. CMTS ДОЛЖНА ответить на сообщение Gate-Delete командой Gate-Delete-Ack, указывающей на успех, или командой Gate-Delete-Err, указывающей на неудачу. Идентификатор Передачи в ответе ДОЛЖЕН соответствовать Идентификатору Передачи в запросе.

Ошибки в удаленном Шлюзе ДОЛЖНЫ фиксироваться в ответе Gate-Delete-Err. Объект Ошибки ДОЛЖЕН содержать один из следующих Кодов Ошибки:

2 = Неизвестный идентификатор шлюза;

127 = Другая, неизвестная ошибка.

На CMTS, если таймер T1, T2 (только в состоянии Резервирования), или T4 истекает, Шлюз ДОЛЖЕН удаляться. Когда CMTS удаляет Шлюз без запроса от Сервера, обеспечивающего выполнение правил, CMTS ДОЛЖНА отправить сообщение Отчета о состоянии шлюза (с Предусмотренным битом установленным на 0) на Сервер, обеспечивающий выполнение правил, указывая на то, что Шлюз был удален. Если время таймера T2 истекло в период Зарезервированного состояния, CMTS ДОЛЖНА удалить поток с помощью механизмов DOCSIS (т. е. сообщения DSD) и создать сообщение Отчета о состоянии шлюза (с Обязательным битом установленным на 0) для PS, сообщая об этом изменении состояния. Следует заметить, что если время таймера T2 истекает в период состояния использования или Восстановления использования, тогда CMTS ДОЛЖНА отправить сообщение DSC так, как определено в DOCSIS, для освобождения зарезервированных ресурсов, которые превышают количество активных ресурсов, отправить сообщение Отчета о состоянии шлюза для PS, сообщая об освобождении зарезервированных ресурсов, и остаться в прежнем состоянии. После получения сообщения Отчета о состоянии шлюза Сервер, обеспечивающий выполнение правил, ДОЛЖЕН перенаправить его Менеджеру приложений.

6.5.9 Действие для использования шлюза

В Сценарии 1 Сервер, обеспечивающий выполнение правил, отвечает за использование Шлюза с помощью Профиля трафика, содержащего Формат использования. CMTS предоставляет Шлюз и активирует Поток услуг DOCSIS, используя параметры, переданные ей Сервером, обеспечивающим выполнение правил.

6.5.10 Последовательность завершения

Когда PER закрывает свое TCP соединение с PDP, она МОЖЕТ сначала отправить сообщение Запроса на Удаление Состояния (DRQ) (включая объект Описателя, использованный в первоначальном сообщении Запроса). Если PER решает отправить сообщение DRQ, PER ДОЛЖНА использовать код

причины COPS 4 (Разрыв). PEP МОЖЕТ отправить вслед сообщение о Закрытии Клиента. PDP в ответ ДОЛЖНА автоматически удалить любое состояние, относящееся к PEP, когда завершено TCP соединение. Когда PDP собирается завершить работу, ей СЛЕДУЕТ отправить сообщение COPS о Закрытии Клиента на PEP. В сообщении COPS о Закрытии Клиента, PDP НЕ СЛЕДУЕТ отправлять PDP объект адреса переадресации PDPRedirAddr. Если PEP получает сообщение COPS о Закрытии Клиента от PDP с объектом PDPRedirAddr, PEP ДОЛЖНА игнорировать PDPRedirAddr, пока обрабатывает сообщение COPS о Закрытии Клиента.

НЕЛЬЗЯ, чтобы PS и CMTS удаляли шлюзы, как итог неудачного COPS соединения.

6.5.11 Действия для синхронизации состояния

Когда Сервер, обеспечивающий выполнение правил, хочет синхронизировать свое состояние с состоянием CMTS, он ДОЛЖЕН отправить сообщение Запроса на синхронизацию состояния (SSQ). Данный SSQ МОЖЕТ содержать Описание клиента сервера, обеспечивающего выполнение правил. Если дополнительный Описание клиента присутствует, синхронизируется только состояние, связанное с данным описанием. Если CMTS не опознает запрошенный описание, она ДОЛЖНА немедленно отправить сообщение DRQ на Сервер, обеспечивающий выполнение правил, для описателя, который был определен message в сообщении SSQ. Если ни один Описание клиента не определен в сообщении SSQ, все активные состояния для клиентов с Типом Клиента мультимедийной сети IPCom должны синхронизироваться с PDP.

CMTS осуществляет синхронизацию состояния с помощью создания сообщений Запроса для Шлюзов, связанных с Описанием Клиента (если он включен в SSQ), или для всех известных Шлюзов (если ни один Описание клиента не предоставлен). После завершения синхронизации, CMTS ДОЛЖНА создать сообщение о Завершении Синхронизации Состояния (SSC) для PDP. Если инициирующий SSQ содержал Описание клиента, тогда соответствующее SSC ДОЛЖНО также содержать Описание клиента.

7 Описание интерфейса передачи сообщений о событиях

7.1 Введение

Как и в архитектуре IPCom-T, сообщения о событиях в сети IPCom Multimedia содержат подробную информацию об использовании ресурсов QoS, например, об их резервировании, активизации и освобождении. Новым в сети IPCom Multimedia является необходимость отслеживать состояние выполнения правил (запросы, обновления, удаления). Кроме того, поскольку использование сетевых ресурсов выходит за рамки профилей IPCom-T (постоянное использование в течение всего времени), существует необходимость сообщать об объемах используемой информации и времени ее использования.

Сообщения о событиях, как они определены в этих условиях, создаются элементами сети и сохраняются в Сервере регистрации (RKS). Эти сообщения о событиях (EM) затем коррелируются сервером RKS или иной системой резервного хранения информации с целью записи отдельного события услуги. Эти записи могут быть использованы для получения биллинговой информации услуги, данных об использовании сетевых ресурсов, планирования пропускной способности и т. п. Однако EM не предназначены для контроля ошибок.

В настоящее время сообщения о событиях (EM) в сети IPCom Multimedia создают только CMTS и Сервер, обеспечивающий выполнение правил, которые являются частью сети оператора кабельной связи, и считаются доверенными элементами. Другие элементы сети, такие как различные типы клиентов, считаются недоверенными. В том, что касается Администратора приложений, этот элемент может, как входить, так и не входить в состав сети оператора кабельной связи, и, следовательно, не передает сообщения EM непосредственно на RKS. Однако AM может передавать на PS дополнительную информацию в виде участков полей скрытой информации, которые затем, могут быть введены в сообщения EM, создаваемые сервером PS.

Сообщения о событиях в сети IPCom Multimedia представляют собой упрощенный и модифицированный вариант сообщений о событиях в сети IPCom-T. События, относящиеся к телефонии, такие как Call_Answer и Call_Disconnect считаются дополнительными, так как они являются сообщениями о событиях телефонной связи (например, Элемент услуги y). Имеется тенденция максимально возможной интенсификации использования существующих вариантов EM, при одновременной реализации механизмов абстракции для поддержки общих мультимедийных услуг.

В частности в сети IPCom Multimedia будет использоваться четыре из четырнадцати типов сообщений EM, определенных для услуг голосовой связи, включая QoS_Reserve, QoS_Commit,

QoS_Release и Time_Change. Определено три новых типа сообщений EM, относящихся к выполнению правил: Policy_Request, Policy_Delete и Policy_Update. В Таблице 5 представлен общий обзор типов сообщений EM для IP_Cablecom Multimedia.

Таблица 5/J.179 – Типы сообщений EM для IP_Cablecom Multimedia

ID сообщения о событии	Сообщение о событии	Элемент, создающий сообщений	Описание
7	QoS_Reserve	CMTS	Указывает момент времени, когда CMTS резервирует пропускную способность в сети доступа IP_Cablecom. CMTS должна также создать это сообщение, если зарезервированная пропускная способность меняется.
8	QoS_Release	CMTS	Указывает момент времени, когда CMTS освобождает используемую им пропускную способность в сети доступа IP_Cablecom..
17	Time_Change	PS, CMTS	Регистрирует изменение момента времени. Всегда, когда активный генератор (IP_Cablecom) в доверенном элементе сети (PS и CMTS) изменяется более чем на 200 миллисекунд, элемент сети ДОЛЖЕН создать сообщение Time_Change.
19	QoS_Commit	CMTS	Указывает момент времени, когда CMTS занимает пропускную способность в сети доступа IP_Cablecom. CMTS должна также создать это сообщение, если используемая пропускная способность меняется.
31	Policy_Request	PS	Указывает момент времени, когда Сервер, обеспечивающий выполнение правил, принимает от AM новый запрос о выполнении правил.
32	Policy_Delete	PS	Указывает момент времени, когда Сервер, обеспечивающий выполнение правил, удаляет правило.
33	Policy_Update	PS	Указывает момент времени, когда Сервер, обеспечивающий выполнение правил, принимает от AM запрос об обновлении правила.

Несмотря на то, что сообщения о событиях в сети IP_Cablecom Multimedia основаны на событиях сети IP_Cablecom-T, сообщения, относящиеся к услугам телефонной связи, являются для сети IP_Cablecom Multimedia дополнительными, и они перечислены ниже. Более подробно об этих сообщениях и связанных с ними атрибутах можно узнать из Рекомендации J.164 [10].

Таблица 6/J.179 – Типы сообщений EM, относящихся к услугам телефонной связи, для IP_Cablecom-T

ID сообщения о событии	Сообщение о событии	Описание
1	Signaling_Start	Указывает момент времени, когда начинается сигнализация.
2	Signaling_Stop	Указывает момент времени, когда завершается сигнализация.
3	Database_Query	Указывает момент времени, когда интеллектуальное периферийное устройство завершает выполнение одноразового запроса/ответа или поиска в базе данных (например, в базе данных номер 800, в базе данных LNP).
6	Service_Instance	Указывает момент времени, когда CMS передает экземпляр услуги/набора услуг управления вызовом (например, удержание вызова, ожидание вызова).
9	Service_Activation	Указывает момент времени, когда CMS регистрирует попытку активизировать услугу (например, переадресация вызова, ожидание вызова).

Таблица 6/J.179 – Типы сообщений ЕМ, относящихся к услугам телефонной связи, для IPСablecom-Т

ID сообщения о событии	Сообщение о событии	Описание
10	Service_Deactivation	Указывает момент времени, когда CMS регистрирует попытку деактивизировать услугу (например, переадресация вызова, ожидание вызова).
13	Interconnect_Start	Указывает момент времени, когда начинается процесс сигнализации для соединения сетей.
14	Interconnect_Stop	Указывает завершение использования пропускной способности на соединении между сетью IPСablecom и КТСОП.
15	Call_Answer	Указывает, что начато мультимедийное соединение потому, что появилось событие ответа.
16	Call_Disconnect	Указывает момент времени, когда мультимедийное соединение завершилось потому, что вызывающая сторона завершила вызов, отключившись от линии, или, что от линии отключилась вызываемая сторона, и у вызывающей стороны истекло время соединения.
20	Media_Alive	Указывает, что услуга активна за счет продолжающегося существования канального соединения. Это сообщение может быть создано доверенным элементом сети IPСablecom (CMS, MGC и CMTS), если поставщик посчитает это необходимым.

7.2 Требования к серверу регистрации

Сервер регистрации (RKS) – это функция доверенного элемента сети. В настоящей Рекомендации RKS, как правило, описывается, как отдельный элемент, но настоящая Рекомендация не запрещает иным приложениям выполнять функции RKS, при условии, что это приложение соответствует приведенным здесь требованиям.

RKS – это посредник между сетью IPСablecom Multimedia и приложениями резервного хранения информации. Ожидается, что RKS обрабатывает данные, полученные от сети IPСablecom Multimedia, и передает их в приложения резервного хранения информации в формате и в пределах временных рамок, которые определяет оператор кабельной сети. Следовательно, RKS действует как точка разграничения между сетью IPСablecom и приложениями резервного хранения информации.

RKS ДОЛЖЕН иметь возможность принимать и обрабатывать Сообщения о событиях, форматированных в соответствии с настоящей Рекомендацией.

Сообщения RADIUS, в которые инкапсулированы Сообщения о событиях, передаются по протоколу датаграмм пользователя (UDP), который не гарантирует надежной доставки сообщений; поэтому свойства запроса/ответа этого протокола определены здесь. Когда RKS принимает и успешно регистрирует все Сообщения о событиях IPСablecom, содержащиеся в сообщении "Запрос отчета" (Accounting-Request) RADIUS, он ДОЛЖЕН передать сообщение Запрос отчета клиенту. RKS НЕ ДОЛЖЕН передавать ответ на сообщение Запрос отчета, если он не может успешно зарегистрировать все Сообщения о событиях в сообщении "Запрос отчета".

Серверу RKS СЛЕДУЕТ игнорировать Сообщения о событиях, в которых не распознается тип Сообщения о событиях IPСablecom. Серверу RKS СЛЕДУЕТ также игнорировать атрибуты сообщений IPСablecom, в которых не распознается ID атрибута сообщения.

7.3 Общие требования к элементу мультимедийной сети IPСablecom

В настоящем разделе перечислены требования, предъявляемые к элементам сети IPСablecom Multimedia.

7.3.1 ID элемента

Каждый элемент сети IP-Cablecom, который создает Сообщение о событиях, ДОЛЖЕН идентифицировать себя при помощи статического уникального идентификатора (ID) элемента. ID элемента – это статически сконфигурированный номер элемента, уникальный в пределах домена IP-Cablecom, который ДОЛЖЕН лежать в пределах от 0 до 99 999.

7.3.2 Синхронизация

Для элементов, которые создают Сообщения о событиях, чрезвычайно важно, быть точно синхронизированными друг с другом и со стандартным задающим синхрогенератором. Требования в настоящем разделе гарантируют, что такие элементы будут сохранять свою синхронизацию и сообщать о событиях, используя метки времени, которые будут одновременно аккуратными и точными.

Элементы, которые создают Сообщения о событиях, ДОЛЖНЫ использовать Сетевой протокол синхронизации времени, определенный в [2]. Элементы ДОЛЖНЫ работать в режиме 3 (режиме Клиента). Значение NTP-MAXPOLLS НЕ ДОЛЖНО превышать одиннадцати, что соответствует 2048 секундам.

Сообщения о событиях ДОЛЖНЫ содержать метки времени, имеющие точность до одной миллисекунды.

7.3.3 Аспекты первичных и вторичных RKS

Структура IP-Cablecom Multimedia поддерживает архитектуру, которая состоит из первичных и вторичных RKS. Вторичный RKS используется резервный RKS, когда элемент сети (PS, CMTS) не имеет возможности успешно передать сообщение на первичный RKS. Элементы сети IP-Cablecom Multimedia ДОЛЖНЫ поддерживать передачу сообщения о событии на первичный RKS и переключение при отказе на вторичный RKS, когда нарушается связь с первичным RKS. После того, как элемент сети переключился на вторичный RKS, на все время существования этого сеанса связи или шлюза вторичный RKS становится первичным. Сервер, обеспечивающий выполнение правил, оборудован первичным и вторичным серверами RKS, как требуется для приложений, которые он поддерживает. PS ДОЛЖЕН сообщать на CMTS IP адрес и порт первичного RKS и, дополнительно, вторичного RKS в сообщениях о выполнении правил (Gate-Set). PS ДОЛЖЕН поддерживать несколько комплектов первичных и вторичных RKS.

Для гарантии надежной передачи данных элементы сети должны вводить интервал времени для повторных попыток, определяемый пользователем, и количество раз, которое клиент должен повторно предавать сообщение. Должна иметься возможность регулировать этот интервал времени (предлагается: от 10 мс до 10 с) и число повторных попыток (предлагается: от 0 до 9). Число повторных попыток должно относиться к обоим серверам RKS – первичному и вторичному. После того, как число повторных попыток исчерпано, сообщение о событии должно быть записано в файл ошибок, и сообщение о событии должно быть затем удалено из элемента сети.

Если элемент сети IP-Cablecom не получает сообщение Accounting-Response (Получение Отчета) в течение установленного интервала повторных попыток, он ДОЛЖЕН продолжать повторную передачу Запроса Отчета (Accounting-Request) до тех пор, пока не получит от RKS сообщения Accounting-Response или пока не будет достигнуто максимальное число повторных попыток. Элемент сети IP-Cablecom ДОЛЖЕН повторно передать тот же самый Запроса Отчета на первичный RKS, и, если достигнуто число повторных попыток, повторно передать тот же самый Запрос Отчета на вторичный RKS.

Все элементы сети ДОЛЖНЫ сохранять Сообщения о событиях до тех пор, пока они не получат от RKS Подтверждения (Accounting-Response) того, что данные корректно приняты и сохранены, или до тех пор, пока не будет достигнуто максимальное число повторных попыток. Удалить эти Сообщения о событиях элементы сети могут только, когда получено Подтверждение (Ack), или когда достигнуто максимальное число повторных попыток.

После того, как Элемент сети успешно передал сообщения о событиях на вторичный RKS, происходит переключение на вторичный RKS. Это переключение является необратимым, то есть, вторичный RKS становится активным и теперь он – новый первичный RKS. Все последующие сообщения о событиях для данного сеанса связи ДОЛЖНЫ передаваться на новый активный вторичный RKS. Для всех новых сеансов связи PDP ДОЛЖЕН дать команду PER использовать новый активный RKS в качестве первичного (т. е. RKS, который ранее был вторичным, теперь становится первичным). Отметим, что при определенных условиях возможна ситуация, когда в одном сеансе связи один элемент – PS или CMTS – может связаться с первичным RKS, а второй элемент не может. В таких случаях ожидается, что RKS способен распределить сообщения о событиях между первичным и вторичным RKS.

7.3.4 Взаимодействие с сервером PacketCable RKS

Администратор приложений МОЖЕТ ввести в сообщение Gate-Set (Установить шлюз) дополнительный объект Event Generation Info (Информация о создании объекта). Если такой объект в сообщении представлен, он ДОЛЖЕН содержать действующий идентификатор BCID, который может использоваться в AM, PS и CMTS для коррелирования биллинговой информации этого потока. Если Администратор приложений передает BCID на PS, и AM является для PS доверенным элементом, PS МОЖЕТ использовать BCID, предоставленный Администратором приложений.

Если Администратор приложений вводит дополнительный объект Event Generation Info, определяющий IP адреса первичного и вторичного RKS, которые не известны Серверу, обеспечивающему выполнение правил, то Сервер, обеспечивающий выполнение правил, ДОЛЖЕН передавать Сообщения о событиях для этой транзакции на IP адрес того RKS, который является первичным по умолчанию, за исключением случаев переключения при отказе, когда Сообщения о событиях ДОЛЖНЫ передаваться на IP адрес того RKS, который является вторичным по умолчанию.

Администратор приложений МОЖЕТ определить IP адрес первичного RKS в дополнительном объекте Event Generation Info, или Администратор приложений МОЖЕТ разрешить Серверу, обеспечивающему выполнение правил, использовать свои IP адреса серверов RKS, которые по умолчанию являются первичным и вторичным. Если AM определяет IP адрес первичного RKS, он МОЖЕТ также определить и IP адрес вторичного RKS. Администратор приложений указывает, что RKS не определен, установив нулевые значения IP адресов и портов первичного и вторичного RKS.

Вне зависимости от того, какие данные получит от Администратора приложений Сервер, обеспечивающий выполнение правил, PS ДОЛЖЕН дать CMTS команду использовать те же самые значения BCID и IP адресов и портов первичного/вторичного RKS, которые использует Сервер, обеспечивающий выполнение правил. Сервер, обеспечивающий выполнение правил, (PS) должен принять решение о том, какую пару серверов RKS передавать, на основании Идентификатора Администратора приложений (AMID).

7.4 Сообщения о событиях при передаче мультимедийной информации в IP-Cablecom

В настоящем разделе приведено подробное описание и определение каждого Сообщения о событиях, определенного для IP-Cablecom Multimedia.

7.4.1 События выполнения правил

Сообщения о событиях выполнения правил являются новыми для сети IP-Cablecom Multimedia. Они указывают момент времени, когда Сервер, обеспечивающий выполнение правил, принимает запрос о выполнении правил и выполняет роль связки указанного комплекта Сообщений о событиях с каждым случаем использования ресурсов, относящимся к различным экземплярам услуги. Сообщения о событиях выполнения правил используются для указания первоначального запроса о выполнении правил, об обновлении правил и об удалении правил.

PS ДОЛЖЕН ставить метки времени на Сообщения о событиях выполнения правил после получения от AM запроса о выполнении правил. Сразу же после приема первоначального запроса о выполнении правил, PS ДОЛЖЕН создать идентификатор корреляции биллинговой информации (BCID). Каждый созданный BCID ДОЛЖЕН соответствовать требованиям к формату Структуры атрибута идентификатора корреляции биллинговой информации (BCID), приведенным в Таблице 17.

PS ДОЛЖЕН вводить BCID в заголовок EM для всех последовательно создаваемых Сообщениях о событиях выполнения правил связанных с этим запросом. Кроме того, PS ДОЛЖЕН вводить BCID в сообщение Gate-Set, передаваемое на CMTS.

PS ДОЛЖЕН создать сообщения о событиях выполнения правил сразу же после определения результата запроса о выполнении правил. Этот результат может быть основан на внутренних механизмах авторизации и управления установлением соединения Сервера, обеспечивающего выполнение правил, после получения от CMTS ответа на его сообщения Gate-Set и Gate-Delete. PS создает метку времени для сообщения о событии, когда он получает запрос от AM, но он не создает событие до тех пор, пока он не узнает результатов запроса.

7.4.1.1 Policy_Request (Запрос выполнения правил)

Сервер, обеспечивающий выполнение правил ДОЛЖЕН передать на RKS сообщение о событии Policy_Request, если получен запрос на создание нового правила. PS ДОЛЖЕН установить значение поля Policy_Decision_Status либо в состояние Разрешено (1), либо в состояние Отклонено (2), основываясь на данных авторизации и управления установлением соединения.

ПРИМЕЧАНИЕ. – Поскольку PS не передает сообщение о событии Policy_Request до тех пор, пока CMTS не ответит на сообщение Gate-Set, возможно, что сообщения о событиях QoS от CMTS могут придти на RKS раньше, чем сообщение о событии Policy-Request.

Таблица 7/J.179 – Сообщение о событии Policy-Request

Название атрибута	Требуемый (R) или дополнительный (O)	Комментарий
Event_Message_Header (Заголовок Сообщения о Событии)	R	См. Таблицу 16
Application_Manager_ID (Идентификатор Администратора приложений)	R	Содержит уникальный в масштабах сети идентификатор АМ
Subscriber_ID (Идентификатор абонента)	R	IPv4 адрес абонента
Policy_Decision_Status (состояние решения о выполнении правил)	R	1 – Правило разрешено 2 – Правило отклонено
Policy_Denied_Reason (Причина отклонения правила)	O	Требуется, когда Policy_Decision_Status = 2 (Правило отклонено) 1 – Неисправность сервера, обеспечивающего выполнение правил установления соединения 2 – Недостаточно ресурсов 3 – Абонент неизвестен 127 – Другое
FEID	R	ID финансового элемента. Идентифицирует оплачивающий элемент. Его работа обеспечивается сервером PS.
AM_Opaque_Data (Скрытые данные АМ)	O	Если Администратор приложений включает этот объект (ClientSI: Opaque-Data) в сообщение "Policy Request" (COPS DEC), то Сервер, обеспечивающий выполнение правил, ДОЛЖЕН включить его в Сообщение о событии Policy-Request.
Volume_Usage_Limit (Предел объема использования)	O	Если Администратор приложений включает этот объект (ClientSI: Volume-Based-Usage-Limit) в сообщение "Policy Request" (COPS DEC), то Сервер, обеспечивающий выполнение правил, ДОЛЖЕН включить его в Сообщение о событии Policy-Request.
Time_Usage_Limit (Предел времени использования)	O	Если Администратор приложений включает этот объект (ClientSI: Time-Based-Usage-Limit) в сообщение "Policy Request" (COPS DEC), то Сервер, обеспечивающий выполнение правил, ДОЛЖЕН включить его в Сообщение о событии Policy-Request.

7.4.1.2 Policy_Delete (Удалить правило)

Сервер, обеспечивающий выполнение правил, ДОЛЖЕН передать на RKS Сообщение о событии Policy_Delete, когда он получил от АМ сообщение Gate-Delete, указывающее, что для сеанса связи эти ресурсы более не требуются, когда он получил подтверждение Gate-Delete-Ack от CMTS в ответ на сообщение Gate-Delete, переданное Сервером, обеспечивающим выполнение правил, или когда он получил от CMTS сообщение Gate-Report-State, указывающее, что для сеанса связи эти ресурсы более не доступны. PS ДОЛЖЕН всегда создавать сообщение о событии Policy_Delete для завершения сеанса связи, если для установления этого сеанса связи он ранее создал сообщение о событии Policy-Request.

Таблица 8/J.179 – Сообщение о событии Policy_Delete

Название атрибута	Требуемый (R) или дополнительный (O)	Комментарий
Event_Message_Header (Заголовок Сообщения о Событии)	R	См. Таблицу 16

Таблица 8/J.179 – Сообщение о событии Policy_Delete

Название атрибута	Требуемый (R) или дополнительный (O)	Комментарий
Application_Manager_ID (Идентификатор Администратора приложений)	R	Содержит уникальный в масштабах сети идентификатор АМ
Subscriber_ID (Идентификатор абонента)	R	IPv4 адрес абонента
Policy_Deleted_Reason (Причина удаления правила)	R	1 – Запрос Администратора приложений 2 – Решение CMTS 127 – Другое
FEID	R	ID финансового элемента. Идентифицирует оплачивающий элемент. Его работа обеспечивается сервером PS.
AM_Opaque_Data (Скрытые данные АМ)	O	Если Администратор приложений включает этот объект (ClientSI: Opaque-Data), в сообщении "Policy Request" (COPS DEC), то Сервер, обеспечивающий выполнение правил, ДОЛЖЕН включить его в Сообщение о событии Policy_Delete.

7.4.1.3 Policy_Update (Обновить правило)

Сервер, обеспечивающий выполнение правил, ДОЛЖЕН передать на RKS Сообщение о событии Policy_Update, если он принял от АМ запрос на изменение профиля трафика, классификатора, предела объемов, пределов времени или скрытых данных.

Таблица 9/J.179 – Сообщение о событии Policy_Update

Название атрибута	Требуемый (R) или дополнительный (O)	Комментарий
Event_Message_Header (Заголовок Сообщения о Событии)	R	См. Таблицу 16
Application_Manager_ID (Идентификатор Администратора приложений)	R	Содержит уникальный в масштабах сети идентификатор АМ
Subscriber_ID (Идентификатор абонента)	R	IPv4 адрес абонента
Policy_Decision_Status (состояние решения о выполнении правил)	R	1 – Правило разрешено 2 – Правило отклонено
Policy_Denied_Reason (Причина отклонения правила)	O	Требуется, когда Policy_Decision_Status = 2 (Правило отклонено) 1 – Неисправность сервера, обеспечивающего выполнение правил установления соединения 2 – Недостаточно ресурсов 3 – Абонент неизвестен 4 – Неавторизованный АМID 5 – Неопределенное название класса обслуживания 6 – Несовместимая огибающая 127 – Другое

Таблица 9/J.179 – Сообщение о событии Policy_Update

Название атрибута	Требуемый (R) или дополнительный (O)	Комментарий
Policy_Update_Reason (Причина обновления правила)	R	1 – Профиль трафика 2 – Классификатор 3 – Лимит объемов 4 – Лимит времени 5 – Скрытые данные 6 – Несколько обновлений (комбинация 1-5) 127 – Другое
FEID	R	ID финансового элемента. Идентифицирует оплачивающий элемент. Его работа обеспечивается сервером PS.
AM_Opaque_Data (Скрытые данные AM)	O	Если Администратор приложений включает этот объект (ClientSI: Volume-Based-Usage-Limit) в сообщение "Policy Request" (COPS DEC), то Сервер, обеспечивающий выполнение правил, ДОЛЖЕН включить его в Сообщение о событии Policy_Update.
Volume_Usage_Limit (Предел объема использования)	O	Если Администратор приложений включает этот объект (ClientSI: Volume-Based-Usage-Limit) в сообщение "Policy Request" (COPS DEC), то Сервер, обеспечивающий выполнение правил, ДОЛЖЕН включить его в Сообщение о событии Policy_Update.
Time_Usage_Limit (Предел времени использования)	O	Если Администратор приложений включает этот объект (ClientSI: Volume-Based-Usage-Limit) в сообщение "Policy Request" (COPS DEC), то Сервер, обеспечивающий выполнение правил, ДОЛЖЕН включить его в Сообщение о событии Policy_Update.

7.4.2 Резервирование Качества Обслуживания (QoS_Reserve)

Это Сообщение о событиях (EM) указывает время, когда CMTS резервирует полосу частот в сети доступа IPcablecom. CMTS должна также создать это событие, если зарезервированная ширина полосы изменилась.

CMTS ДОЛЖНА отметить время этого события, сразу же после передачи Подтверждения Динамического Добавления Услуг (DSA-ACK) или Подтверждения Динамического Изменения Услуг (DSC-ACK), удостоверяющих успешную отправку Ответа на Динамическое Добавление Услуг (DSA-RSP) или Ответа на Динамическое Изменение Услуг (DSC-RSP), отправленные на кабельный модем (CM), который завершает передачу зарезервированных ресурсов.

Если код подтверждения в сообщении DSA-RSP или DSC-RSP от Кабельного Модема (CM) не говорит об успешном выполнении операции, то Системе завершения вызова для кабельного модема (CMTS) НЕЛЬЗЯ создавать это сообщение.

Таблица 10/J.179 – Сообщение о событиях QoS_Reserve (Резервирование Качества Обслуживания)

Название атрибута	Требуемый (R) или дополнительный (O)	Комментарий
Event Message Header (Заголовок Сообщения о Событии)	R	См. Таблицу 16
QoS_Descriptor (Дескриптор Качества Обслуживания)	R	Отсутствует
SF_ID (Идентификатор потока услуг)	R	Отсутствует
Flow_Direction (Направление Потока)	R	Отсутствует
Element_Requesting_QoS (Элемент, запрашивающий QoS)	R	0 = Клиент 1 = Сервер, обеспечивающий выполнение правил 2 = Встроенный Клиент

7.4.3 QoS_Commit (Обязательства по Качеству Обслуживания)

Сообщение о Событиях QoS_Commit указывает время, в которое CMTS выделяет полосу частот в Сети доступа IP_Cablecom. CMTS ДОЛЖНА также создавать это сообщение, если меняется выделенная ширина полосы частот.

CMTS ДОЛЖНА отметить время этого события сразу же после передачи сообщения DSA-ACK или DSC-ACK на CM, который завершает передачу, выделяя ресурсы.

Если код подтверждения в DSA-RSP или DSC-RSP от CM не подтверждает успешный прием сообщений, то Системе завершения вызова для кабельного модема (CMTS) НЕЛЬЗЯ создавать это сообщение.

Таблица 11/J.179 – Сообщение о событиях QoS_Commit (Обязательствах по Качеству Обслуживания)

Название атрибута	Требуемый (R) или дополнительный (O)	Комментарий
Event Message Header (Заголовок сообщения о событии)	R	Смотри Таблицу 16
QoS_Descriptor (Дескриптор Качества Обслуживания)	R	Отсутствует
SF_ID (Идентификатор потока услуг)	R	Отсутствует
Flow_Direction (Направление Потока)	R	Отсутствует

7.4.4 QoS_Release (Освобождение Качества Обслуживания)

Сообщение о Событиях QoS_Release указывает время, в которое CMTS освобождает зарезервированные ресурсы и/или полосу частот в сети доступа IP_Cablecom.

CMTS ДОЛЖНА отметить время этого события сразу же после передачи Запроса на Динамическое Удаление Услуг (DSD-REQ), который содержит команду удалить полосу частот.

Таблица 12/J.179 – Сообщение о событиях QoS_Release (Освобождение Качества Обслуживания)

Название атрибута	Требуемый (R) или дополнительный (O)	Комментарий
Event Message Header	R	Смотри Таблицу 16
SF_ID	R	Отсутствует
Flow_Direction	R	Отсутствует
QoS_Release_Reason (Причина Освобождения Качества Обслуживания)	R	1 – Шлюз закрыт Сервером, обеспечивающий выполнение правил (PS) 2 – истекло время неактивности, определенное для Восстановления ресурса (T4) 3 – Ошибка Кабельного Модема (CM) 4 – Предварительно освобождено 5 – Запрос Протокола резервирования ресурсов (RSVP) PathTear 6 – Запрос Кабельного Модема (CM) 7 – Закончилось время, определенное таймером T2 127 – Другое
Gate_Usage_Info	R	Отсутствует
Gate_Time_Info	R	Отсутствует

7.4.5 Time_Change (Изменение Времени)

Это событие описывает момент изменения времени. Всякий раз, как (IP_Cablecom) показания часов на элементе сети (PS или CMTS) изменяются более чем на 200 миллисекунд, сетевой элемент ДОЛЖЕН создавать сообщение об Изменении Времени. Оно включает в себя событие сдвига времени (Переход на летнее/зимнее время), пошаговые настройки для синхронизации с эталонным генератором Сетевой Оконечной Станции (NTP) и ручные изменения настроек времени. Атрибут Event_Time (Время События) в заголовке Сообщения о Событии ДОЛЖЕН отражать новую (отрегулированную) метку

времени. Следует отметить, что сообщение Time_Change (Изменение Времени) не требуется при настройках пропуска, осуществляемых Сетевой Оконечной Станцией (NTP).

Сетевые элементы (PS или CMTS) ДОЛЖНЫ отправлять сообщение о событии Time_Change (Изменение Времени) на активный (на данный момент – первичный) Сервер регистрации (RKS). Сообщение о событиях Time_Change ДОЛЖНО создаваться, когда шлюз(ы) в данное время существуют в CMTS. Сообщение о событии Time_Change может не создаваться, когда в CMTS нет шлюзов. Вне зависимости от того, сколько шлюзов может существовать в CMTS, только одно сообщение о событиях посылается на каждый первичный RKS. Другими словами, если CMTS имеет несколько шлюзов, из которых все направлены на один и тот же Сервер регистрации (RKS), то на этот RKS должно быть передано одно сообщение о событиях Time_Change (Изменения Времени).

Идентификатор корреляции биллинга (BCID) в заголовке сообщения о событии Time_Change (Изменения Времени) ДОЛЖЕН создаваться элементом сети локально во время события. BCID не относится ни к одному сеансу связи, связанному с Идентификатором корреляции биллинга (BCID), это уникальный BCID для этого события.

Таблица 13/J.179 – Сообщения о Событиях Time_Change (Изменение Времени)

Название атрибута	Требуемый (R) или дополнительный (O)	Комментарий
Заголовок Сообщения о Событиях	R	Смотри Таблицу 16
Time_Adjustment (Регулировка времени)	R	Отсутствует

7.5 Атрибуты сообщений о событиях для мультимедийной сети IP-Cablecom

В этом разделе описываются и определяются атрибуты сети IP-Cablecom, включенные в Сообщения о Событиях IP-Cablecom.

Таблица 14 определяет соответствие между сообщениями о событиях и связанными с ними атрибутами. В таблице 15 приводится подробное описание каждого из этих атрибутов.

Таблица 14/J.179 – IP-Cablecom атрибуты, соотнесенные с Сообщениями о Событиях (EM) для мультимедийной сети IP-Cablecom

EM идентификатор атрибута	EM название атрибута	7 – QoS_Reserve	8 – QoS_Release	17 – Time_Change	19 – QoS_Commit	31 – Policy_Request	32 – Policy_Delete	33 – Policy_Update
1	Event_Message_Header (Заголовок Сообщения о Событиях)	X	X	X	X	X	X	X
30	SF_ID (Идентификатор потока услуг)	X	X		X			
32	QoS_Descriptor (Дескриптор Качества Обслуживания)	X			X			
38	Time_Adjustment (Настройка Времени)			X				
49	FEID (Идентификатор потока событий)					X	X	X
50	Flow_Direction (Направление Потoka)	X	X		X			
61	AM_Opaque_Data (Скрытая информация Менеджера приложений)					X	X	X
62	Subscriber_ID (Идентификатор абонента)					X	X	X
63	Volume_Usage_Limit (Лимит использования Объема)					X		X
64	Gate_Usage_Info (Информация об использовании шлюза)		X					
65	Element_Requesting_QoS (Элемент, запрашивающий QoS)	X						
66	QoS_Release_Reason (Причина Освобождения QoS)		X					

Таблица 14/J.179 – IP-Cablecom атрибуты, соотношенные с Сообщениями о Событиях (EM) для мультимедийной сети IP-Cablecom

EM идентификатор атрибута	EM название атрибута	7 – QoS_Reserve	8 – QoS_Release	17 – Time_Change	19 – QoS_Commit	31 – Policy_Request	32 – Policy_Delete	33 – Policy_Update
67	Policy_Denied_Reason (Причина Отклонения Правила)					X		X
68	Policy_Deleted_Reason (Причина Удаления Правила)						X	
69	Policy_Update_Reason (Причина Обновления Правила)							X
70	Policy_Decision_Status (Статус решения о выполнении Правила)					X		X
71	Application_Manager_ID (Идентификатор Менеджера Приложения)					X	X	X
72	Time_Usage_Limit (Лимит использования Времени)					X		X
73	Gate_Time_Info (Информация по времени использования Шлюза)		X					

В таблице 15 представлено более подробное определение каждого атрибута сообщения о событии IP-Cablecom. Значение данных атрибута может быть представлено либо в простом формате данных (одно поле данных), либо более сложной структурой данных.

Таблица 15/J.179 – IP-Cablecom атрибуты MM

ID атрибута EM	длина атрибута EM	название атрибута EM	тип значения атрибута EM	Описание данных атрибута
1	76 байта	EM_Header	Структура данных. См. Таблицу 16	Общая информация, по каждому Сообщению о событии IP-Cablecom
30	4 байта	SF_ID	Целое число без знака	Идентификатор потока услуг, это 32-битное целое число, назначенное Системой завершения вызова для кабельного модема (CMTS) для каждого Потока услуг DOCSIS, определенное в пределах RF MAC домена DOCSIS. Предполагается, что Идентификаторы Потока услуг будут либо восходящими (USFID), либо нисходящими (DSFID). USFID и DSFID выбираются из с одного и того же цифрового поля Идентификатора Потока услуг.
32	Разная; мин 8 байт	QoS_Descriptor	Структура данных. Смотри Таблицу 19	Данные параметров QoS (Качества Обслуживания)
38	8 байт	Time_Adjustment	Назначенное целое число	Настройка времени синхрогенератора элемента (PS, CMTS). Время измеряется в миллисекундах, уточняя величину изменения времени.

Таблица 15/J.179 – IP-Cablecom атрибуты MM

ID атрибута EM	длина атрибута EM	название атрибута EM	тип значения атрибута EM	Описание данных атрибута
49	Разная длина, максимум 247 байт	FEID	ASCII цепочка символов.	Идентификатор материальной сущности. Первые 8 байт представляют собой данные, определенные кабельным оператором. По умолчанию, первые 8 байт заполнены нулями. Начиная с 9-го байта, в поле содержится доменное имя кабельного оператора, которое однозначно идентифицирует оператора для целей биллинга и расчетов. Размер доменного имени кабельного оператора ограничивается 239 байтами.
50	2 байт	Flow Direction	Целое число без знака	Направление потока: 0 = Зарезервировано 1 = Восходящий поток 2 = Нисходящий поток
61	8 байт	AM_Opaque_Data	Целое число без знака	Скрытые данные, переданные Менеджером приложений
62	4 байта	Subscriber_ID	Целое число без знака	4-байтовые объединенные значения, представляющие собой IPv4 адрес
63	8 байт	Volume_Usage_Limit	Целое число без знака	Предельный объем в байтах, определенный Менеджером приложений
64	8 байт	Gate_Usage_Info	Целое число без знака	Число байтов, переданное по радиосети DOCSIS, начиная с байта после заголовка MAC HCS и до конца Циклической проверки избыточности (CRC)
65	2 байт	Element_Requesting_QoS	Целое число без знака	0 = Клиент 1 = Сервер, обеспечивающий выполнение правил 2 = Встроенный клиент
66	2 байта	QoS_Release_Reason	Целое число без знака	1 – Шлюз закрыт Сервером, обеспечивающий выполнение правил (PS) 2 – истекло время неактивности, определенное для Восстановления ресурса (T4) 3 – Ошибка Кабельного Модема (CM) 4 – Предварительно освобождено 5 – Запрос Протокола резервирования ресурсов (RSVP) PathTear 6 – Запрос Кабельного Модема (CM) 7 – Закончилось время, определенное таймером T2 127 – Другое
67	2 байта	Policy_Denied_Reason	Целое число без знака	1 – Ошибка контроля доступа Сервера, обеспечивающего выполнение правил 2 – Недостаток ресурсов 3 – Неизвестный абонент 4 – Неавторизованный AMID 5 – Неопределенное Название класса услуг 6 – Несовместимый формат 127 – Другое

Таблица 15/J.179 – IP-Cablecom атрибуты MM

ID атрибута EM	длина атрибута EM	название атрибута EM	тип значения атрибута EM	Описание данных атрибута
68	2 байта	Policy_Deleted_Reason	Целое число без знака	1 – Запрос Менеджера приложений 2 – Решение Системы завершения вызова для кабельного модема (CMTS) 127 – Другое
69	2 байта	Policy_Update_Reason	Целое число без знака	1 – Профиль трафика 2 – Классификатор 3 – Лимит объема 4 – Лимит времени 5 – Скрытые данные 6 – Множественные обновления (комбинация из 1–5) 127 – Другое
70	2 байта	Policy_Decision_Status	Целое число без знака	1 – Принятое правило 2 – Отклоненное правило
71	4 байта	Application_Manager_ID	Целое число без знака	Уникальный идентификатор для всей сети, назначенный для Менеджера приложений
72	4 байта	Time_Usage_Limit	Целое число без знака	Лимит времени в секундах, определенный Менеджером приложений (AM)
73	4 байта	Gate_Time_Info	Целое число без знака	Количество секунд, в течение которых шлюз был либо в состоянии Используется, либо в состоянии Восстановления использования

7.5.1 Структура атрибутов EM_Header (Заголовка Сообщений о Событиях)

В Таблице 16 содержится подробное описание полей в структуре атрибута EM_Header (Заголовка сообщений о событиях). Этот атрибут заголовка сообщения о событии ДОЛЖЕН быть первым атрибутом в каждом сообщении о событиях сети IP-Cablecom.

Таблица 16/J.179 – Структура атрибутов EM_Header (Заголовка Сообщений о Событиях)

Название поля	Семантика	Тип значения	Длина
Version ID (Идентификатор версии)	Идентифицирует версию структуры данного заголовка EM. 1 = IP-Cablecom 1.0 2 = IP-Cablecom 1.1 3 = IP-Cablecom Multimedia ПРИМЕЧАНИЕ. – Значение 2 или 3 указывает, что в этом заголовке используется поле Event_Object (Объект События). Элементы сети PS и CMTS ДОЛЖНЫ иметь Идентификатор версии равный 3.	Целое число без знака	2 байта
BCID (Идентификатор корреляции биллинга)	Уникальный идентификатор для передачи внутри сети.	Структура данных. Показана в Таблице 17	24 байта
EM Type (Тип Сообщения о Событиях)	Определяет тип сообщения о событиях.	Целое число без знака	2 байта
Element Type (Тип элемента)	Определяет тип элемента – источника сообщения: 0 = Зарезервированный 1 = Зарезервированный 2 = CMTS 3 = Зарезервированный 4 = Сервер, обеспечивающий выполнение правил	Целое число без знака	2 байта
Element ID (Идентификатор элемента)	Уникальный идентификатор для всей сети 5 цифр (статически определенный номер элемента, уникальный в пределах домена IP-Cablecom в пределах от 0 до 99999)	Выровненная по правому краю, дополненная пробелами до требуемого размера строка символов ASCII	8 байт
Time Zone (Временная зона)	Определяет время перехода на зимнее/летнее время и отставание от всемирного координированного времени (UTC). Время перехода на летнее/зимнее время: 0 = Стандартное время 1 = Время перехода Отставание от всемирного координированного времени (UTC) + ЧММСС Отставание рассчитывается с точки зрения сетевых элементов (PS и CMTS); но не с точки зрения абонента.	Строка символов ASCII	1 байт 7 байт
Sequence Number (Номер последовательности)	Каждый элемент сети ДОЛЖЕН назначить уникальное и равномерно возрастающее Целое число без знака для каждого сообщения о событиях, передаваемого на Сервер регистрации (RKS). В тексте настоящей Рекомендации, термин "равномерно возрастающий" следует понимать, как увеличивающийся на 1. RKS использует это для определения в том случае, когда сообщение о событиях от указанных элементов сетей не получено.	Целое число без знака	4 байта

Таблица 16/J.179 – Структура атрибутов EM Header (Заголовка Сообщений о Событиях)

Название поля	Семантика	Тип значения	Длина
Event_time (Время события)	Время и дата создания события. С точностью до миллисекунд. Формат: ггггммддччммсс.mmm	Строка символов ASCII	18 байт
Status (Состояние)	Индикаторы состояния	Смотри Таблицу 18	4 байта
Priority (Приоритет)	Указывает важность назначения по отношению к другим сообщениям о событиях. 255 = самый высокий приоритет. 0 = самый низкий приоритет. 128 = по умолчанию.	Целое число без знака	1 байт
Attribute Count (Отсчет атрибута)	Указывает на количество атрибутов, следующих (или прилагающихся к) после этого заголовка в текущем сообщении о событиях.	Целое число без знака	2 байта
Event Object (Объект события)	Поле Event_Object позволяет сгруппировывать услуги. 0 = Сообщение о событиях по расчетам 1 = Зарезервировано Элементы сети PS и CMTS ДОЛЖНЫ установить значение поля Event_Object равным 0, если Идентификатор версии заголовка сообщения о событиях равен 3 (Сообщение о событиях в мультимедийной сети IP-Cablecom Multimedia на RKS). RKS ДОЛЖЕН уничтожить сообщения о событиях, когда значение поля Event_Object установлено в 1.	Целое число без знака	1 байт

7.5.2 Структура поля BCID (Идентификатора корреляции биллинга)

В Таблице 17 описывается поле Идентификатора корреляции биллинга (BCID). RKS, или некоторые другие приложения резервного хранения информации, используют BCID для корреляции сообщений о событиях, которые были созданы для единичной отправки. Это одно из полей Атрибута Заголовка сообщения о событиях. BCID является уникальным для каждой передачи в сети. Все сообщения о событиях, исходящие от одного и того же элемента сети с одинаковым Идентификатором корреляции биллинга (BCID), ДОЛЖНЫ посылаться на один и тот же первичный RKS, кроме ситуаций перехвата управления. В этом случае сообщения о событиях ДОЛЖНЫ посылаться на вторичный RKS.

Таблица 17/J.179 – Описание поля BCID (Идентификатора корреляции биллинга)

Название поля	Семантика	Тип значения	Длина
Timestamp (Временная метка)	32-бита высшего порядка метки времени Сетевой Оконечной Станции (NTP)	Целое число без знака	4 байта
Element_ID (Идентификатор элемента)	Уникальный идентификатор для всей сети 5 цифр (статически определенный номер элемента, уникальный в пределах домена IPCablecom в пределах от 0 до 99999)	Выровненная по правому краю, дополненная пробелами до требуемого размера строка символов ASCII	8 байт
Time Zone (Временная зона)	Определяет время перехода на зимнее/летнее время и отставание от всемирного скоординированного времени (UTC). Время перехода на летнее/зимнее время: 0 = Стандартное время 1 = Время перехода Отставание от всеобщего скоординированного времени (UTC) ± ЧЧММСС Отставание рассчитывается с точки зрения сетевых элементов (PS и CMTS); но не с точки зрения абонента.	Строка символов ASCII	1 байт 7 байт
Event Counter (Отсчет События)	Равномерно возрастающее значение для каждой Передачи	Целое число без знака	4 байта

7.5.3 Структура поля Status (Состояние)

Поле Status (Состояние) Атрибута Заголовка сообщения о событиях – это 32-битная маска. Нулевой бит – это бит низкого порядка; поле трактуется как 4-битное целое число без знака. В Таблице 18 представлено описание поля Status (Состояние).

Таблица 18/J.179 – Описание поля Status (Состояние)

Начальный бит	Семантика	Отсчет битов
0–1	Индикатор ошибки: 0 = Нет ошибки 1 = Возможная ошибка 2 = Известная ошибка 3 = Зарезервировано	2
2	Происхождение События: 0 = Доверенный Элемент 1 = Недоверенный Элемент	1
3	Замещающее сообщение о событиях: 0 = Не замещающее, посылающему элементу известны все данные 1 = замещающее, данные посланы доверенным элементом или от лица недоверенного элемента	1
4–31	Зарезервировано. Биты поля Status (Состояние) с 4 по 31 ДОЛЖНЫ быть установлены в 0.	28

7.5.4 Структура атрибута дескриптора QoS

В Таблице 19 описывается структура дескриптора данных QoS.

Таблица 19/J.179 – Структура атрибута дескриптора QoS

Название поля	Семантика	Тип значения	Длина
Status_Bitmask (Битовая маска Статуса)	Битовая маска описывает содержимое структуры. (Смотри Таблицу 20)	Битовый массив	4 байта
Service_Class_Name (Название класса услуги)	Название профиля услуги	Выровненная по правому краю, дополненная пробелами до требуемого размера строка символов ASCII	16 байт
QoS_Parameter_Array (Массив параметров QoS)	Параметры QoS. Содержание определяется Битовой маской Состояния.	Массив целых чисел без знака	Массив варьируемой длины 32-битовых целых чисел без знака

В Таблице 20 описывается поле QoS Status Bitmask (Битовой маски состояния QoS) атрибута Дескриптора QoS. Биты со 2 по 17 описывают содержимое QoS_Parameter_Array (Массива Параметров Качества Услуг). Каждый из этих битов указывает на наличие (бит = 1) или отсутствие (бит = 0) указанного параметра QoS в массиве. Местонахождение определенного параметра QoS в массиве соответствует порядку, в котором бит этого параметра находится в битовой маске, начиная с бита низкого порядка.

Каждый параметр QoS, находящийся в Массиве Параметров Качества Услуг (QoS_Parameter_Array) должен занимать четыре байта. Определение и расшифровка параметров QoS могут быть найдены в Приложении Рекомендации по Радиочастотному интерфейсу DOCSIS. Параметры QoS, определение которых занимает менее четырех байт, должны быть выровнены по правому краю (учитывая, что 4 байта рассматриваются как Целое число без знака) в пределах четырех байт, назначенных для элемента массива.

Таблица 20/J.179 – Битовая маска статуса QoS

Начальный бит	Семантика	Отсчет битов
0	Индикация состояния: 0 = Неверное значение 1 = Ресурс Зарезервирован, но не Активирован 2 = Неверное значение 3 = Ресурс Зарезервирован и Активирован	2
2	Тип Планирования Потока услуг	1
3	Номинальный интервал разрешающих сигналов	1
4	Допустимый уровень неустойчивой синхронизации	1
5	Число Разрешающих сигналов за Интервал	1
6	Размер Услуги без запроса разрешения	1
7	Приоритет трафика	1
8	Максимальная скорость непрерывной передачи	1
9	Максимальная импульсная скорость трафика	1
10	Минимальная зарезервированная скорость передачи трафика	1
11	Минимальный размер пакета	1
12	Максимальный объединенный импульс	1
13	Правило Запроса/Передачи	1

Таблица 20/J.179 – Битовая маска статуса QoS

Начальный бит	Семантика	Отсчет битов
14	Номинальный интервал опроса	1
15	Допустимый уровень неустойчивой синхронизации опроса	1
16	IP тип перерегулирования услуги	1
17	Максимальное время ожидания нисходящего потока данных	1

7.6 Протокол отчета RADIUS (Службы дистанционной аутентификации пользователей)

В данном разделе описывается протокол, используемый между элементами сети IPCom, которые создают сообщения о событиях (PS, CMTS), и Сервером Регистрации (RKS). Эти элементы сети ДОЛЖНЫ поддерживать Систему учета Службы дистанционной аутентификации пользователей (RADIUS) (РЧЦ 2866) [8] с расширением сети IPCom, как указывается в настоящей Рекомендации.

Протокол учета RADIUS это протокол клиент/сервер, который состоит из двух типов сообщений: Accounting-Request (Запрос Отчета) и Accounting-Response (Получение Отчета). Элементы сети IPCom, которые создают сообщения о событиях, являются клиентами Службы дистанционной аутентификации пользователей (RADIUS), которые посылают сообщения Accounting-Request на RKS. RKS – это сервер RADIUS, который передает сообщения Accounting-Response обратно на элементы сети IPCom, сообщая, что он успешно получил и сохранил сообщение о событиях.

Сообщения о событиях отформатированы как пакеты Запроса Отчета (Accounting-Request) и Получения Отчета (Accounting-Response) (RADIUS), как указано в [8].

7.6.1 Аутентификация и конфиденциальность

В разделе 8 приводятся подробности относительно использования IPsec для обеспечения аутентификации и конфиденциальности сообщений RADIUS, а также подробности правильного использования совместно используемых секретных данных RADIUS.

7.6.2 Стандартные атрибуты Службы дистанционной аутентификации пользователей (RADIUS)

Каждое сообщение RADIUS начинается со стандартного заголовка RADIUS, который показан в Таблице 21.

Таблица 21/J.179 – Заголовок сообщений RADIUS

Название поля	Семантика	Длина поля
Code (Код)	Accounting-Request (Запрос Отчета) = 4 Accounting-Response (Получение Отчета) = 5	1 байт
Identifier (Идентификатор)	Используется для согласования сообщений Запроса и Получения Отчета.	1 байт
Length (Длина)	Общая длина сообщения RADIUS минимальное значение = 20 максимальное значение = 4096	2 байта
Authenticator (Аутентификатор)	Рассчитывается в соответствии со Спецификацией RADIUS	16 байт

Два стандартных атрибута RADIUS ДОЛЖНЫ следовать за Заголовком сообщения RADIUS: NAS-IP-Address и Acct_Status_Type. Эти два поля включены для улучшения взаимодействия сетей с помощью существующих инструментов сервера RADIUS, учитывая то, что они являются обязательными атрибутами в пакете Accounting-Request RADIUS.

Атрибут NAS-IP-Address указывает создателя сообщения Accounting-Request и ДОЛЖЕН содержать IP адрес элемента сети IPCom, создающего сообщение.

Атрибут Acct_Status_Type, как правило, указывает на то, отмечает ли Accounting-Request начало оказания услуг пользователю (Start) или его окончание (Stop). Сообщение Accounting-Request сети IPCom может содержать начало, окончание или обновление услуг пользователю. Поэтому

значение Acct-Status-Type Interim-Update (Временного Обновления) используется для отражения сообщений о событиях сети IPCablecom.

Таблица 22/J.179 – Обязательные атрибуты RADIUS

Название	Тип	Длина	Значение
NAS-IP-Address	4	6	IP адрес элемента сети IPCablecom, создающего сообщение
Acct_Status_Type	40	6	Interim-Update (Временное Обновление) = 3

Таблица 23/J.179 – Acct_Status_Type (Тип Статуса Отчета) RADIUS

Тип	Длина	Значение
40	6 байт	Interim-Update (Временное Обновление) = 3

Атрибуты сети IPCablecom закодированы в структуре Особых Атрибутов Поставщика (VSA) RADIUS, как описывается в этом разделе. Дополнительные атрибуты IPCablecom, или атрибуты, определяемые поставщиком, могут добавляться к существующим сообщениям о событиях путем прибавления к сообщению дополнительных Особых Атрибутов Поставщика (VSA) RADIUS.

Особый атрибут поставщика включает в себя поле для идентификации поставщика, и Полномочный орган по цифровым адресам в Интернет (IANA) присвоил сети IPCablecom SMI Номер 4491 для Частного Предприимательства в Организации Сетей (Network Management Private Enterprise Number) для кодирования этих атрибутов.

Таблица 24/J.179 – Структура Особых Атрибутов Поставщика (VSA) Radius для атрибутов IPCablecom

Название поля	Семантика	Длина поля
Type (Тип)	Спецификация поставщика = 26	1 байт
Length (Длина)	Общая длина атрибута ПРИМЕЧАНИЕ. – Значение это Длина Поставщика + 8	1 байт
Vendor ID (Идентификатор поставщика)	CableLabs = 4491	4 байта
Vendor Attribute Type (Тип атрибута поставщика)	Тип атрибута IPCablecom	1 байт (смотри Таблицу 15)
Vendor Attribute Length (Длина Атрибута поставщика)	Длина атрибута IPCablecom	1 байт (смотри Таблицу 15) ПРИМЕЧАНИЕ. – Значение равно Длине поставщика +2
Vendor Attribute Value (Значение атрибута поставщика)	Значение атрибута IPCablecom	Байт Длины Поставщика

7.6.3 Синтаксис пакета Запроса Отчета (accounting-request) IPCablecom RADIUS

```
<<RADIUS Accounting-Request> ::=
  <RADIUS message Header>
  <RADIUS NAS-IP-Address Attribute>
  <RADIUS Acct-Status-Type Attribute>
  <Packet Cable EM>
<Packet Cable EM> ::=
  <RADIUS VSA for IPCablecom EM Header Attribute>
  <IPCablecom EM Attribute List>
```

```

<IPCablecom EM Attribute List> ::=
  <RADIUS VSA for IPCablecom EM Attribute> |
  <IPCablecom EM Attribute List>
  <RADIUS VSA for Packet Cable EM Attribute>>

```

Заголовок сообщений о событиях это первый атрибут внутри данного сообщения о событии. Порядок атрибутов сообщения о событиях, которые следуют за заголовком сообщения о событиях, является произвольным.

IPCablecom расширяет Запрос RADIUS, вводя новые атрибуты и новые значения для существующих атрибутов. Так как протокол RADIUS таким образом расширяется, ожидается, что существующие инструменты сервера RADIUS потребуют минимального обновления, для того чтобы поддерживать совокупный сбор сообщений о событиях сети IPCablecom.

8 Требования безопасности

Система безопасности для интерфейсов мультимедийной сети IPCablecom использует механизмы безопасности, описанные как в разделе [11], так и в разделе [1]. В Таблице 25 приводится краткое изложение механизмов безопасности для каждого интерфейса мультимедийной сети IPCablecom.

Таблица 25/J.179 – Интерфейсы безопасности мультимедийной сети

Интерфейс	Описание	Механизмы безопасности
pkt-mm-1	CMTS – CM	Аутентификация на основе Кода аутентификации сообщений со случайными данными (HMAC), определенная Приложением В/J.112.
pkt-mm-2	PS – CMTS	IP-безопасный Протокол совместного использования Eudora (ESP), использующий Обмен ключами по сети Интернет (IKE) или управление ключами на базе системы Kerberos.
pkt-mm-3	AM – PS	IP-безопасный Протокол совместного использования Eudora (ESP), использующий Обмен ключами по сети Интернет (IKE) или управление ключами на базе системы Kerberos.
pkt-mm-4	PS – RKS	IP-безопасный Протокол совместного использования Eudora (ESP), использующий Обмен ключами по сети Интернет (IKE) или управление ключами на базе системы Kerberos.
pkt-mm-5	CMTS – RKS	IP-безопасный Протокол совместного использования Eudora (ESP), использующий Обмен ключами по сети Интернет (IKE) или управление ключами на базе системы Kerberos.
pkt-mm-6	Клиент – CMTS	Вне рассмотрения для этой версии настоящей Рекомендации
pkt-mm-7	Клиент – AM	Вне рассмотрения для этой версии настоящей Рекомендации
pkt-mm-8	AM – Равноправный узел	Вне рассмотрения для этой версии настоящей Рекомендации
pkt-mm-9	CMTS – IP сеть, управляемая кабельным оператором	Вне рассмотрения для этой версии настоящей Рекомендации
pkt-mm-10	Клиент – Равноправный пользователь	Вне рассмотрения для этой версии настоящей Рекомендации

Следующие параграфы описывают систему безопасности, которая применима к любому интерфейсу мультимедийной сети IPCablecom и определяет дополнительные требования или расширения, в случае необходимости.

8.1 CMTS – CM QoS интерфейс (pkt-mm-1)

QoS сообщения Приложения В/J.112 аутентифицируются, используя HMAC (Hash Message Authentication Code – Код аутентификации сообщений со случайными данными), который является криптографическими случайными данными, снабженными ключами. Вычисление атрибута Кода аутентификации сообщений со случайными данными (HMAC), который должен быть включен в QoS сообщение Приложения В/J.112 описывается в В.С.1.4.1 раздела [1].

8.2 Policy Server – CMTS COPS интерфейс (Услуги с общими открытыми правилами предоставления) (pkt-mm-2)

COPS интерфейс Policy Sever – CMTS ДОЛЖЕН защищаться с использованием протокола IPsec ESP, как указывается в пункте 7.2.1.3.2 раздела [11]. Требования управления ключами для этого интерфейса ДОЛЖНЫ сочетаться с пунктом 7.2.1.4.1 раздела [11]. Для этого интерфейса Сервер, обеспечивающий

выполнение правил, ДОЛЖЕН отвечать всем требованиям Контроллера шлюза, указанным в пунктах 7.2.1.3.2 и 7.2.1.4.1 of [11]. Обмен ключами по сети Интернет (IKE) с ключами, заранее позволяющими совместное использование, является обязательным для инструмента, в то время как IKE с сертификатами и IP-безопасность на базе системы Kerberos, являются дополнительными.

В случае если используется IP-безопасность на базе системы Kerberos, пункт 6.4.5 раздела [11] определяет основные имена различных услуг, предоставляемых системой Kerberos. Первый компонент основного имени является уникальным для каждого типа услуг системы Kerberos. Пункт 6.4.5 раздела [11] уже определяет первый компонент основного имени Системы завершения вызова для кабельного модема (CMTS). Первым компонентом основного имени Сервера, обеспечивающего выполнение правил, ДОЛЖЕН быть:

policyserver:<ElementID>

где <ElementID> определяется в пункте 6.4.5 раздела [11].

В случае если используется IKE с сертификатами, имя субъекта в сертификате сервера имеет следующий атрибут, определенный в пункте 8.2.3.4.3 раздела [11]:

OU=<Sub-System Name>

Значение <Sub-System Name> обозначает тип сервера. Значение <Sub-System Name> для Системы завершения вызова для кабельного модема (CMTS) уже определено в пункте 8.2.3.4.3 раздела [11]. Значение <Sub-System Name> для Сервера, обеспечивающего выполнение правил, ДОЛЖНО иметь следующий вид: policyserver.

8.3 Application Manager – Policy Server COPS интерфейс (Услуги с общими открытыми правилами предоставления) (pkt-mm-3)

COPS Интерфейс Application Manager – Policy Server ДОЛЖЕН защищаться с использованием протокола IPsec ESP, как указывается в пункте 7.2.1.3.2 раздела [11]. Требования управления ключами для этого интерфейса ДОЛЖНЫ соответствовать пункту 7.2.1.4.1 раздела [11]. Для этого интерфейса Менеджер приложений ДОЛЖЕН отвечать всем требованиям Контроллера шлюза, указанным в пунктах 7.2.1.3.2 и 7.2.1.4.1 раздела [11]. IKE с ключами, заранее позволяющими совместное использование, является обязательным для инструмента, в то время, как IKE с сертификатами и IP-безопасность на базе системы Kerberos, являются дополнительными.

В случае если используется IP-безопасность на базе системы Kerberos, пункт 6.4.5 раздела [11] определяет основные имена различных услуг, предоставляемых системой Kerberos. Первый компонент основного имени является уникальным для каждого типа услуг системы Kerberos. Первый компонент основного имени Сервера, обеспечивающего выполнение правил, указывается в пункте 8.2/J.170. Первым компонентом основного имени Менеджера приложений ДОЛЖЕН быть:

am:<ElementID>

где <ElementID> определяется в пункте 6.4.5 раздела [11].

В случае если используется IKE с сертификатами, имя субъекта в сертификате сервера имеет следующий атрибут, указанный в пункте 8.2.3.4.3 раздела [11]:

OU=<Sub-System Name>

Значение <Sub-System Name> обозначает тип сервера. Значение <Sub-System Name> для Сервера, обеспечивающего выполнение правил, определяется в пункте 8.2/J.170. Значение <Sub-System Name> для Менеджера приложений ДОЛЖНО состоять из двух символов: am.

8.4 Policy Server – RKS интерфейс сообщения о событии (pkt-mm-4)

Интерфейс сообщения о событии Policy Server – RKS ДОЛЖЕН защищаться с использованием протокола IPsec ESP, как указывается в пункте 7.3.2 раздела [11]. Управление ключами для этого интерфейса ДОЛЖНО быть идентичными тому, которое определено для интерфейса CMTS-RKS в пункте 7.3.3.2 раздела [11]. IKE с ключами, заранее позволяющими совместное использование, является обязательным для инструмента, в то время как IKE с сертификатами и IP-безопасность на базе системы Kerberos, являются дополнительными.

В случае если используется IP-безопасность на базе системы Kerberos, пункт 6.4.5 раздела [11] определяет основные имена различных услуг, предоставляемых системой Kerberos. Первый компонент основного имени является уникальным для каждого типа услуг системы Kerberos. Пункт 6.4.5 раздела [11] уже определяет первый компонент основного имени Сервера Регистрации. Первый компонент основного имени Сервера, обеспечивающего выполнение правил, определяется в пункте 8.2/J.170.

В случае если используется IKE с сертификатами, имя субъекта в сертификате сервера имеет следующий атрибут, указанный в пункте 8.2.3.4.3 раздела [11]:

OU=<Sub-System Name>

Значение <Sub-System Name> обозначает тип сервера. Значение <Sub-System Name> для Сервера регистрации уже определено в пункте 8.2.3.4.3 раздела [11]. Значение <Sub-System Name> для Сервера, обеспечивающего выполнение правил, определяется в пункте 8.2 раздела [11].

8.5 CMTS – RKS интерфейс сообщения о событии (pkt-mm-5)

Интерфейс сообщения о событии CMTS – RKS ДОЛЖЕН защищаться с использованием протокола IPsec ESP, как указывается в пункте 7.3.2 раздела [11]. Управление ключами для этого интерфейса определяется в пункте 7.3.3.2 раздела [11]. IKE с ключами, заранее позволяющими совместное использование, является обязательным для инструмента, в то время, как IKE с сертификатами и IP-безопасность на базе системы Kerberos, являются дополнительными.

9 Соответствие профиля трафика FlowSpec (Спецификации потока) с DOCSIS

Профиль трафика указывает, что атрибуты QoS потока IP или Поток услуг Приложения В/Ж.112 следует использовать при установлении авторизации, резервации и действий использования. Профиль трафика может быть определен одним из следующих методов:

- FlowSpec (Спецификация потока);
- Название Класса услуги DOCSIS;
- Особая параметризация DOCSIS.

Этот раздел описывает процедуры соответствия для получения особых для DOCSIS параметров QoS из различных вариантов Профиля трафика. Профиль трафика может включать в себя авторизацию, резервацию или форматы использования. Как указано в разделе [3], Спецификация потока состоит из TSpec (Спецификации трафика) и дополнительно RSpec.

9.1 Соответствие FlowSpecs с типами расписаний DOCSIS

Спецификация потока поддерживает два типа услуг: Управление нагрузкой и Гарантированная услуги управления нагрузкой предоставляют минимальные гарантии полосы частот, но не дают гарантий времени ожидания/задержки. Гарантированные услуги дают гарантии полосы частот и времени ожидания/задержки. Услуга с гарантированным качеством может быть приблизительно выражена через DOCSIS Опрос в реальном времени и типы расписаний размера Услуги без запроса разрешения (UGS). Услуга Управления нагрузкой может быть близко выражена через тип расписания Лучшей Попытки DOCSIS. Сервисный номер FlowSpec в определении FlowSpec различается у услуги Управления нагрузкой и Гарантированной услуги. Сервисный номер 5 указывает на то, что определением является услуга Управления нагрузкой, а Сервисный номер 2 указывает на то, что определением является Услуга с гарантированным качеством. Далее, услуга Управления нагрузкой содержит только параметры сегмента метки TSpec (Спецификации трафика), а не RSpec. Услуга с гарантированным качеством ДОЛЖНА содержать как TSpec, так и RSpec.

Для приложений, чувствительных к времени ожидания и помехам, таких, как голосовые услуги, MPEG видео или игры, может понадобиться Услуга с гарантированным качеством. CMTS тогда может использовать параметры профиля трафика, определенные в FlowSpec для выбора одного из двух типов расписания DOCSIS, которые может предоставить Услуга с гарантированным качеством: Услуга Опроса в реальном времени (RTPS) и Услуга Услуги без запроса разрешения (UGS). Для других приложений, которые не чувствительны к времени ожидания, может потребоваться услуга Управления нагрузкой, которая может использоваться для предоставления минимальных гарантий полосы частот. В Таблице 26 дается краткое изложение каждой альтернативы.

Таблица 26/J.179 – Типы соответствий FlowSpecs

Тип расписания DOCSIS	Сервисный номер FlowSpec	Пример приложения
Услуга Услуги без запроса разрешения (UGS)	2 (Гарантированная)	Голос через Протокол Интернета (IP)
Услуга Опроса в реальном времени (RTPS)	2 (Гарантированная)	Виртуальная частная сеть (VPN)
Наилучший из возможных (BE)	5 (Контролируемая Загрузка)	Интернет данные "Наилучший из возможных"

Общая процедура преобразования FlowSpec в DOCSIS для услуги с восходящим потоком данных происходит следующим образом:

- После получения сообщения Gate-Set (Установки Шлюза) вместе с FlowSpec CMTS ДОЛЖНА проанализировать Сервисный Заголовок TSpec (Спецификации трафика) для определения того, была запрошена Контролируемая Загрузка или Услуга с гарантированным качеством.
- Если была запрошена Контролируемая Загрузка, тогда CMTS ДОЛЖНА использовать только параметры TSpec для назначения параметров расписания DOCSIS для определения Параметров трафика DOCSIS для типа Планирования "Наилучшей из возможных" DOCSIS.
- Если была запрошена Услуга с гарантированным качеством, тогда CMTS ДОЛЖНА изучить значения параметров Спецификации трафика (TSpec) для Зарезервированной Скорости (R) и Скорости Сегмента (r). Если эти два значения равны, тогда CMTS ДОЛЖНА использовать TSpec и RSpec для определения параметров трафика DOCSIS для DOCSIS типов планирования UGS.
- Если зарезервированная скорость (R) и Скорость сегмента (r) не равны, тогда CMTS ДОЛЖНА использовать TSpec и RSpec для определения параметров трафика DOCSIS для типов планирования Опроса в реальном времени DOCSIS.

Следует заметить, что два других типа расписания DOCSIS не упоминаются выше. Это:

- Услуга Услуги без запроса разрешения с выявлением активности;
- Услуга Опроса не в реальном времени.

Если Менеджер приложений хочет запросить любую из данных услуг, он может сделать это только, используя либо Название класса Услуги, либо специфический для DOCSIS метод параметризации определения Профиля трафика.

9.2 Преобразование FlowSpecs в параметры трафика DOCSIS

Спецификация потока (FlowSpec) состоит из двух частей: TSpec и RSpec. TSpec описывает трафик для потока, а RSpec описывает желаемую услугу; следует заметить, что для услуги управления нагрузкой RSpec не используется. Параметры RSpec ДОЛЖНЫ быть определены для гарантированной услуги. CMTS ДОЛЖНА игнорировать параметры RSpec для услуги управления нагрузкой. RSpec используется для предоставления гарантий времени ожидания для гарантированных услуг. Пожалуйста, обратитесь к Запросам Комментариев (RFC) 2210 раздела [3], 1305 раздела [2], 2211 раздела [4], и 2212 раздела [5] за более подробной информацией о том, как эти параметры следует использовать Менеджерам Приложений для определения профиля трафика. Следует заметить, что интерпретация мультимедийной сетью IP-Cablecom Спецификаций потока отличается от RFC в следующих отношениях:

- Услуга с гарантированным качеством, как определено в разделе [5], контролирует время ожидания постановки в очередь Слоя 3 (т.е. задержек, связанных с пакетным планированием), поскольку в мультимедийной сети IP-Cablecom мы в первую очередь имеем дело с контролем времени ожидания доступа DOCSIS MAC слоя. Следовательно, мы резервируем ресурсы полосы частот в соответствии с параметром TSpec, а не с параметром R RSpec.
- Как указано в разделе [4], Услуга Управления нагрузкой определяет только гарантированную минимальную скорость для потока. Услуга Управления нагрузкой мультимедийной сети IP-Cablecom облегчает определение максимальной скорости для потока так же, как и определение потоков без гарантированной минимальной скорости.
- В мультимедийной сети IP-Cablecom Параметр ненапряженного периода времени гарантированной услуги не требуется, поэтому поле переопределяется, для того чтобы дать возможность контролировать неустойчивую синхронизацию опроса DOCSIS.

Параметры TSpec:

- Глубина сегмента (b), байт;
- Скорость сегмента (r), байт/секунду;
- Максимальный размер датаграммы (M), байт;
- Минимальная управляемая единица (m), байт;
- Пиковая скорость (p), байт/секунду.

Параметры RSpec:

- зарезервированная скорость (R), байт/секунду;
- Ненапряженный период времени (S), микросекунды.

Преобразование параметра, в грубой аппроксимации, включает в себя следующие ассоциации для BE ("Наилучший из возможных") восходящего направления данных DOCSIS и нисходящего направления данных Потокa Услуг Управления нагрузкой. Текущая процедура преобразования будет включать в себя нормализацию этих параметров для рассмотрения анализа заголовка Слоя 2 и Слоя 3.

- Глубина сегмента TSpec (b) \sim Максимальной импульсной скорости трафика DOCSIS;
- Максимальный размер датаграммы TSpec (M) \sim < не требуется в DOCSIS >;
- Минимальная управляемая единица TSpec (m) \sim Размеру пакета допустимого минимума зарезервированной скорости DOCSIS;
- Доля Сегмента TSpec (r) \sim Минимальной зарезервированной скорости DOCSIS;
- Пиковая скорость TSpec (p) \sim Максимальной поддерживаемой скорости DOCSIS для услуги управления нагрузкой.

Для нисходящих потоков информации Гарантированной услуги параметры RSpec добавлены для обеспечения времени ожидания и гарантий резервирования.

- Глубина сегмента TSpec (b) \sim Максимальной импульсной скорости трафика DOCSIS;
- Максимальный размер датаграммы TSpec (M) \sim < не требуется в DOCSIS >;
- Минимальная управляемая единица TSpec (m) \sim Размеру пакета допустимого минимума зарезервированной скорости DOCSIS;
- Скорость сегмента TSpec (r) \sim Минимальной зарезервированной скорости DOCSIS;
- зарезервированная скорость RSpec (R) \sim Максимальной поддерживаемой скорости DOCSIS для гарантированной услуги;
- Ненапряженный период времени RSpec \sim Время ожидания нисходящего потока данных DOCSIS.

Соответствие параметра, приблизительно выраженное, включает в себя следующие ассоциации для потоков услуг UGS DOCSIS.

- Глубина сегмента TSpec (b) = Максимальному размеру датаграммы TSpec (M) = Минимальной управляемой единице TSpec (m) \sim Размеру Услуги без запроса разрешения DOCSIS;
- Скорость сегмента TSpec (r) = Пиковой скорости TSpec (p) = Зарезервированной Скорости RSpec (R) \sim < не требуется в DOCSIS >;
- Ненапряженный период времени RSpec \sim Допустимому уровню неустойчивой синхронизации DOCSIS.

Точно так же следующие ассоциации применяются для потоков услуги опроса в реальном времени DOCSIS:

- Глубина сегмента TSpec (b) \sim Максимальной импульсной скорости трафика DOCSIS;
- Максимальный размер датаграммы TSpec (M) \sim < не требуется в DOCSIS >;
- Скорость сегмента TSpec (r) \sim Максимальной поддерживаемой скорости DOCSIS для гарантированной услуги;
- зарезервированная скорость RSpec (R) \sim используется для вычисления интервала опроса;
- Ненапряженный период времени RSpec \sim Допустимому уровню неустойчивой синхронизации.

Данная абстрактная модель позволяет стандартным инструментам RSVP (Протокола резервирования ресурсов) (как предусматривалось в Сценариях 2 и 3) запрашивать и получать услугу управления нагрузкой или гарантированную услугу из сети без необходимости запрашивать информацию, специфическую для DOCSIS.

В некоторых ситуациях, когда Менеджер приложений и Сервер, обеспечивающий выполнение правил имеют четкую информацию о DOCSIS, он МОЖЕТ назначить Профиль трафика для шлюза, используя Название Класса услуги DOCSIS или формат параметризации, специфический для DOCSIS.

Следует заметить, что существуют несколько параметров Потока услуг DOCSIS, которые не могут быть решены напрямую из FlowSpec; в таком случае, Рекомендация для мультимедийной сети IP-Cablecom назначает значения по умолчанию для таких параметров Потока информации. Если Менеджер приложений/Сервер, обеспечивающий выполнение правил, хочет назначить эти параметры Потока услуг для чего-то другого, отличного от того, которое определяется по умолчанию настоящей Рекомендацией, Менеджер приложений/Сервер, обеспечивающий выполнение правил ДОЛЖЕН использовать либо названия классов услуг, либо форматы параметризации, специфические для DOCSIS, назначенные для профиля трафика.

Для Гарантированной услуги Минимальная зарезервированная скорость и Максимальные поддерживаемые скорости установлены с одинаковым значением и базируются на Скорости Сегмента 'r'. Это происходит из-за того, Услуга с гарантированным качеством предоставляет гарантии времени ожидания, а это означает, что поток не может поддерживаться при скорости большей, чем скорость, при которой источник согласился создавать (когда резервирование было сделано изначально). Резервирование, сделанное при помощи Профиля трафика, при назначении Скорости Сегмента 'r', означает, что источник не будет поддерживать поток трафика больше, чем 'r'. Таким образом, будет неверно использовать Зарезервированную скорость 'R' для отражения любой поддерживаемой скорости DOCSIS (или минимальной или максимальной), в случае Гарантированной услуги.

Однако для Планирования опроса в реальном времени CMTS использует Зарезервированную скорость R для расчета интервала опроса таким образом, что источники трафика могут пульсировать при скорости R без увеличения времени задержки, при которой совокупность пакетов ожидает возможности для восходящей передачи данных DOCSIS. Не смотря на то, что источник трафика может создавать трафик при скорости 'R', CMTS обеспечит, чтобы поддерживаемая скорость не воздействовала на 'r' сверх времени.

В случае Услуги Управления нагрузкой из-за того, что она не предоставляет гарантий времени ожидания, и потому что мы хотим приспособить одну из них, для того чтобы использовать специфическое для DOCSIS понятие гарантированного минимума так же, как максимально поддерживаемые скорости, Скорость сегмента TSpec 'r' соответствует минимальной скорости DOCSIS, а Пиковая скорость TSpec 'p' соответствует Максимальной поддерживаемой скорости DOCSIS. Если для 'r' указывается ноль или бесконечное значение, тогда параметр Минимальной зарезервированной скорости DOCSIS ДОЛЖЕН игнорироваться. Если для 'p' указывается ноль или бесконечное значение, тогда параметр Максимальной поддерживаемой скорости DOCSIS ДОЛЖЕН игнорироваться.

Если возникает синтаксический или семантический конфликт между спецификацией Радиочастотного интерфейса DOCSIS и настоящей спецификацией, преимущество ДОЛЖНА иметь спецификация RFI DOCSIS, кроме специально оговоренных случаев.

9.3 Параметры восходящих потоков данных DOCSIS

Для всех вычислений размеров пакетов восходящего потока данных (кроме специально оговоренных случаев) должна использоваться следующая формула. Пакетный протокольный блок данных (PDU) ДОЛЖЕН рассчитываться с первого байта, следующего за DOCSIS MAC HCS до окончания Циклической проверки избыточности (CRC). Это значение включает в себя служебные сигналы заголовка Ethernet размером в 18 байт (6 байт для адреса источника, 6 байт для адреса назначения, 2 байта для длины, и 4 байта для CRC). Это значение также объединяет служебные сигналы MAC слоя DOCSIS, включая базовый заголовок DOCSIS (6 байт), расширенный заголовок UGS (3 байт) и расширенный заголовок VPI+ (5 байт).

В уравнениях, используемых во всех последующих разделах, используются следующие переменные:

ENET = служебные сигналы Ethernet (18 или 22-байтовые), используемые по умолчанию 18-байтовые ДОЛЖНЫ использоваться всегда, кроме особо оговоренных случаев (то, как CMTS определяет, когда использовать 22-байтовые, находится вне зоны рассмотрения настоящей Рекомендации). В случае потока UGS, пакеты, использующие расширенные заголовки Ethernet со служебными сигналами, для которых они не предназначены, приведут к уменьшению размера пакетов (пакеты, превышающие размер разрешающего сигнала, должны быть уменьшены в размерах). В случае потока RTPS пакеты, использующие расширенные заголовки Ethernet со служебными сигналами, для которых они не предназначены, приведут к тому, что пакеты будут отосланы на первичный ("Наилучший из возможных") Поток услуги.

DOCSIS = заголовок DOCSIS = 6 байт

VPI = VPI заголовок DOCSIS = 5 байт

UGS = UGS Расширенный заголовок DOCSIS = 3 байта

9.3.1 Планирование Услуги без запроса разрешения (UGS)

Планирование Услуги без запроса разрешения ДОЛЖНО использоваться, когда Сервисный номер равен 2 (Гарантировано), Пиковая Скорость, Скорость сегмента и зарезервированная скорость равны, а Максимальный размер датаграммы равен Минимальной управляемой единице.

Объекты восходящего потока данных DOCSIS ДОЛЖНЫ быть настроены, как указано ниже. Все отметки качества Потока услуг сервисных кодирований TLV (состоящих из метки, сведений о длине и собственно значения), которые не определены здесь, ДОЛЖНЫ использоваться в своих значениях по умолчанию, как указывает DOCSIS.

Размер Услуги без запроса разрешения DOCSIS включает в себя служебные сигналы MAC слоя DOCSIS вдобавок к размеру пакета PDU, вычисляемого с помощью формулы, определенной в параграфе 9.3. Служебные сигналы MAC слоя DOCSIS включают в себя базовый заголовок DOCSIS (6 байт), расширенный заголовок UGS (3 байта) и дополнительно VPI+ расширенный заголовок (5 байт).

$$\text{Размер Услуги без запроса разрешения DOCSIS} = M + \text{ENET} + \text{DOCSIS} + \text{UGS} + \text{VPI}$$

Вышеуказанный пример подразумевает, что VPI+ раздела [12] задействован.

НЕЛЬЗЯ, чтобы параметры Максимальной поддерживаемой скорости трафика DOCSIS и размера пакета Допустимой Минимальной зарезервированной скорости использовались для восходящих потоков данных.

Параметры Числа разрешающих сигналов за интервал DOCSIS ДОЛЖНЫ быть установлены равными 1.

Номинальный Интервал разрешающих сигналов DOCSIS ДОЛЖЕН быть установлен равным Максимальному размеру датаграммы, разделенному на Зарезервированную скорость, переведенную в микросекунды.

$$\text{Номинальный Интервал разрешающих Сигналов DOCSIS} = M/R \times 1\,000\,000.$$

Параметр Допустимого уровня неустойчивой синхронизации DOCSIS ДОЛЖЕН быть установлен равным Ненапряженному Периоду. Если это значение меньше, чем длительность минислота DOCSIS, тогда взамен его ДОЛЖНА использоваться длительность минислота. Если значение нуля назначено, тогда ДОЛЖНО использоваться значение по умолчанию, равное 800 мкс.

НЕЛЬЗЯ, чтобы Параметр Номинального интервала опроса DOCSIS назначался в Профиле трафика для потоков услуг UGS. НЕЛЬЗЯ, чтобы Параметр допустимого уровня неустойчивой синхронизации DOCSIS назначался в Профиле трафика для потоков услуг UGS.

Параметр Правила Запроса/Передачи DOCSIS является битовой маской; биты 0–6 и 8 ДОЛЖНЫ быть установлены для потоков услуг UGS.

9.3.2 Планирование опроса в реальном времени

Планирование Опроса в реальном времени ДОЛЖНО использоваться, когда Сервисный номер равен 2 (Услуга с гарантированным качеством), а Пиковая скорость не равна Скорости Сегмента, или Максимальный размер датаграммы не равен Минимальной управляемой единице.

Объекты восходящего потока DOCSIS ДОЛЖНЫ быть установлены, как указано ниже. Все отметки качества Потока услуг сервисных кодировок TLV, которые не определены здесь, ДОЛЖНЫ использоваться в своих значениях по умолчанию, как указывается DOCSIS.

Параметр Максимальной поддерживаемой скорости трафика указывается в битах в секунду и включает в себя служебные сигналы слоя Ethernet. Пересчет из параметров, специфических для IP, включает в себя первое определение скорости пакетизации путем деления Скорости Сегмента на Минимальную управляемую единицу. Затем данное значение умножается на размер пакета, Минимальную управляемую единицу, включая служебные сигналы MAC слоя, а готовый продукт переводится из байтов в биты.

$$\text{Максимальная поддерживаемая скорость трафика DOCSIS} = r/m \times (m + \text{ENET}) \times 8$$

Параметр Максимальной импульсной скорости трафика ДОЛЖЕН быть установлен больше, чем:

- 1) Глубина сегмента, включая служебные сигналы Ethernet, рассчитанная с использованием Минимальной управляемой единицы; или

2) минимальное значение, определенное DOCSIS, равное 1522.

Максимальная импульсная скорость трафика DOCSIS = max ((Глубина сегмента/m) × (m + ENET), 1522)

Параметр минимальной зарезервированной скорости трафика DOCSIS равен Максимальной поддерживаемой скорости трафика DOCSIS.

Минимальная зарезервированная скорость трафика DOCSIS = $r/m \times (m + ENET) \times 8$

Параметр Правила Запроса/Передачи DOCSIS является битовой маской; рекомендованное значение по умолчанию должно быть равным 0x1F.

Параметр Номинального интервала опроса DOCSIS ДОЛЖЕН быть установлен равным Минимальной управляемой единице, разделенной на Зарезервированную скорость, переведенную в микросекунды.

Номинальный интервал опроса DOCSIS = $m/R \times 1\,000\,000$

Параметр Допустимого уровня неустойчивой синхронизации опроса DOCSIS ДОЛЖЕН быть установлен равным Ненапряженному периоду. Если это значение не равно нулю, но меньше, чем длительность минислота, тогда оно ДОЛЖНО быть установлено равным длительности минислота. Если значение нуля назначено, тогда значение Допустимого уровня неустойчивой синхронизации по умолчанию устанавливается равным 800 мкс.

Номинальная Неустойчивая Синхронизация Опроса DOCSIS = S

9.3.3 Планирование услуги "Наилучший из возможных"

Планирование услуги "Наилучший из возможных" ДОЛЖНО использоваться, когда Сервисный номер равен 5 (Контролируемая Загрузка).

Объекты восходящего потока DOCSIS ДОЛЖНЫ быть установлены, как указано ниже. Все отметки качества Потока услуг сервисных кодировок TLV, которые не определены здесь, ДОЛЖНЫ использоваться в своих значениях по умолчанию, как указывается DOCSIS.

Приоритет трафика DOCSIS должен быть установлен равным 5.

Параметр Максимальной поддерживаемой скорости трафика DOCSIS указывается в битах в секунду, включая слой Ethernet со служебными сигналами. Пересчет из параметров, специфических для IP, включает в себя первое определение скорости пакетирования путем деления Пиковой скорости на Минимальную управляемую единицу. Полученное значение затем умножается на размер пакета, Минимальную управляемую единицу, исправленную, для того чтобы включить в себя служебные сигналы слоя Ethernet, а затем весь продукт переводится из байтов в биты. Максимальная поддерживаемая скорость трафика DOCSIS ДОЛЖНА быть пересчитана из Минимальной управляемой единицы.

Максимальная поддерживаемая скорость трафика DOCSIS = $p/m \times (m + ENET) \times 8$

Параметр Максимальной импульсной скорости трафика DOCSIS ДОЛЖЕН быть установлен большим, чем:

- 1) Глубина сегмента, включая служебные сигналы Ethernet, рассчитанная с помощью Минимальной управляемой единицы; или
- 2) минимальное значение, определенное DOCSIS, равное 1522.

Максимальная импульсная скорость трафика DOCSIS = max ((Глубина сегмента / m) × (m + ENET), 1522)

Параметр минимальной зарезервированной скорости трафика DOCSIS рассчитывается так же, и Максимальная поддерживаемая скорость трафика DOCSIS, за исключением того, что вместо параметра Пиковой скорости, используется Скорость сегмента.

Минимальная скорость зарезервированного трафика DOCSIS = $r/m \times (m + ENET) \times 8$

9.3.4 Кодировка классификации пакетов восходящего потока данных

9.3.4.1 Запрос классификации пакетов восходящего потока данных DOCSIS

Объекты восходящего потока данных DOCSIS ДОЛЖНЫ быть определены, как указано ниже. Все отметки качества Потока услуг сервисных кодировок TLV, которые не определены здесь, ДОЛЖНЫ использоваться в своих значениях по умолчанию, как указывается DOCSIS.

Параметр Идентификатора классификатора DOCSIS ДОЛЖЕН использоваться.

Параметр Идентификатора потока услуг DOCSIS ДОЛЖЕН использоваться.

Параметр Приоритета правила DOCSIS ДОЛЖЕН быть установлен равным значению Приоритета в объекте Классификатора.

Параметр Состояния активирования классификации DOCSIS ДОЛЖЕН быть установлен как активный (1) в случаях, когда Шлюз, использующий Поток услуг выделен, для всех других случаев он ДОЛЖЕН быть установлен как неактивный (0).

Действие Динамического изменения услуги DOCSIS МОЖЕТ использовать операции Классификатора добавления DSC (0), Классификатора замены DSC (1) и Классификатора удаления DSC (2) согласно Рекомендации Радиочастотного Интерфейса DOCSIS.

Параметр IP протокола DOCSIS ДОЛЖЕН быть установлен равным значению Идентификатора Протокола, назначенного в объекте Классификатора, если значение не равно нулю, и игнорироваться в противном случае.

Параметр IP адрес источника DOCSIS ДОЛЖЕН быть идентичным адресу объекта Классификатора до тех пор, пока обеспечивается значение, не равное нулю. Если адрес, установленный в объекте Классификатора, равен нулю, то данный параметр ДОЛЖЕН игнорироваться.

Параметр Маски IP источника DOCSIS ДОЛЖЕН игнорироваться.

Параметры Открытия IP порта источника DOCSIS и Закрытия IP порта источника DOCSIS ДОЛЖНЫ быть установлены равными значению порта объекта Классификатора до тех пор, пока обеспечивается значение, не равное нулю. Если значение, установленное в объекте Классификатора, равно нулю, оба параметра Открытия IP порта источника DOCSIS и Закрытия IP порта источника DOCSIS ДОЛЖНЫ игнорироваться.

Параметр IP адрес Назначения DOCSIS ДОЛЖЕН быть установлен равным объекту Классификатора до тех пор, пока обеспечивается значение, не равное нулю. Если адрес, установленный в объекте Классификатора, равен нулю, данный параметр ДОЛЖЕН игнорироваться.

Параметр Маски IP Назначения DOCSIS ДОЛЖЕН игнорироваться.

Параметры Старта IP порта назначения DOCSIS и Окончания IP порта назначения DOCSIS ДОЛЖНЫ быть установлены равными значению порта объекта Классификатора до тех пор, пока обеспечивается значение, не равное нулю. Если значение, установленное в объекте Классификатора, равно нулю, оба параметра Старта IP порта назначения DOCSIS и Конца IP порта Назначения DOCSIS ДОЛЖНЫ игнорироваться.

Параметры Кодировки классификации Ethernet LLC Пакетов DOCSIS ДОЛЖНЫ игнорироваться.

Параметры Кодировки классификации 802.1P/Q Пакетов DOCSIS ДОЛЖНЫ игнорироваться.

9.4 Параметры нисходящих потоков данных DOCSIS

9.4.1 Кодировка нисходящих потоков данных QoS для гарантированной услуги

TLV кодировки качества услуг нисходящего Потока услуг DOCSIS ДОЛЖНЫ быть установлены, как указано ниже. Все TLV кодировки качества услуг Потока услуг, которые не указаны здесь, ДОЛЖНЫ использоваться в их значениях по умолчанию, как указывается DOCSIS.

Параметры нисходящих потоков данных DOCSIS рассчитываются при помощи MAC заголовка DOCSIS из байта, следующего за HCS до окончания Циклической проверки избыточности (CRC). Данное значение включает в себя служебные сигналы заголовка Ethernet.

Исходя из этих служебных сигналов, параметр размера пакета Допустимой Минимальной зарезервированной скорости DOCSIS ДОЛЖЕН рассчитываться как:

$$\text{размер пакета Допустимой Минимальной зарезервированной скорости DOCSIS} = m + \text{ENET}$$

Параметр Максимальной поддерживаемой скорости трафика DOCSIS указывается в битах в секунду, включая служебные сигналы MAC слоя. Пересчет из параметров, определенных для IP, включает в себя первое определение скорости пакетизации путем деления Скорости Сегмента на Минимальную управляемую единицу. Данное значение затем умножается на размер пакета, Минимальную управляемую единицу, исправленную, чтобы включать в себя служебные сигналы MAC слоя, а затем готовый продукт переводится из байтов в биты. Максимальная поддерживаемая скорость трафика DOCSIS ДОЛЖНА рассчитываться как:

$$\text{Максимальная поддерживаемая скорость трафика DOCSIS} = r/m \times (m + \text{ENET}) \times 8$$

Минимальная зарезервированная скорость трафика DOCSIS равна Максимальной поддерживаемой скорости трафика DOCSIS.

Следует заметить, что Максимальная поддерживаемая скорость трафика DOCSIS и Минимальная зарезервированная скорость трафика DOCSIS рассчитываются немного по-разному в мультимедийной сети IP-Cablecom и в IP-Cablecom DQoS. Мультимедийная сеть IP-Cablecom базируется на r , а IP-Cablecom DQoS базируется на p . Это происходит вследствие того факта, что в DQoS $r = p$, в то время как в мультимедийной сети данные значения различаются (в этом случае r является значением правильной скорости при использовании).

Параметр Максимальной импульсной скорости трафика DOCSIS ДОЛЖЕН быть установлен больше, чем:

- 1) Глубина сегмента, включая служебные сигналы DOCSIS, рассчитанная с помощью Минимальной управляемой единицы; или
 - 2) минимальное значение, определенное DOCSIS, равное 1522.
- Максимальная импульсная скорость трафика DOCSIS = $\max ((\text{Bucket Depth} / m) \times (m + \text{ENET}), 1522)$

Параметр Приоритета трафика DOCSIS ДОЛЖЕН быть установлен на 5.

Параметр Времени задержки нисходящего потока данных DOCSIS ДОЛЖЕН быть установлен равным Ненапряженному периоду при условии, что Ненапряженный период не равен нулю. Если Ненапряженный период равен нулю, НЕЛЬЗЯ, чтобы данный параметр заполнялся.

9.4.2 Кодировка нисходящих потоков данных QoS для услуги управления нагрузкой

TLV кодировки качества услуг нисходящего Потока услуг DOCSIS ДОЛЖНЫ быть настроены так, как указано ниже. Все TLV кодировки качества услуг Потока услуг, которые не указаны здесь, ДОЛЖНЫ использоваться в их значениях по умолчанию, как указывается DOCSIS.

Параметры нисходящих потоков данных DOCSIS рассчитываются при помощи MAC заголовка DOCSIS из байта, следующего за HCS до окончания Циклической проверки избыточности (CRC). Данное значение включает в себя служебные сигналы заголовка Ethernet.

Исходя из этих служебных сигналов, параметр размера пакета Допускаемой Минимальной зарезервированной скорости DOCSIS ДОЛЖЕН рассчитываться как:

$$\text{размер пакета Допускаемой Минимальной зарезервированной скорости DOCSIS} = m + \text{ENET}$$

Параметр Максимальной поддерживаемой скорости трафика указывается в битах в секунду, включая служебные сигналы MAC слоя. Пересчет из параметров, специфических для IP, включает в себя первое определение скорости пакетизации путем деления Пиковой скорости на Минимальную управляемую единицу. Данное значение затем умножается на размер пакета, Минимальную управляемую единицу, исправленную так, чтобы включать в себя служебные сигналы MAC слоя, а готовый продукт переводится из байт в биты. Максимальная поддерживаемая скорость трафика DOCSIS ДОЛЖНА рассчитываться как:

$$\text{Максимальная поддерживаемая скорость трафика DOCSIS} = p/m \times (m + \text{ENET}) \times 8$$

Параметр минимальной зарезервированной скорости трафика DOCSIS рассчитывается схожим образом с Максимальной Поддерживаемой скоростью трафика DOCSIS, за исключением того, что вместо Пиковой скорости используется Скорость сегмента.

$$\text{Параметр минимальной зарезервированной скорости трафика DOCSIS} = r/m \times (m + \text{ENET}) \times 8$$

Параметр Максимальной импульсной скорости трафика DOCSIS ДОЛЖЕН быть установлен больше, чем:

- 1) Глубина сегмента, включая служебные сигналы DOCSIS, рассчитанная с помощью Максимального Размера Датаграммы; или
- 2) минимальное значение, определенное DOCSIS, равное 1522.

$$\text{Параметр Максимальной импульсной скорости трафика} = \max ((\text{Bucket Depth} / M) \times (M + \text{ENET}), 1522)$$

Параметр Приоритета трафика DOCSIS ДОЛЖЕН быть установлен к 5.

НЕЛЬЗЯ, чтобы заполнялся параметр Времени задержки нисходящего потока данных DOCSIS.

9.4.3 Кодировка классификации пакетов нисходящих потоков данных

9.4.3.1 Запрос классификации пакетов нисходящих потоков данных DOCSIS

Объекты классификации нисходящего потока данных DOCSIS ДОЛЖНЫ быть настроены так, как указывается ниже. Все TLV кодировки качества услуг Потока услуг, которые не указаны здесь, ДОЛЖНЫ использоваться в их значениях по умолчанию, как указывается DOCSIS..

Параметр Идентификатора классификатора DOCSIS ДОЛЖЕН использоваться.

Параметр Идентификатора потока услуг DOCSIS ДОЛЖЕН использоваться.

Параметр Правила приоритета DOCSIS ДОЛЖЕН быть настроен так, чтобы соответствовать значению Приоритета, назначенному в объекте Классификатора.

Параметр Состояния Активирования Классификации DOCSIS ДОЛЖЕН быть установлен как активный (1) в тех случаях, когда Шлюз, использующий Поток услуг, выделен, а для всех других случаев он ДОЛЖЕН быть установлен как неактивный (0).

Действие Динамического Изменения Услуг DOCSIS МОЖЕТ использовать операции Классификатора добавления DSC (0), Классификатора замены DSC (1) и Классификатора удаления DSC (2) согласно Рекомендации Радиочастотного Интерфейса DOCSIS.

Параметр IP Протокола DOCSIS ДОЛЖЕН быть настроен так, чтобы быть равным значениям Идентификатора Протокола, указанным в объекте Классификатора, если значение не равно нулю и игнорироваться во всех других случаях.

Параметр IP адрес источника DOCSIS ДОЛЖЕН быть настроен так, чтобы быть идентичным адресу, указанному в объекте Классификатора до тех пор, пока обеспечивается значение, не равное нулю. Если адрес, назначенный в объекте Классификатора, равен нулю, данный параметр ДОЛЖЕН игнорироваться.

Параметр Маски IP источника ДОЛЖЕН игнорироваться.

Параметры Старта IP порта источника DOCSIS и Конца IP порта источника DOCSIS ДОЛЖНЫ быть настроены так, чтобы быть равными значению порта объекта Классификатора до тех пор, пока обеспечивается значение, не равное нулю. Если значение, назначенное в объекте Классификатора, равно нулю, оба параметра Старта IP порта источника DOCSIS и Конца IP порта источника DOCSIS ДОЛЖНЫ игнорироваться.

Параметр IP адрес Назначения DOCSIS ДОЛЖЕН быть настроен так, чтобы быть идентичным адресу назначения, указанному в объекте Классификации до тех пор, пока обеспечивается значение, не равное нулю. Если адрес, указанный в объекте Классификации, равен нулю, данный параметр ДОЛЖЕН игнорироваться.

Параметр Маски IP Назначения DOCSIS ДОЛЖЕН игнорироваться.

Параметры Старта IP порта Назначения DOCSIS и Конца IP порта Назначения DOCSIS ДОЛЖНЫ быть настроены так, чтобы быть равными значению порта объекта Классификатора до тех пор, пока обеспечивается значение, не равное нулю. Если значение, назначенное в объекте Классификатора, равно нулю, оба параметра Старта IP порта Назначения DOCSIS и Конца IP порта Назначения DOCSIS ДОЛЖНЫ игнорироваться.

Кодировки классификации LLC Пакетов Ethernet DOCSIS ДОЛЖНЫ игнорироваться.

Кодировки классификации 802.1P/Q Пакетов DOCSIS ДОЛЖНЫ игнорироваться.

10 Потоки сообщений

Этот раздел предоставляет два сценария взаимодействия между разными элементами сети, представленными ранее в данной Рекомендации. Первое взаимодействие обозначается как относительно высокий уровень обмена основными сообщениями, который применяется внутри структуры мультимедийной сети IP-Cablecom с целью авторизации, резервации и выделения доступа сетевых ресурсов под управлением Сценария 1. Второе взаимодействие предоставляет очень подробное описание каждого сообщения и атрибута, используемых в интерфейсах мультимедийного Качества услуг IP-Cablecom и сообщений о событиях.

10.1 Общая последовательность сообщений

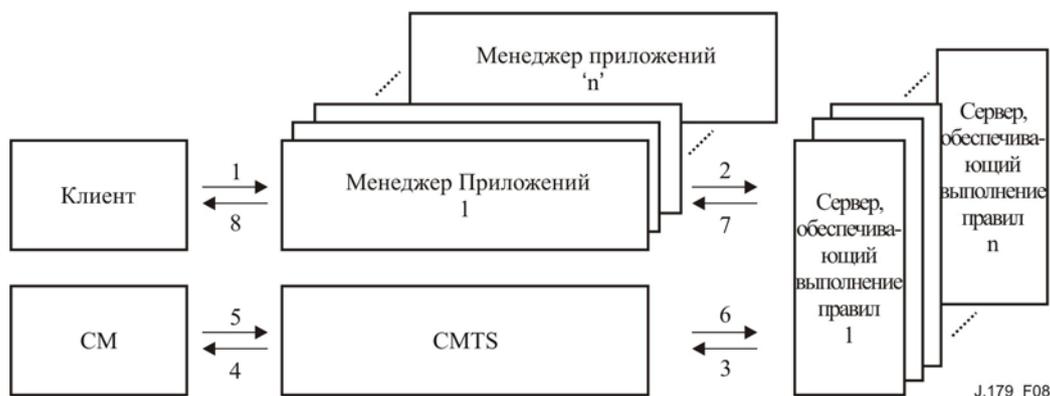


Рисунок 8/J.179 – Общая последовательность сообщений

- 1) Клиент отправляет запрос настройки сеанса связи для Менеджера приложений через сигналы Слоя Приложения. Клиент может аутентифицироваться на Менеджере Приложений во время этого этапа.
- 2) Перед тем, как активировать этот сеанс связи, Менеджер приложений запрашивает Открытие Шлюза (Gate-Set) (в сообщении Решения COPS) и отправляет его на Сервер, обеспечивающий выполнение правил, с целью определить будет ли разрешено продолжить запрос настройки сеанса. Сообщение включает в себя:
 - i) AMID;
 - ii) Идентификатор абонента;
 - iii) Идентификатор передачи;
 - iv) Классификатор;
 - v) Профиль трафика для потока;
 - vi) Спецификацию Шлюза.
- 3) После получения запроса, Сервер, обеспечивающий выполнение правил, проверяет запрос на соответствие правилам и, если запрос принимается, отправляет сообщение Gate-Set Системе завершения вызова для кабельного модема. (CMTS). Сообщение включает в себя:
 - i) AMID;
 - ii) Идентификатор абонента;
 - iii) Идентификатор передачи;
 - iv) Классификатор;
 - v) Профиль трафика для потока (Авторизованный, Зарезервированный и Выделенный);
 - vi) Спецификацию Шлюза.
- 4) CMTS использует классификатор и информацию Профиля трафика для инициации активирования потока путем создания необходимых DSx DOCSIS сообщений.
- 5) CM подтверждает соответствующим DSx messaging (Механизмом сигнализации)
- 6) CMTS отправляет Gate-Set-Ack (Запрос на открытие шлюза) на Сервер, обеспечивающий выполнение правил, в ответ на сообщение Gate-Set, полученное на Этапе 3. Сообщение включает в себя:
 - i) AMID;
 - ii) Идентификатор передачи;
 - iii) Идентификатор шлюза;
 - iv) Идентификатор абонента.

- 7) В ответ Сервер, обеспечивающий выполнение правил, создаст Gate-Set-Ack для AM; оно говорит Менеджеру приложений, что Запрос правила был принят, и запрос клиента может продолжаться, а необходимые ресурсы в основной сети были зарезервированы. Сообщение включает в себя:
 - i) AMID;
 - ii) Идентификатор передачи;
 - iii) Идентификатор шлюза;
 - iv) Идентификатор абонента.
- 8) Менеджер приложений после получения Gate-Set-Ack проинформирует клиента о том, что установление сеанса связи может быть продолжено.

10.2 Подробная последовательность сообщений

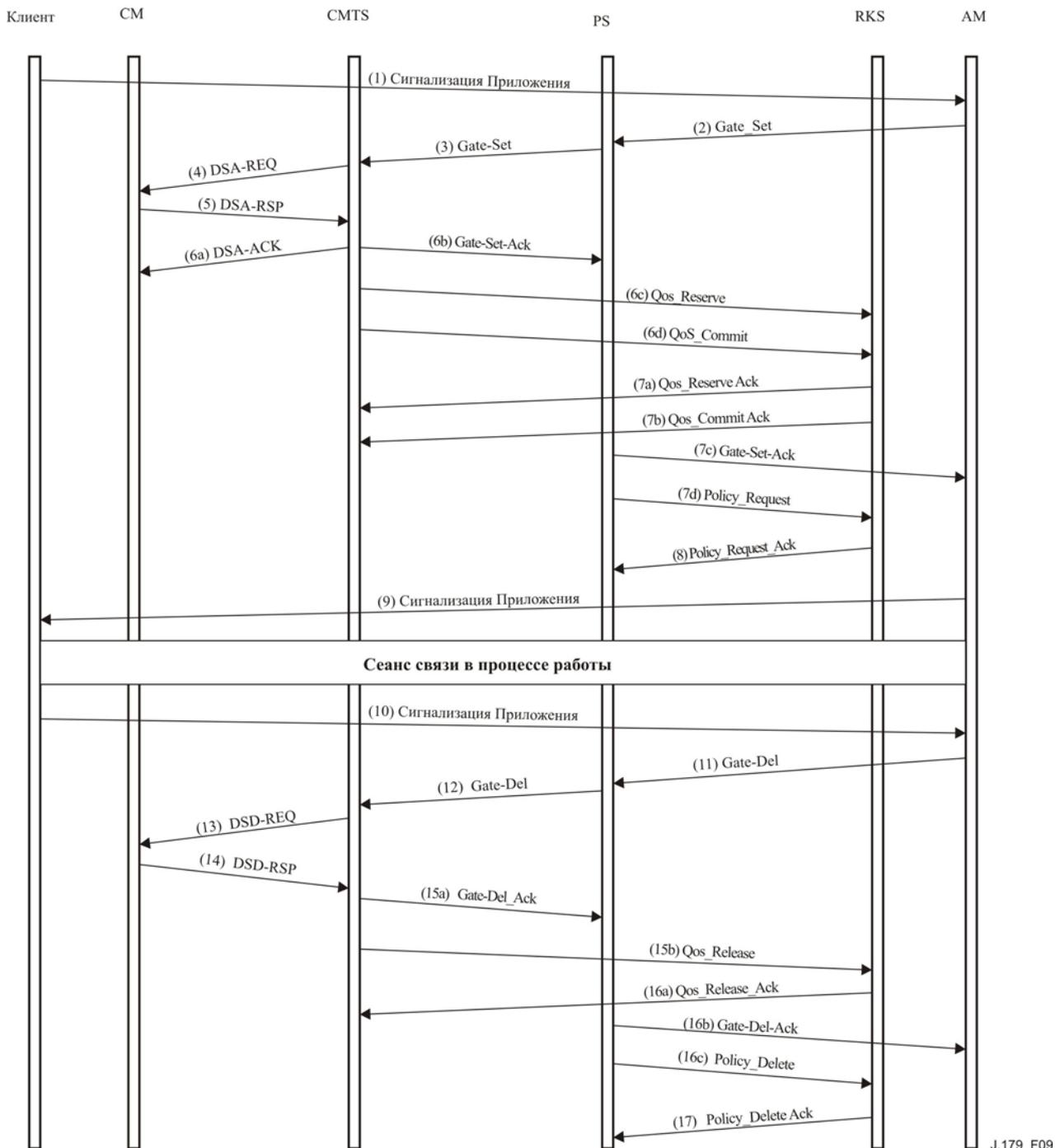


Рисунок 9/J.179 – Подробная последовательность сообщений

Следующие страницы дают подробное описание сообщений, которыми обменивались в примере сеанса мультимедийной сети IP-Cablecom. Число полос частот является только примером и не относится ни к одной из существующих услуг. Только сетевые ресурсы доступа к восходящим потокам данных были зарезервированы и выделены для ясности. Также из сообщений DOCSIS для ясности были удалены TLV (Тип-Длина-Значение (методы, используемые в элементах протокола форматирования)), относящиеся к VPI.

- 1) Клиент инициирует сеанс связи, запрашивая у Менеджера приложений необходимые ресурсы для использования в приложениях. Примером этого может служить видеоигра, загружаемая с носителя, которая запрашивает ресурсы для игры в онлайн. Этот тип сигналов находится вне зоны рассмотрения данной Рекомендации.

- 2) После получения сигналов приложения от клиента, Менеджер приложений отправляет сообщение Gate-Set на Сервер, обеспечивающий выполнение правил, с запросом ресурсов для этого сеанса связи.

0		1		2		3	
Заголовок COPS							
Версия 0x1	Метки 0x0	Код операции 0x02		Тип клиента 0x800A			
Длина сообщения 0x00000088							
Объект описателя COPS							
Длина 0x0008				С-номер 0x01		С-Тип 0x01	
Описатель 0x00001234							
Контекстный объект COPS							
Длина 0x0008				С-номер 0x02		С-Тип 0x01	
Тип запроса (R-Туре) 0x0008 (Запрос конфигурации)				Тип сообщения (M-Туре) 0x0000			
Объект метки решения COPS							
Длина 0x0008				С-номер 0x06		С-Тип 0x01	
Код команды 0x0001 (Конфигурация установки)				Метки 0x0000			
Заголовок Объекта определенных клиентом данных решения COPS							
Длина 0x00A0				С-номер 0x06		С-Тип 0x04	
Мультимедийный объект Идентификатора передачи							
Длина 0x0008				S-номер 0x01		S-Тип 0x01	
Идентификатор передачи 0x9999				Команда шлюза 0x0004 (Gate-Set)			
Мультимедийный объект AMID							
Длина 0x0008				S-номер 0x02		S-Тип 0x01	
AMID 0x00005678							
Мультимедийный объект Идентификатора абонента							
Длина 0x0008				S-номер 0x03		S-тип 0x01	
Идентификатор абонента 0x01010101							
Мультимедийный объект Спецификации Шлюза							
Длина 0x0010				S-номер 0x05		S-тип 0x01	
Метки 0x01	DSCP/TOS поле 0x00			DSCP/TOS маска 0x00		Идентификатор Класса сеанса связи 0x00	
Таймер T1 0x00C8 (200 секунд)				Таймер T2 0x012C (300 секунд)			

0	1	2	3
Таймер T3 0x003C (60 секунд)		Таймер T4 0x001E (30 секунд)	
Мультимедийный объект Спецификации потока			
Длина 0x0024		S-номер 0x07	S-тип 0x01
Формат 0x07	Сервисный номер 0x02	Зарезервировано	Зарезервировано
Комбинированные Авторизованные Зарезервированные и Выделенные Форматы			
Скорость метки сегмента [г] (закодированная как плавающая точка IEEE) 0x461C4000 (10 000 бит/с)			
Размер метки сегмента [b] (закодированный как плавающая точка IEEE) 0x43480000 (200 байт)			
Пиковая скорость данных [р] (закодированная как плавающая точка IEEE) 0x461C4000 (10 000 бит/с)			
Минимальная управляемая единица [m] 0x000000C8 (200 байт)			
Максимальный размер пакета [M] 0x000000C8 (200 байт)			
Скорость [R] (закодированная как плавающая точка IEEE) 0x461C4000 (10 000 бит/с)			
Ненапряженный период времени [S] 0x00000320 (800 μs)			
⋮			
Мультимедийный объект классификатора			
Длина 0x0018		S-номер 0x06	S-Тип 0x01
Зарезервировано	Идентификатор протокола 0x11 (17 UDP)	DSCP/TOS поле 0x00	DSCP/TOS маска 0x00
IP адрес источника 0x01010101			
IP адрес точки назначения 0x02020202			
Порт источника 0x1234		Порт точки назначения 0x9876	
Приоритет 0x0040 (64)		Зарезервировано	

- 3) После того, как PS получит сообщение Gate-Set от Менеджера приложений, он проверяет, авторизован ли запрос и, если да, отправляет сообщение Gate-Set Системе завершения вызова для кабельного модема (CMTS).

0	1	2	3
Заголовок COPS			
Версия 0x1	Метки 0x0	Код операции 0x02	Тип клиента 0x800A
Длина сообщения 0x000000B4			
Объект описателя COPS			
Длина 0x0008		C-номер 0x01	C-тип 0x01
Описатель 0x00005678			
Контекстный объект COPS			

0	1	2	3
Длина 0x0008		С-номер 0x02	С-тип 0x01
Тип запроса (R-Туре) 0x0008 (Запрос конфигурации)		Тип сообщения (M-Туре) 0x0000	
Объект меток решения COPS			
Длина 0x0008		С-номер 0x06	С-тип 0x01
Код команды 0x0001 (Конфигурация установки)		Метки 0x0000	
Заголовок Объекта определенных клиентом данных решения COPS			
Длина 0x00CC		С-номер 0x06	С-тип 0x04
Мультимедийный объект идентификатора передачи			
Длина 0x0008		S-номер 0x01	S-тип 0x01
Идентификатор передачи 0x0001		Команда шлюза 0x0004 (Gate-Set)	
Мультимедийный объект AMID			
Длина 0x0008		S-номер 0x02	S-тип 0x01
AMID 0x00005678			
Мультимедийный объект идентификатора абонента			
Длина 0x0008		S-номер 0x03	S-тип 0x01
Идентификатор абонента 0x01010101			
Мультимедийный объект спецификации шлюза			
Длина 0x0010		S-номер 0x05	S-тип 0x01
Направление 0x01	DSCP/TOS поле 0x00	DSCP/TOS маска 0x00	Идентификатор Класса сеанса связи 0x00
Таймер T1 0x00C8 (200 секунд)		Таймер T2 0x012C (300 секунд)	
Таймер T3 0x003C (60 секунд)		Таймер T4 0x001E (30 секунд)	
Мультимедийный объект спецификации потока			
Длина 0x0024		S-номер 0x07	S-тип 0x01
Формат 0x07	Сервисный номер 0x02	Зарезервировано	Зарезервировано
Комбинированные Авторизованные Зарезервированные и Выделенные форматы			
Скорость метки сегмента [r] (закодированная как плавающая точка IEEE) 0x461C4000 (10 000 бит/с)			
Размер метки сегмента [b] (закодированный как плавающая точка IEEE) 0x43480000 (200 байт)			
Пиковая скорость данных [p] (закодированная как плавающая точка IEEE) 0x461C4000 (10 000 бит/с)			
Минимальная управляемая точка [m] 0x000000C8 (200 байт)			
Максимальный размер пакета [M] 0x000000C8 (200 байт)			
Скорость [R] (закодированная как плавающая точка IEEE) 0x461C4000 (10 000 бит/с)			
Ненапряженный период времени [S] 0x00000320 (800 μ s)			

0	1	2	3
Мультимедийный объект классификатора			
Длина 0x0018		S-номер 0x06	S-тип 0x01
Зарезервировано	Идентификатор протокола 0x11	DSCP/TOS поле 0x00	DSCP/TOS маска 0x00
IP адрес источника 0x01010101			
IP адрес точки назначения 0x02020202			
Порт источника 0x1234		Порт точки назначения 0x9876	
Приоритет 0x0040 (64)		Зарезервировано	
Мультимедийный объект информации создания события			
Длина 0x002C		S-номер 0x08	S-тип 0x01
Адрес первичного Сервера регистрации 0x03030303			
Порт первичного Сервера регистрации 0x1111		Зарезервировано	
Адрес вторичного сервера регистрации 0x04040404			
Порт вторичного сервера регистрации 0x1111		Зарезервировано	
BCID 0x3e4812082020202020313436302d3035303030300003db77			

- 4) Если контроль допуска Системы завершения вызова для кабельного модема (CMTS) был осуществлен успешно, то CMTS начнет инициирование резервирования и выделения сетевых ресурсов доступа, отправив DSA на Кабельный модем.

0	1	2	3
Заголовок управления MAC			

Идентификатор передачи 0x0007		Поток услуги US 0x18	Длина 0x29
Идентификатор потока услуги 0x02	Длина 0x04	Значение 0x0000	
Значение (прод.) 0001		Идентификатор услуги 0x03	Длина 0x02
Значение 0x0001		Установка параметров QoS 0x06	Длина 0x01
Значение 0x06 (Ad.+Act.)	Тип планирования 0x0F	Длина 0x01	Значение 0x06
Размер UGS 0x13	Длина 0x02	Значение 0x00E8 (232 байта)	
Ном. Инт. разр. сигнала 0x14	Длина 0x04	Значение 0x0000	

0	1	2	3
Значение (прод.) 4E20 (20 000 µs)		Количество разрешающих сигналов за Интервал 0x16	Длина 0x01
Значение 0x01	RX/TX Правило 0x10	Длина 0x04	Значение 0x00
Значение (прод.) 00017F			Доп. уровень неустойчивой синхронизации 0x15
Длина 0x04	Значение 0x000003		
Значение (прод.) 20 (800 µs)	Классификатор пакета US 0x16	Длина 0x0x2B	ID классификатора 0x02
Длина 0x02	Значение 0x0001		Идентификатор потока услуг 0x04
Длина 0x04	Значение 0x000000		
Длина (прод.) 01	Приоритет правила 0x05	Длина 0x01	Значение 0x40
Состояние действия классификатора 0x06	Длина 0x01	Значение 0x01 (активное)	Классификатор пакета IP 0x09
Длина 0x001A	Протокол IP 0x02	Длина 0x02	Значение 0x00
Значение (прод.) 11 (17 UDP)	Адрес источника IP 0x03	Длина 0x04	Значение 0x01
Значение (прод.) 010101			Старт порта источника IP 0x07
Длина 0x02	Значение 0x1234		Конец порта источника IP 0x08
Длина 0x02	Значение 0x1234		Старт порта назначения IP 0x09
Длина 0x02	Значение 0x9876		Конец порта назначения IP 0x0A
Длина 0x02	Значение 0x9876		

5) CM отвечает Системе завершения вызова для кабельного модема (CMTS) сообщением DSA-RSP.

0	1	2	3
MAC Заголовок управления			

Идентификатор передачи 0x0007		Код подтверждения 0x00	

6а) CMTS завершает передачу сообщением DSA-ACK.

0	1	2	3
MAC Заголовок управления			

Идентификатор передачи 0x0007		Код подтверждения 0x00	

- 6b) После того, как сообщение DSA-RSP будет получено Системой завершения вызова для кабельного модема (CMTS) от Кабельного модема (CM) с подтверждением успешной передачи, CMTS пошлет сообщение Gate-Set-Ack на Сервер, обеспечивающий выполнение правил.

0		1		2		3	
Заголовок COPS							
Версия 0x1	Метки 0x1	Код операции 0x03		Тип клиента 0x800A			
Длина сообщения 0x0000003C							
Объект описателя COPS							
Длина 0x0008				С-номер 0x01		С-тип 0x01	
Описатель 0x00005678							
Объект типа сообщения COPS							
Длина 0x0008				С-номер 0x12		С-тип 0x01	
Тип сообщения (R-Type) 0x0001 (Успешно)				Зарезервировано			
Заголовок объекта SI клиента COPS							
Длина 0x0024				С-номер 0x09		С-тип 0x01	
Мультимедийный объект идентификатора передачи							
Длина 0x0008				S-номер 0x01		S-тип 0x01	
Идентификатор передачи 0x0001				Команда шлюза 0x0005 (Gate-Set-Ack)			
Мультимедийный объект AMID							
Длина 0x0008				S-номер 0x02		S-тип 0x01	
AMID 0x00005678							
Мультимедийный объект идентификатора абонента							
Длина 0x0008				S-номер 0x03		S-тип 0x01	
Идентификатор абонента 0x01010101							
Мультимедийный объект идентификатора шлюза							
Длина 0x0008				S-номер 0x04		S-тип 0x01	
Идентификатор шлюза 0x12345678							

- 7а) После получения и записи сообщения о событии QoS_Reserve RKS подтверждает получение сообщения.

0	1	2	3
Заголовок Ответа на запрос отчета Radius			

- 7б) После получения и записи сообщения о событии QoS_Commit RKS подтверждает получение сообщения.

0	1	2	3
Заголовок Ответа на запрос отчета Radius			

- 7с) Как результат получения сообщения Gate-Set-Ack (Запроса на установку шлюза) от Системы завершения вызова для кабельного модема (CMTS), Сервер, обеспечивающий выполнение правил, отправит сообщение Gate-Set-Ack Менеджеру приложений для завершения передачи.

0	1	2	3
Заголовок COPS			
Версия 0x1	Метки 0x1	Код операции 0x03	Тип клиента 0x800A
Длина сообщения 0x0000003C			
Объект описателя COPS			
Длина 0x0008		С-номер 0x01	С-тип 0x01
Описатель 0x00001234			
Объект типа сообщения COPS			
Длина 0x0008		С-номер 0x12	С-тип 0x01
Тип сообщения (R-Type) 0x0001 (Удалено)		Зарезервировано	
Заголовок сообщения SI клиента COPS			
Длина 0x0024		С-номер 0x09	С-тип 0x01
Мультимедийный объект идентификатора передачи			
Длина 0x0008		S-номер 0x01	S-тип 0x01
Идентификатор передачи 0x9999		Команда шлюза 0x0005	
Мультимедийный объект AMID			
Длина 0x0008		S-номер 0x02	S-тип 0x01
AMID 0x00005678			
Мультимедийный объект идентификатора абонента			
Длина 0x0008		S-номер 0x03	S-тип 0x01
Идентификатор абонента 0x01010101			

0	1	2	3
Мультимедийный объект идентификатора шлюза			
Длина 0x0008		S-номер 0x04	S-тип 0x01
Идентификатор шлюза 0x12345678			

7d) Сервер, обеспечивающий выполнение правил, также отправит сообщение о событии Policy_Request на RKS, для того чтобы проследить Запрос правила и соответственный отклик.

0	1	2	3
Заголовок запроса отчета Radius			

Спец. поставщика Radius 0x1A	Длина 0x54	Идентификатор поставщика 0x0000	
Идентификатор поставщика (прод.) 118B		Тип (Заголовок EM) 0x01	Длина 0x4E
Версия 0x0001		BCID 0x3E48	
BCID (прод.) 12082020202020313436302D3035303030300003DB77			

		Тип сообщения о событиях 0x0015 (Policy_Request)	
Тип элемента 0x0004 (Сервер, обеспечивающий выполнение правил)		Идентификатор элемента 0x2020202035363738	

Временная зона 0x302E303530303030			

Номер последовательности 0x0000			
Номер последовательности (прод.) 0001		Время события 0x3230	
Время события (прод.) 30333132303630303030302E323130			

Состояние 0x00000000			
Приоритет 0x80 (128)	Счетчик атрибута 0x0004		Объект события 0x00
Спец. поставщика Radius 0x1A	Длина 0x0C	Идентификатор поставщика 0x0000	
Идентификатор поставщика (прод.) 118B		Тип 0x3D	Длина 0x06
Идентификатор Менеджера приложений 0x00005678			
Спец. поставщика Radius 0x1A	Длина 0x0C	Идентификатор поставщика 0x0000	
Идентификатор поставщика (прод.) 118B		Тип 0x34	Длина 0x06

0	1	2	3
Идентификатор абонента 0x01010101			
Спец. поставщика Radius. 0x1A	Длина 0x0A	Идентификатор поставщика 0x0000	
Идентификатор поставщика (прод.) 118B		Тип 0x3C	Длина 0x04
Состояние принятые решения 0x0001 (Правило принято)		Спец. поставщика Radius 0x1A	Длина 0x1C
Идентификатор поставщика 0x0000118B			
Тип 0x31	Длина 0x16	FEID 0x0000	
FEID (прод.) 000000000000005061636B65744361626C65			

- 8) После получения и записи сообщения о событии Policy_Request RKS подтверждает получение сообщения.

0	1	2	3
Заголовок ответа на запрос отчета Radius			

- 9) Менеджер приложений ответит клиенту, чтобы проинформировать его о том, что он теперь может играть в игру. Данные сигналы находятся вне рассмотрения данной Рекомендации.
- 10) Когда клиент закончит работу с приложением, он уведомит Менеджер приложений. Данные сигналы находятся вне рассмотрения данной Рекомендации.
- 11) Менеджер приложений завершит сеанс связи, отправив сообщение Gate-Delete на Сервер, обеспечивающий выполнение правил.

0	1	2	3
Заголовок COPS			
Версия 0x1	Метки 0x0	Код операции 0x02	Тип клиента 0x800A
Длина сообщения 0x00000044			
Объект описателя COPS			
Длина 0x0008		С-номер 0x01	С-тип 0x01
Описатель 0x00001234			
Контекстный объект COPS			
Длина 0x0008		С-номер 0x02	С-тип 0x01
Тип запроса (R-Type) 0x0008 (Запрос настройки)		Тип сообщения (M-Type) 0x0000	
Объект меток решения COPS			
Длина 0x0008		С-номер 0x06	С-тип 0x01

0	1	2	3
Код команды 0x0001 (Настройка установки)		Метки 0x0000	
Заголовок объекта решения данных принятия, определенных клиентом COPS			
Длина 0x0014		С-номер 0x06	С-тип 0x04
Мультимедийный объект идентификатора передачи			
Длина 0x0008		С-номер 0x01	С-тип 0x01
Идентификатор передачи 0x9998		Команда шлюза 0x000A (Gate-Delete)	
Мультимедийный объект AMID			
Длина 0x0008		С-номер 0x02	С-тип 0x01
AMID 0x00005678			
Мультимедийный объект идентификатора абонента			
Длина 0x0008		С-номер 0x03	С-номер 0x01
Идентификатор абонента 0x01010101			
Мультимедийный объект идентификатора шлюза			
Длина 0x0008		С-номер 0x04	С-тип 0x01
Идентификатор шлюза 0x12345678			

- 12) Сервер, обеспечивающий выполнение правил, даст указание Системе завершения соединения для кабельного модема (CMTS) разорвать сеанс связи, отправив сообщение Gate-Delete.

0	1	2	3
Заголовок COPS			
Версия 0x1	Метки 0x0	Код операции 0x02	Тип клиента 0x800A
Длина сообщения 0x00000044			
Объект описателя COPS			
Длина 0x0008		С-номер 0x01	С-тип 0x01
Описатель 0x00005678			
Контекстный объект COPS			
Длина 0x0008		С-номер 0x02	С-тип 0x01
Тип запроса (R-Type) 0x0008 (Запрос настройки)		Тип сообщения (M-Type) 0x0000	
Объект меток решения COPS			
Длина 0x0008		С-номер 0x06	С-тип 0x01
Код команды 0x0001 (Настройка установки)		Метки 0x0000	
Заголовок объекта решения данных принятия, определенных клиентом COPS			

0	1	2	3
Длина 0x0014		С-номер 0x09	С-тип 0x01
Мультимедийный объект идентификатора передачи			
Длина 0x0008		С-номер 0x01	С-тип 0x01
Идентификатор передачи 0x0002		Команда шлюза 0x000A (Gate-Delete)	
Мультимедийный объект AMID			
Длина 0x0008		С-номер 0x02	С-тип 0x01
AMID 0x00005678			
Мультимедийный объект идентификатор абонента			
Length 0x0008		S-Num 0x03	S-Type 0x01
Идентификатор абонента 0x01010101			
Мультимедийный объект идентификатора шлюза			
Длина 0x0008		С-номер 0x04	С-тип 0x01
Идентификатор шлюза 0x12345678			

13) CMTS снимет резервацию сетевых ресурсов доступа, отослав сообщение DSD-REQ на CM.

0	1	2	3
MAC заголовок управления			

Идентификатор передачи 0x0008		Зарезервировано	
SFID 0x00000001			

14) CM подтвердит удаление сеанса связи, отослав сообщение DSD-RSP.

0	1	2	3
MAC заголовок управления			

Идентификатор передачи 0x0008		Код подтверждения 0x00	Зарезервировано

15a) CMTS завершит передачу события Gate-Control, отослав сообщение Gate-Delete-Ack.

0	1	2	3
Заголовок COPS			
Версия 0x1	Метки 0x1	Код операции 0x03	Тип клиента 0x800A

0	1	2	3
Длина сообщения 0x00000034			
Объект описателя COPS			
Длина 0x0008		С-номер 0x01	С-тип 0x01
Описатель 0x00005678			
Объект типа сообщения COPS			
Длина 0x0008		С-номер 0x12	С-тип 0x01
Тип сообщения (R-Type) 0x0001	Зарезервировано		
Заголовок объекта SI клиента COPS			
Длина 0x001C		С-номер 0x09	С-тип 0x01
Мультимедийный объект идентификатора передачи			
Длина 0x0008		S-номер 0x01	S-тип 0x01
Идентификатор передачи 0x0002	Команда шлюза 0x000B (Gate-Delete-Ack)		
Мультимедийный объект AMID			
Длина 0x0008		S-номер 0x02	S-тип 0x01
AMID 0x00005678			
Мультимедийный объект идентификатора шлюза			
Длина 0x0008		S-номер 0x04	S-тип 0x01
Идентификатор шлюза 0x12345678			

- 15b) Также после получения сообщения DSD-RSP, CMTS проинформирует RKS о том, что сетевые ресурсы доступа были освобождены, отправив сообщение о событии QoS_Release.

0	1	2	3
Заголовок запроса отчета Radius			

Спец. поставщика Radius 0x1A	Длина 0x54	Идентификатор поставщика 0x0000	
Идентификатор поставщика (прод.) 118B		Тип (Заголовок EM) 0x01	Длина 0x4E
Версия 0x0001		BCID 0x3E48	
BCID (прод.) 120820202020313436302D3035303030300003DB77			

		Тип сообщения о событии 0x0008 (QoS_Release)	
Тип элемента 0x0002 (CMTS)		Идентификатор элемента 0x2020202031323334	

Временная зона 0x302D303530303030			

0	1	2	3
		Номер последовательности 0x0000	
Номер последовательности (прод.) 0003		Время события 0x3230	
Время события (прод.) 30323132303630303030302E333030			
Состояние 0x00000000			
Приоритет 0x80 (128)	Счетчик атрибута 0x0005		Объект события 0x00
Спец. поставщика Radius 0x1A	Длина 0x0C	Идентификатор поставщика 0x0000	
Идентификатор поставщика (cont.) 118B		Тип 0x1E	Длина 0x06
SF_ID 0x00000001			
Спец. поставщика Radius 0x1A	Длина 0x0A	Идентификатор поставщика 0x0000	
Идентификатор поставщика (прод.) 118B		Тип 0x32	Длина 0x04
Направление потока 0x0001 (восходящий)		Спец. поставщика Radius 0x1A	Длина 0x0A
Идентификатор поставщика 0x0000118B			
Тип 0x38	Длина 0x04	Причина освобождения QoS 0x0001 (PS закрыл шлюз)	
Спец. поставщика Radius 0x1A	Длина 0x0C	Идентификатор поставщика 0x0000	
Идентификатор поставщика (прод.) 118B		Тип 0x36	Длина 0x06
Информация по использованию QoS 0x77777777 (байт)			
Спец. поставщика Radius 0x1A	Длина 0x0C	Идентификатор поставщика 0x0000	
Идентификатор поставщика (прод.) 118B		Тип 0x3F	Длина 0x06
Информация по времени QoS 0x77777777 (секунд)			

16а) После получения и записи сообщения о событиях QoS_Release RKS подтверждает получение сообщения.

0	1	2	3
Заголовок ответа на запрос отчета Radius			

- 16b) После получения Gate-Delete-Ack от Системы завершения соединения для кабельного модема (CMTS) Сервер, обеспечивающий выполнение правил, пошлет Gate-Delete-Ack для завершения передачи Gate-Control.

0		1		2		3	
Заголовок COPS							
Версия 0x1	Метки 0x1	Код операции 0x03		Тип клиента 0x800A			
Длина сообщения 0x00000034							
Объект описателя COPS							
Длина 0x0008				С-номер 0x01		С-тип 0x01	
Описатель 0x00001234							
Объект типа сообщения COPS							
Длина 0x0008				С-номер 0x12		С-тип 0x01	
Тип сообщения (R-Type) 0x0001 (Удачное)				Зарезервировано			
Заголовок объекта SI клиента COPS							
Длина 0x001C				С-номер 0x09		С-тип 0x01	
Мультимедийный объект идентификатора передачи							
Длина 0x0008				S-номер 0x01		S-тип 0x01	
Идентификатор передачи 0x9998				Команда шлюза 0x000B (Gate-Delete-Ack)			
Мультимедийный объект AMID							
Длина 0x0008				S-номер 0x02		S-тип 0x01	
AMID 0x00005678							
Мультимедийный объект идентификатора шлюза							
Длина 0x0008				S-номер 0x04		S-тип 0x01	
Идентификатор шлюза 0x12345678							

- 16с) Сервер, обеспечивающий выполнение правил, отправляет сообщение о событии Policy_Delete на RKS, для того чтобы завершить текущий процесс.

0		1		2		3	
Заголовок запроса отчета Radius							

Спец. поставщика Radius 0x1A		Длина 0x54		Идентификатор поставщика 0x0000			
Идентификатор поставщика (прод.) 118B				Тип (Заголовок EM) 0x01		Длина 0x4E	
Версия 0x0001				BCID 0x3E48			
BCID (прод.) 12082020202020313436302D3035303030300003DB77							

0	1	2	3
		Тип сообщения о событии 0x0016 (Policy_Delete)	
Тип элемента 0x0004 (Сервер, обеспечивающий выполнение правил)		Идентификатор элемента 0x2020202035363738	
		Временная зона 0x302D303530303030	
		Номер последовательности 0x0000	
Номер последовательности (прод.) 0002		Время события 0x3230	
Время события (прод.) 3032313230363030303030302E343030			
Состояние 0x00000000			
Приоритет 0x80	Счетчик атрибута 0x0004		Объект события 0x00
Спец. поставщика Radius 0x1A	Длина 0x0C	Идентификатор поставщика 0x0000	
Идентификатор поставщика (прод.) 118B		Тип 0x3D	Длина 0x06
Идентификатор Менеджера приложений 0x00005678			
Спец. поставщика Radius. 0x1A	Длина 0x0C	Идентификатор поставщика 0x0000	
Идентификатор поставщика (прод.) 118B		Тип 0x34	Длина 0x06
Идентификатор абонента 0x01010101			
Спец. поставщика Radius 0x1A	Длина 0x0A	Идентификатор поставщика 0x0000	
Идентификатор поставщика (прод.) 118B		Тип 0x3A	Длина 0x04
Причина удаления правила 0x0001 (Запрос Менеджера приложений)		Спецификация поставщика Radius 0x1A	Длина 0x1C
Идентификатор поставщика 0x0000118B			
Тип 0x31	Длина 0x16	FEID 0x0000	
FEID (прод.) 000000000000005061636B65744361626C65			

- 17) После получения и записи сообщения о событиях Policy_Delete RKS подтверждает получение сообщений.

0	1	2	3
Заголовок ответа на запрос отчета Radius			

11 Выводы для последующего изучения

Следующие выводы были определены как предметы обсуждения для последующего изучения.

- Требования к работе с ошибками (т.е. обязательные коды для определенных ошибок для определенных условий)
- Сообщение Gate Control, направляемое в пределах структуры мультимедийной сети.
- Требования синхронизации состояния (т.е. степень синхронизации, масштаб, частота и т.п.) и механизм протокола.
- Поддержка протокола для перехвата управления и стратегий избыточности. Также, каким образом шлюзы должны управляться во время события неудавшегося COPS соединения.
- Формат управления Сервера, обеспечивающего выполнение правил, и механизм снабжения: обеспечение Сервера управления звонками (CMS) настроенными для работы с мультимедиа XML описаниями типа документа (DTD).
- Поддержка для Подавления Заголовка Полезной Загрузки (PHS).
- Доставка сообщения Контроля Шлюза при неудавшемся соединении (в настоящее время такие сообщения удаляются).

Приложение I

Основная информация

I.1 Введение

В этом приложении описывается архитектура, которая обеспечивает платформу на базе IP для поддержки разнообразия мультимедийных приложений и услуг, требующих обработки QoS для доступа к сетевым Серверам Регистрации (RKS) в сети CableModem. Эта архитектура определяет функциональные компоненты и интерфейсы протоколов, которые позволят каждому кабельному оператору поставлять улучшенные с помощью QoS мультимедийные услуги, которые отвечают их уникальным требованиям бизнеса.

Так как данная архитектура не зависит от деталей уровней приложений определенных мультимедийных предложений, специальных обеспечений, сигналов и Системы поддержки Операций (OSS), функции, требуемые для обеспечения определенной услуги, не рассматриваются в данной Рекомендации. Более того, мультимедийная сеть IPcablecom сосредотачивается на поставке надежных Качеств Услуг (QoS) в сети доступа, особо выделяя технические проблемы правила авторизации, сигналы QoS, учет использования ресурсов и безопасность.

I.1.1 Обзор IPcablecom

Проект IPcablecom нацелен на определение спецификаций интерфейса, используемого поставщиками для развития взаимодействующего оборудования, способного поддерживать передачу по каналам IP голоса, видеофайлов и других высокоскоростных услуг мультимедиа через кабельные системы на основе Гибридного соединения – оптоволоконно/коаксиальный кабель (HFC), которые соответствуют Рекомендациям по широкополосному сетевому доступу Cablecom.

Голос по каналам IP (VoIP) был первой такой услугой, предназначенной для доставки на базе платформы IPcablecom. Текущий набор Рекомендаций IPcablecom, вместе известных как IPcablecom-T, определяет собой архитектуру IPcablecom, оптимизированную для доставки резидентных услуг VoIP. Смотри Рекомендацию МСЭ-Т J.160.

I.1.2 Мультимедийная мотивация IPcablecom

Как и VoIP, наиболее популярные мультимедийные приложения (к примеру, игры онлайн, потоковые медиа-средства, видеообщение в реальном) чувствительны к времени задержки передачи в пределах сети. Далее, после того, как появляются новые приложения, предназначенные для использования преимуществ сетей, они также предъявляют свои уникальные требования по полосе частот и времени задержки.

В настоящее время пользователи широкополосных услуг получают мультимедийные услуги через доставку данных по "Наилучшему из возможных". Это приводит к противоречивым онлайн-результатам, которые различаются по качеству, исходя из возможности полосы частот и загруженности сети. Сеть, которая может резервировать ресурсы и предоставлять полосу частот по требованию, как указывают сервисные требования, сможет считаться способной предоставить большое разнообразие новых услуг своим пользователям.

С целью направить эти потребности для услуг VoIP, IPcablecom на данный момент назначил механизмы сигналов динамического Качества Услуг (DQoS), которые позволяют голосовым приложениям запрашивать и получать полосу частот от слоя канала передачи данных CableModem. Текущая структура DQoS также поддерживает установление безопасного сеанса связи путем аутентификации и авторизации конечной точки и базирующейся на QoS модели отслеживания использования. Исходя из этих основных возможностей, архитектура IPcablecom хорошо подходит для поддержки существующих и будущих приложений, улучшенных при помощи Качества Услуг (QoS), и услуг кроме одной только телефонии.

Основной целью мультимедийной сети IPcablecom является определение основной структуры архитектуры, предназначенной для поддержки мультимедийных приложений на базе QoS. Как центр этой структуры определены механизмы Качества Услуг в CableModem и DQoS Спецификациях IPcablecom. Успешное завершение этого начинания обеспечит сильное техническое основание для поддержки предложений специфических мультимедийных услуг, о которых будет сказано в дальнейшем.

I.2 Объекты и рамки мультимедийной сети IPCom

Главной целью мультимедийной сети IPCom является развитие архитектуры общего назначения, которая:

- Поддерживает широкий спектр услуг, предоставленных QoS, кроме одного только голоса;
- Основана на существующих механизмах, определенных в Рекомендациях IPCom-T и CableModem;
- Требуется минимальный набор расширений, кроме только IPCom-T;
- Уменьшает развитие запутанности путем удаления требований, специфических для телефонии, там, где они не применяются (к примеру, межсоединение Телефонной сети общего пользования (PSTN), электронное наблюдение, модели телефонного биллинга и т. д.);
- Сосуществует с архитектурой IPCom-T таким образом, что:
 - требований мультимедийной сети IPCom достаточно для поддержки базирующейся на QoS платформе доставки мультимедийных услуг;
 - требования мультимедийной сети IPCom могут быть добавлены к уже существующим значимым функциональным компонентам сети IPCom-T;
 - требования сети IPCom-T могут быть добавлены к значимым функциональным компонентам мультимедийной сети IPCom;
- Поддерживает Адаптеры мультимедийного терминала (MTA) IPCom-T как устройства "Типа клиента 2" (определенные внутри) в мультимедийной архитектуре IPCom;
- Взаимодействует с IPCom2Home (МСЭ-Т Рек. J.191) и CableModem (МСЭ-Т Рекомендации J.112 и J.122) архитектурами.

Этот раздел описывает требования, которые были определены с намерением удовлетворить вышеуказанные требования и обрисовать общий план работ, которые были инициированы архитектурой.

I.2.1 Требования

Данная архитектура описывает в общих чертах взаимодействие разных элементов сети, включая Устройства Клиента, Менеджеры приложений, Серверы, обеспечивающие выполнение правил, Системы завершения вызова для кабельных модемов (CMTS) и Кабельные Модемы. Эти элементы сети формально определены в разделе Структуры Мультимедиа этого Приложения. Тем не менее, для некоторых из этих сетевых элементов были сделаны специфические допущения касательно полномочий управления и отношений доверия, и эти допущения зафиксированы ниже как Требования мультимедийной сети IPCom. Требования высокого уровня относительно сигналов QoS, управления ресурсами, сообщений о событиях и безопасности также включены в этот раздел.

IPCom Multimedia является сигналами приложения, безразличными к протоколу взаимодействия между Устройствами Клиента и Менеджером приложений. Считается, что Устройства Клиента и Менеджер приложений могут поддерживать многообразие приложений и протоколов сигналов (к примеру, HTTP, SIP, H.323, DCS, NCS и др.).

Устройства Клиента в архитектуре мультимедийной сети IPCom:

- 1) находятся непосредственно в сети доступа оператора или в доме;
- 2) могут быть автономными устройствами или могут содержать встроенный Кабельный модем; и
- 3) являются обоснованно недоверенными элементами сети, и, исходя из этого, для них в сети оператора могут потребоваться некоторые формы аутентификации пользователя, приложения или сообщения приложения.

Менеджеры приложений в архитектуре мультимедийной сети IPCom:

- 1) находятся в сети, управляемой оператором;
- 2) управляются оператором; и
- 3) отвечают за то, что клиентский Запрос услуги от сети оператора будет авторизован, с тем чтобы получить данную услугу.

Серверы, обеспечивающие выполнение правил, в архитектуре мультимедийной сети IP-Cablecom:

- 1) находятся в сети, управляемой оператором;
- 2) управляются оператором; и
- 3) отвечают за принятие правил, относящихся к QoS, основанных на правилах, установленных оператором.

Системы завершения вызова для кабельных модемов (CMTS) в архитектуре мультимедийной сети IP-Cablecom отвечают за выполнение решений, относящихся к QoS.

QoS сигналы и требования управления ресурсами:

- Механизмы динамического запроса ресурсов должны определяться, включая в себя:
 - Доступ ко всем моделям планирования QoS кабельного модема;
 - Запросы ресурсов, ограниченных временем;
 - Запросы ресурсов, ограниченных объемом.
- Должны поддерживаться однофазные и двухфазные модели резервирования ресурсов.
- Должны поддерживаться однонаправленные резервирования; должна быть разрешена поддержка двунаправленных резервирований.
- Менеджеры приложений могут инициировать запросы резервирования от лица Абонентского оборудования.
- Архитектура должна обеспечивать способы обнаружения ошибки сервера и/или клиента и восстанавливать соответствующие ресурсы.

Требования к сбору информации в сообщении о событии:

- Должен быть определен полный набор сообщений о событиях, для того чтобы отслеживать использование ресурсов источника, включая:
 - Событие правила, указывающее на запрос ресурсов доступа к сети, подчиненных правилам, определенным оператором;
 - Событие правила, указывающее на освобождение ресурсов доступа к сети;
 - События QoS, указывающие на резервирование, предоставление и освобождение ресурсов QoS;
 - Добавочную поддержку (и) использования ресурсов потока, основанного на объеме (счетчики измеренных пакетов).
- Следующая информация должна содержаться в сообщениях:
 - Источник запроса (к примеру, абонент или поставщик услуги);
 - Характеристики запрошенных ресурсов;
 - Решение по авторизации правила.

Требования безопасности:

- Защита требуется и должна быть назначена для значимых интерфейсов.
- Клиенты, которые инициируют сигналы QoS, могут затребовать некоторые формы авторизации пользователя или приложения.

1.2.2 Обзор

Следующие пункты описывают в общих чертах текущий обзор начальной фазы инициативы мультимедийной сети IP-Cablecom:

- Архитектура будет обращаться к элементам сети, которые находятся:
 - 1) в сети доступа; или
 - 2) в пределах одной IP сети, управляемой оператором.

- Архитектура определит протоколы и потребности интерфейсов для поддержки правил авторизации, контроля допуска, QoS, учета ресурсов и механизмов безопасности.
- Архитектура не будет обращаться к вопросам, специфическим для приложения (к примеру, обеспечение услуг, сигнализация, биллинг и др.).
- Архитектура не будет обращаться к обеспечению и требованиям OSS для элементов мультимедийной сети IPCom.
- Архитектура сосредоточится на управлении QoS между CMTS и CM.
- Архитектура не предотвратит поставку широковещательных услуг, даже она однозначно не предназначена для широковещательных анализов.
- Архитектура не будет обращаться к прослеживанию Перевода Сетевого Адреса (NAT) и требованиям взаимодействия в данное время.
- Архитектура не сможет во время данной фазы определить сквозные требования QoS.
- Архитектура не предоставит поддержку для "Типа Клиента 1" и "Сценария 1" (как определено внутри) во время данной фазы. С целью иметь завершенность и учета будущих разработок это приложение описывает все три типа клиентов и все три сценария.
- Архитектура не обеспечит открытия динамической топологии (т.е. взаимоотношений между Менеджерами Приложений, Серверами, обеспечивающими выполнение правил, Системами завершения вызова для кабельных модемов (CMTS), Серверами Регистрации (RKS) и пр.) на данном этапе.
- Архитектура не будет обращаться к аутентификации Клиента Менеджером приложений.
- Архитектура не будет обращаться к специфическим механизмам, с помощью которых Сервер, обеспечивающий выполнение правил, обеспечивает и управляет правилами.
- Архитектура не будет поддерживать сбор приложений или событий, специфических для услуг, для воплощения в аудит использования ресурсов.

I.3 Структура мультимедийной сети IPCom

Для облегчения поставки качественных широкополосных мультимедийных приложений, требующих гарантий QoS, мультимедийная структура предлагает выполняемые QoS функции общего назначения, основанные на механизмах, определенных в основной части спецификаций IPCom-T. Для поддержки этой цели, несколько ключевых элементов сети было определено и запрофилировано. На Рисунке I.1 изображены компоненты мультимедийной сети IPCom, которые находятся внутри IPCom, управляемой оператором.



Рисунок I.1/J.179 – Элементы мультимедийной сети оператора

В дополнение к возможностям на базе параметров QoS, содействующих CMTS, архитектура мультимедийной сети оператора состоит из группы серверов, которая может быть в дальнейшем разделена на следующие области:

- Менеджер приложений и (дополнительно) Мультимедийный сервер, исполняющий роль ведущего узла для приложений, инициированных QoS;
- Структура администрирования правила, обеспечивающая авторизацию QoS и контроль допущений во время поддержки управления сетевыми ресурсами потока;
- Подсистема обмена сообщениями о событии, используемая для мониторинга и записи информации по использованию ресурсов.

Системы поддержки операций для обеспечения снабжения, управления сетью и функциями мониторинга могут также быть включены в настройку мультимедийной сети оператора, хотя эти элементы выходят за рамки обзора данной архитектуры.

1.3.1 Модель отношения архитектуры мультимедийной сети IP-Cablecom

В дополнение к элементам, находящимся внутри сети центрального блока управления оператора, некоторое количество абонентского оборудования, находящегося в предпосылках клиента, также было определено с целью завершенности модели. На Рисунке I.2 показана структура архитектуры мультимедийной сети IP-Cablecom и устанавливаются ключевые интерфейсы между компонентами. Данные интерфейсы были отмечены идентификаторами, которые будут описаны в последующем обсуждении.

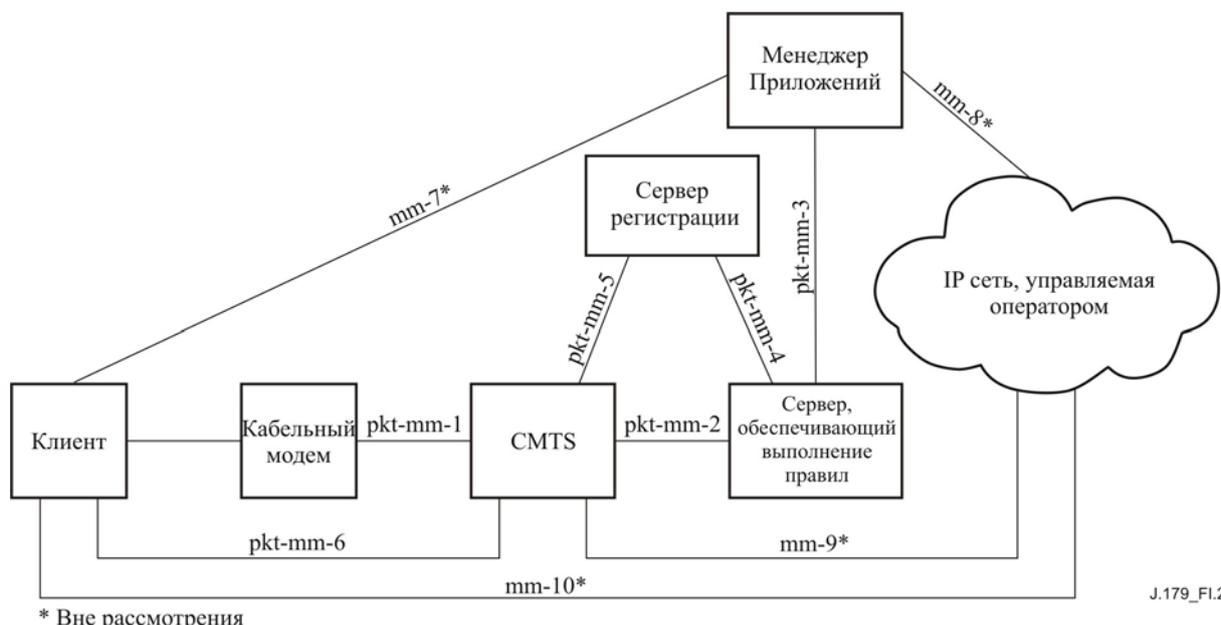


Рисунок I.2/J.179 – Структура архитектуры мультимедийной сети IP-Cablecom

В этой архитектуре Клиенты могут поддерживать или не поддерживать структуру мультимедийной сети IP-Cablecom. Клиенты, поддерживающие структуру и ее механизмы сигналов QoS, явно запрашивают сетевые ресурсы от своего собственного имени, которые авторизованы в центральном блоке управления Сервером, обеспечивающим выполнение правил. Клиенты, которые не поддерживают механизмы сигналов QoS, запрашивают сетевые ресурсы от своего имени посредством Менеджера приложений, с которым они взаимодействуют.

Вне зависимости от метода сигнализации QoS, запросы ресурсов сети доступа всегда подчиняются правилам, которые регулируются на Системе завершения вызова для кабельного модема (CMTS), которая выступает как Точка обязательного выполнения стратегического решения (PEP) и реализована на Сервере, обеспечивающем выполнение правил (PS), который выступает как Точка принятия стратегического решения (PDP).

- Принятые правила могут быть получены Системой завершения вызова для кабельного модема (CMTS) от Сервера, обеспечивающего выполнение правил. В таком случае CMTS однозначно трактует Запрос правила, как результат в данное время неавторизованного, однако

совместимого запроса ресурса QoS. Основываясь на конечном решении, исходный запрос QoS обслуживается или отклоняется.

- В качестве альтернативы, принятые решения могут направляться на CMTS Сервером, обеспечивающим выполнение правил. В этом случае Сервер, обеспечивающий выполнение правил, установит выполнение правила раньше запроса ресурса QoS, основываясь на запросе правила, исходящего от Менеджера приложений. Менеджер приложений создает такой запрос, основываясь на взаимодействии с Клиентом (посредством некоторых необозначенных механизмов сигнализации).

Как Сервер, обеспечивающий выполнение правил, так и CMTS создают сообщения о событии, для того чтобы отследить запросы QoS и их использование. Такие сообщения о событии посылаются на Сервер регистрации (RKS), где они могут быть использованы для биллинга или других целей учета.

В Таблице I.1 описываются все интерфейсы, которые присутствуют на Рисунке I.2. Интерфейсы, определенные в данной Рекомендации, маркируются как "pkt-mm-x", другие же интерфейсы, включенные для полноты, маркируются как "mm-x".

Таблица I.1/J.179 – Мультимедийные интерфейсы сети IP-Cablecom

Интерфейс	Описание	Примечание
pkt-mm-1	CMTS – CM	CM может запросить QoS у CMTS посредством сигналов DSx сети CableModem. С другой стороны, CMTS может указать Кабельному Модему (CM) настроить, разорвать или изменить Поток услуг сети CableModem с целью обеспечить запрос QoS, также посредством сигнализации DSx.
pkt-mm-2	PS – CMTS	Этот интерфейс является основным для структуры управления правилами. Он контролирует Принятие решения, которое может: а) отправляться Сервером, обеспечивающим выполнение правил (PS), на CMTS, или б) отправляться с Сервера, обеспечивающего выполнение правил (PS) Системой завершения вызова для кабельного модема (CMTS). Этот интерфейс также позволяет проводить удаленный запрос QoS от имени клиента. В некоторых сценариях этот интерфейс может также использоваться для информирования Сервера, обеспечивающего выполнение правил (PS), о том, что ресурсы QoS стали неактивны.
pkt-mm-3	AM – PS	Менеджер приложений (AM) может запросить, чтобы PS установил Принятие решения на CMTS. Дополнительно, AM может также запросить, чтобы PS удаленно запросил CMTS от имени клиента. Этот интерфейс может также использоваться для информирования AM об изменении состояния ресурсов QoS.
pkt-mm-4	PS – RKS	PS отправляет сообщения о событии на Сервер регистрации (RKS), для того чтобы отследить Принятие решения, относящегося к QoS.
pkt-mm-5	CMTS – RKS	CMTS отправляет сообщение о событии на Сервер регистрации (RKS), для того чтобы отследить запросы на и само использование QoS (к примеру, добавление Потока услуг, изменения, удаления, и метрики объема).
pkt-mm-6	Клиент – CMTS	Клиент может использовать этот интерфейс для прямого запроса и управления сетевыми ресурсами QoS. В случае авторизации, эти ресурсы обеспечиваются Системой завершения вызова для кабельного модема (CMTS).
mm-7	Клиент – AM	Этот интерфейс может использоваться клиентом для взаимодействия с Менеджером приложений (AM) и для непрямого запроса и управления ресурсами QoS. Этот интерфейс находится вне рамок рассмотрения данного приложения.

Таблица I.1/J.179 – Мультимедийные интерфейсы сети IP-Cablecom

Интерфейс	Описание	Примечание
mm-8	АМ – Равноправный узел	АМ может использовать этот интерфейс для взаимодействия с некоторыми другими участниками приложения в вопросе. Этот интерфейс находится вне рамок рассмотрения данного приложения.
mm-9	CMTS – IP сеть, управляемая оператором	Этот интерфейс на CMTS может использоваться для поддержки сквозных запросов QoS за рамками сети доступа. Этот интерфейс находится вне рамок рассмотрения данного приложения.
mm-10	Клиент – Равноправный клиент	Клиент может использовать этот интерфейс для взаимодействия с некоторыми другими участниками приложения в вопросе. Этот интерфейс находится вне рамок рассмотрения данного приложения.

I.3.2 Мультимедийные компоненты

В этом разделе мы изложим подробности предыдущего обсуждения касательно структуры архитектуры, добавив некоторые детали для каждого элемента сети.

I.3.2.1 Клиент

Мультимедийный клиент является логической сущностью, которая может отправлять или получать данные. Мультимедийная сеть IP-Cablecom определяет три разных типа клиентов, которые различаются тем, как сигналы клиентов QoS и как принятия правил, соотносящиеся с QoS, установлены в CMTS.

Тип Клиента 1 представляет собой существующие конечные точки "наследства" (к примеру, ПК приложения, игровые консоли), которым не хватает специфических знаний QoS или способности к сигнализации. Этот Клиент ничего не знает о CableModem, IPCable2Home, или механизмах сообщений IP-Cablecom, и потому никакие связанные требования не могут быть размещены на нем. Такие клиенты могут иметь вид от простых устройств аналогового аудио и видеоприложений до комплексных сетевых внешних устройств и электронных устройств потребителя, таких как телевизионные абонентские приставки или игровые консоли. Этот Клиент общается с Менеджером приложений с целью запроса услуги и не запрашивает ресурсы QoS напрямую от сети доступа оператора.

Тип Клиента 2 похож на Адаптер мультимедийного терминала (MTA) телефонии сети IP-Cablecom-Т тем, что поддерживает сигнализацию QoS на базе Динамического Качества обслуживания (DQoS) IP-Cablecom. Этот Клиент знает о мультимедийных QoS IP-Cablecom и общается с Менеджером приложений с целью запроса услуг и получения маркера для ресурсов сети доступа. Затем Клиент предоставляет свой маркер при запросе ресурсов QoS в сети доступа (pkt-mm-1, pkt-mm-6).

Тип Клиента 3 запрашивает QoS на базе Протокола Резервирования ресурсов (RSVP) без взаимодействия с Менеджером приложений. Этот Клиент знает о базирующихся на стандартах Рабочей группы по стандартам Internet (IETF) RSVP и использует этот протокол для запроса ресурсов QoS из сети доступа напрямую от CMTS.

I.3.2.2 Сервер, обеспечивающий выполнение правил

Структура управления правилом для инициативы мультимедийной сети IP-Cablecom базируется на действии рабочей группы Протокола распределения ресурсов (RAP) Рабочей группы по стандартам Internet (IETF). Как определено и описано в РЧЦ (RFC) 2753, элемент сети Сервера, обеспечивающего выполнение правил (PS), выполняет авторизацию, назначенную оператором, и процедуры управления ресурсами. Вдобавок к параметрам запрошенных ресурсов и состоянию доступных ресурсов принятые решения могут включать в себя идентификатор клиента и информацию по соответствующему профилю, параметры приложения, разбор безопасности, время суток и т. д. Также некоторые операторы могут решить использовать множественные Серверы, обеспечивающие выполнение правил, и распределять определенные принятия правил между этими серверами с целью обеспечить расширяемость и требования толерантности к ошибкам.

Основные функции Сервера, обеспечивающего выполнение правил, включают в себя:

- Механизм запроса принятые решения, осуществляемый Менеджерами Приложений (pkt-mm-3, пассивная модель приёма сообщений) или Системами завершения вызова для кабельного модема (CMTS) (pkt-mm-2, система с активным опросом сообщений);

- Механизм доставки принятые решения, используемый для установления принятые решения на CMTS (pkt-mm-2);
- Механизм разрешения удаленного управления сообщениями QoS для CMTS от лица Менеджера Приложения (для клиентов, не имеющих собственных возможностей для сигнализации QoS);
- Интерфейс записи события на Сервер регистрации (pkt-mm-4), используемый для регистрации запроса правил, которая может также коррелироваться с записями использования сетевых ресурсов.

Сервер, обеспечивающий выполнение правил, может поддерживать две различные модели установления принятые решения на CMTS:

- Сервер, обеспечивающий выполнение правил, может устанавливать (проталкивать) принятие правил на CMTS перед тем, как на CMTS придет запрос резервации QoS.
- CMTS может запросить Принятие решения от Сервера, обеспечивающего выполнение правил, когда запрос резервирования QoS прибывает на CMTS.

Правила могут содержать следующую информацию:

- Правила, определяющие ресурсы, авторизованные сервером, обеспечивающим выполнение правил:
 - Сервер, с правом преимущественного использования сети;
 - Абонент, с правом преимущественного использования сети;
 - Полоса частот (определенная с использованием параметров признака сегмента);
 - Гарантии времени задержки;
 - Время истечения срока правила;
 - Пределы объема правила.
- Правила, обозначающие нехватку/значение полосы частот, основываясь на времени суток.
- Правила преимущественного права на покупку.

На минимуме, при сценарии "толчка" сервер, обеспечивающий выполнение правил, должен выполнять следующие функции:

- Аутентифицировать и контролировать сообщения о правилах от Менеджера приложений;
- Обработать сообщения о правилах, базирующиеся на правилах, определенных оператором;
- Определять правильную сущность CMTS, к которой должно проталкиваться правило;
- Соотносить решения по правилам и другие сообщения в соответствии с CMTS;
- Отправлять сообщения о событиях, отслеживая эти запросы, на RKS.

На минимуме, при сценарии "тяги" сервер, обеспечивающий выполнение правил. Должен выполнять следующие функции:

- Если Менеджер приложений участвует в оказании услуг, аутентифицировать и контролировать сообщения о правилах от Менеджера приложений;
- Соотносить сообщения по правилам и другие в соответствии с CMTS;
- Обработать сообщения о правилах, базирующихся на правилах, определенных оператором;
- Отправлять сообщения о событиях, отслеживая эти запросы, на RKS.

Сервер, обеспечивающий выполнение правил, может выполнять следующие функции:

- Отслеживать использование ресурсов, базирующихся на поддерживаемом изнутри состоянии информации (к примеру, таймеры);
- Отслеживать авторизованные ресурсы по пользователю, с правом преимущественного использования сети, услуги, с правом преимущественного использования сети, или общем базисе.

1.3.2.3 Система завершения вызова для кабельного модема

Мультимедийная сеть IP-Cablecom предоставляет доступ к полному набору алгоритмов планирования восходящего потока данных CMTS, как определено в Рекомендациях сети CableModem. В частности архитектура определяет "Профиль трафика" мультимедийной сети IP-Cablecom, который предоставляет уровень абстракции от связанных Типов Планирования CableModem (UGS, UGS/AD, и др.). Далее,

особенности и допущения, характерные для телефонии, обнаруженные в спецификации Динамического качества обслуживания (DQoS) сети IP-Cablecom-T, будут обобщены для обеспечения инфраструктуры QoS, которая может использоваться большим количеством типов клиентов и приложений.

CMTS поддерживает как однофазную, так и двухфазную модели резервирования для управления ресурсами сети доступа. В двухфазной модели ресурсы сети доступа заранее зарезервированы, затем предоставлены для использования, так как они понадобятся позже. CMTS также поддерживает однофазную модель резервирования, в которой ресурсы сети доступа одновременно зарезервированы и предоставлены для немедленного использования.

CMTS устанавливает значимый поток(и) в сети доступа CableModem с помощью интерфейса pkt-mm-1. CMTS отправляет сообщение о событиях для резервирования ресурсов QoS и использования на Сервер регистрации с помощью идентификатора интерфейса pkt-mm-5. Наконец, CMTS следит за потоками услуг на базе QoS и отчетами к ним как указано в (дополнительной) подсистеме Управления отчетом в рекомендациях.

1.3.2.4 Менеджер приложений

Менеджер приложений играет координирующую роль, включая сигнализацию приложений и семантику так же, как и взаимодействие со структурой правила мультимедийной сети IP-Cablecom, как упомянуто в предыдущем обсуждении элемента Сервера, обеспечивающего выполнение правил. Следует заметить, что Менеджер приложений может работать вместе с Мультимедийным сервером или, при условии разделенной модели, два элемента могут существовать отдельно.

Менеджер приложений соединяется с клиентом с помощью интерфейса mm-7. Исходя из этих сведений о предложении определенной услуги, Менеджер приложений должен обозначить или определить определенные параметры QoS, необходимые для предоставления услуг Типу Клиента 1. После того, как эта информация подтверждается, Менеджер приложений отправляет сообщение на Сервер, обеспечивающий выполнение правил, с помощью интерфейса pkt-mm-3. Если необходимо, Менеджер приложений может использовать интерфейс mm-8 для синхронизации с Мультимедийным сервером.

Тип Клиента 2 также взаимодействует с Менеджером приложений и отправляет информацию запроса услуги с помощью интерфейса mm-7. Опять же, Менеджер приложений должен обозначить параметры QoS, необходимые для предоставления услуг Типу Клиента 2. Менеджер приложений отправляет Запрос правила на Сервер, обеспечивающий выполнение правил, с помощью интерфейса pkt-mm-3. После успешной авторизации, Менеджер приложений получает пароль от Сервера, обеспечивающего выполнение правил, и отправляет этот пароль клиенту с помощью протокола mm-7. Если необходимо, Менеджер приложений может использовать интерфейс mm-8 для синхронизации с Мультимедийным сервером.

Тип Клиента 3 не нуждается в Менеджере приложений, хотя присутствие Сервера приложений во время исполнения сценариев поставки сложных услуг является очень желательным.

1.3.2.5 Сервер регистрации

Сервер регистрации (RKS) получает сообщение о событиях, указывающих на использование ресурсов сети доступа QoS. RKS соединяется с Сервером, обеспечивающим выполнение правил, (pkt-mm-4) и CMTS (pkt-mm-5). RKS не получает информации, требуемой для приложения, непосредственно от Менеджера приложений. Наоборот, информация, особая для приложения, может быть включена в сообщение о событиях как скрытая информация, отправленная от Менеджера приложений на Сервер, обеспечивающий выполнение правил, и внедренная в сообщение о событии запроса правила на RKS.

1.4 Управляемые удаленно QoS с правилом активного опроса (Сценарий 1)

Как указывалось выше, три сценария архитектуры были назначены для поддержки трех типов клиентов. Модель авторизации "управляемая удаленно QoS с правилом активного опроса" (Сценарий 1) поддерживает Тип Клиента 1, который в свою очередь не поддерживает оригинальные механизмы сигнализации QoS. Обзор высокого уровня взаимодействия элементов, включенный в этот сценарий показан на Рисунке 1.3.

Клиент запрашивает услугу, особую для приложения, отправляя "Запрос услуги" Менеджеру приложений. После получения этого запроса, Менеджер приложений определяет потребность QoS в запрошенной услуге и отправляет "Запрос правила" на Сервер, обеспечивающий выполнение правил. Сервер, обеспечивающий выполнение правил, в свою очередь утверждает "Запрос правила" по отношению к правилам, назначенным оператором, и, если решение положительное, отправляет сообщение "Установки правила" CMTS. CMTS осуществляет контроль допущения запрошенного формата (удостоверяя, что соответствующий ресурс свободен, для того чтобы удовлетворить запрос),

устанавливает Принятие решения и (в конечном итоге) устанавливает поток(и) услуги с запрошенными уровнями QoS.

Следует заметить, что фактическое управление потоком(ами) услуг (т.е. добавление, изменение, удаление запроса) может строго контролироваться и отслеживаться Менеджером приложений с помощью расширения основных механизмов сигнализации, описанных здесь, для установления принятые решения. В Сценарии 1 нет прямого сообщения между Клиентом и CMTS.

Следует заметить, что сообщения между Клиентом и Менеджером приложений, включая детали "Запроса услуги", находятся вне обзора данной Рекомендации. Возможно, что Клиент не имеет никаких сведений о QoS и услугах простого запроса (к примеру, пользователь хочет сыграть в многопользовательскую игру с другом) от Менеджера приложений в сообщении "Запроса Услуги". Также возможно, что Клиент имеет весь спектр сведений о требованиях своих QoS (к примеру, пользователь запрашивает гарантированную 128 Кбит/с услугу для доступа в свою частную виртуальную сеть (VPN), защищаемую IPSec) и сообщает эту дополнительную информацию в "Запросе Услуги". Механизм, с помощью которого Менеджер приложений определяет требования QoS для запрошенной услуги, находится вне рассмотрения данной архитектуры/

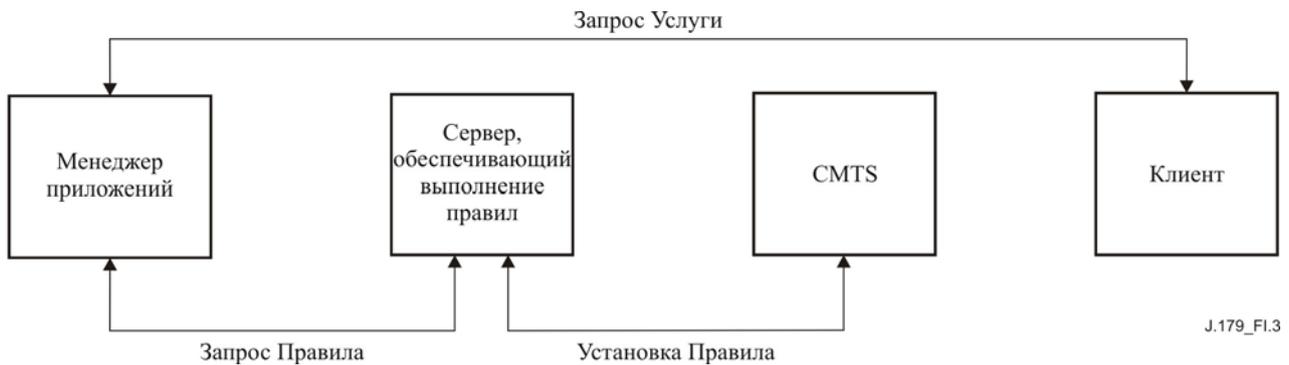


Рисунок I.3/J.179 – Структура авторизации для Сценария 1

При выполнении Сценария 1, CMTS поддерживает однофазную модель резервирования ресурсов, как показано на Рисунке I.4, для того чтобы дать возможность Клиенту активировать и использовать ресурсы сети. (Двухфазная модель резервирования ресурсов также поддерживается в этом сценарии, как будет описано позже в этом разделе.)

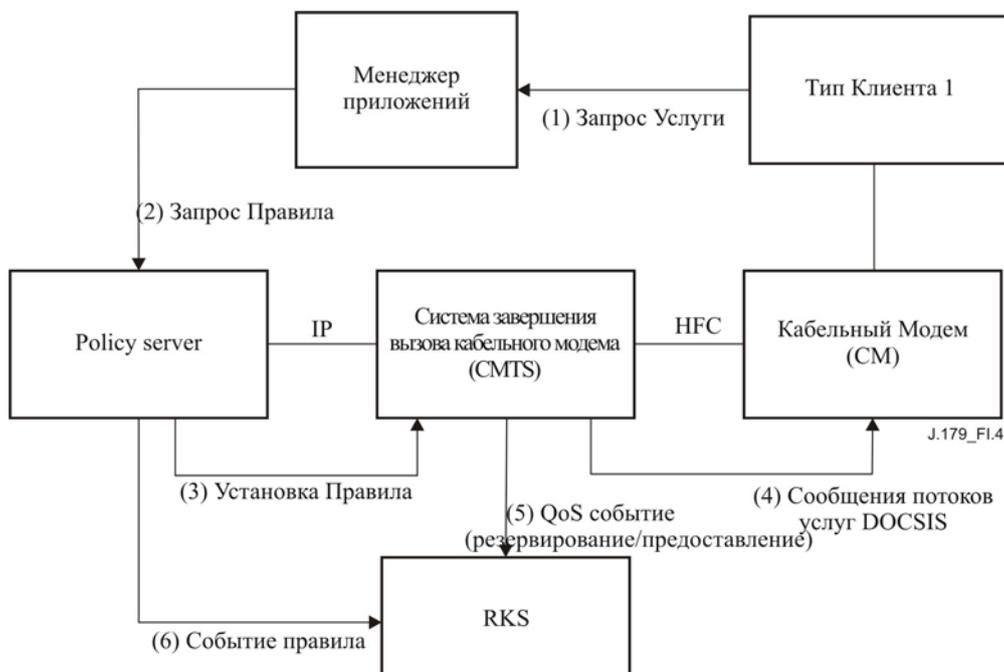


Рисунок I.4/J.179 – Однофазная модель резервации ресурсов для Сценария 1

На основе этой последовательности однофазного обмена сообщениями, в Таблице I.2 представлено краткое изложение высокого уровня каждого из этих сообщений. Детали, особые для сообщений протокола и объектов, были обозначены для соответствующих спецификаций мультимедийной сети IP/Cablecom.

Таблица I.2/J.179 – Детали сообщения однофазного резервирования для Сценария 1

Сообщение	Функция	Поля	Кандидат протокола	Комментарий
(1) Запрос услуги	Клиент запрашивает услугу у Менеджера приложений.	<нет>	Вне рассмотрения мультимедийной сети IP/Cablecom	Этот протокол должен поддерживать аутентификацию как Клиента, так и Менеджера приложений. Также протокол должен предоставлять необходимую информацию Менеджеру приложений для передачи нужд QoS запрошенной услуги.
(2) Запрос правила	Менеджер приложений запрашивает установку QoS от имени клиента.	IP/Cablecom MM QoS Тип, IP/Cablecom MM Класс сеанса связи, Параметры Полосы частот и Времени Задержки, Классификатор трафика, Возможность скрытого Биллинга	Контроль Шлюза (COPS)	Сервер, обеспечивающий выполнение правил, использует правила, установленные оператором, для того чтобы позволить или отвергнуть запрос.

Таблица I.2/J.179 – Детали сообщения однофазного резервирования для Сценария 1

Сообщение	Функция	Поля	Кандидат протокола	Комментарий
(3) Установка Правил	Сервер, обеспечивающий выполнение правил, отправляет сообщение CMTS, назначая свое Принятие решения и запрашивая установление Потока услуг.	IPcablecom MM QoS Тип, IPcablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Возможность скрытого биллинга (для AM и PS)	Контроль Шлюза (COPS)	В случае применения однофазной модели, этот запрос предназначен для авторизации, резервации и предоставления ресурсов QoS.
(4) Обмен сообщениями CableModem	CMTS устанавливает потоки сообщений, расширенные QoS.	Тип планирования CableModem, Параметры Полосы частот и Времени задержки, Классификатор трафика	Механизм сигнализации CableModem	Функции QoS здесь основаны на механизмах, определенных в спецификации РЧИ (RFI) CableModem.
(5) Событие QoS	CMTS создает надлежащее сообщение о событии, указывающее на использование QoS и другие параметры биллинга	IPcablecom MM QoS Тип, IPcablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Возможность скрытого биллинга (для AM и PS), Принятие решения, Данные использования Услуги, Время суток	Обмен сообщениями о событии (RADIUS)	Это сообщение должно содержать необходимые конструкции, для того чтобы позволить преобразование сообщения(й) и принятия(й), сделанных в расчете на определенную услугу для поддержки и/или взаимодействия.
(6) Событие Правила	Сервер, обеспечивающий правил, создает надлежащее сообщение о событии, указывающее на Запрос правила и предпринятое действие.	IPcablecom MM QoS Тип, IPcablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Возможность скрытого биллинга (для AM и PS), Принятие решения	Обмен сообщениями о событии (RADIUS)	Это сообщение должно содержать необходимые конструкции, для того чтобы позволить преобразование сообщения(й) и принятия(й), сделанных в расчете на определенную услугу для поддержки и/или взаимодействия.

Информация, собранная в колонке Поля Таблицы I.2, предназначена для предоставления примера типа информации, которое содержит каждое сообщение. Детали каждого сообщения протокола были обозначены для документов соответствующей спецификации.

Сценарий 1 также поддерживает двухфазную модель резервации ресурса, как иллюстрируется на Рисунке I.5. Здесь Менеджер приложений сначала требует, чтобы ресурсы сети доступа QoS были авторизованы и зарезервированы. После того, как данные ресурсы резервируются, Менеджер приложений может продолжать диалог с Клиентом относительно услуги. В нужное время Менеджер приложений требует предоставления ресурсов сети доступа. Данная двухфазная модель резервирования/предоставления гарантирует, что ресурсы сети доступа доступны, перед тем, как предложить услугу Клиенту.

Следует заметить, что подтверждения для каждого показанного сообщения включены не подробно, а выражены в общих чертах. Каждое сообщение подтверждения может быть отправлено только тогда, когда известен конечный итог соответствующего запроса. Это очень важно в последовательности подтверждений сообщений 5 (Резервирование DOCSIS), 3 (Установка Правила) и 2 (Запрос правила), так как Менеджер приложений, скорее всего, будет ожидать положительного подтверждения резервирования прежде, чем продолжить диалог с Клиентом и впоследствии предоставить ресурсы.



Рисунок I.5/J.179 – Двухфазная модель резервирования ресурсов для Сценария 1

Краткое изложение сообщений, используемых в Рисунке I.5, приводится ниже в Таблице I.3. Следует заметить, что сообщения (7-10) добавлены для поддержки сигнальной фазы обязательства.

Таблица I.3/J.179 – Детали сообщения двухфазного резервирования ресурса для Сценария 1

Сообщение	Функция	Поля	Кандидат протокола	Комментарии
(1) Запрос услуги	Клиент запрашивает услугу у Менеджера приложений.	<нет>	Вне рассмотрения мультимедийной сети IP-Cablecom	Этот протокол должен поддерживать аутентификацию клиента и Менеджера приложений. Также этот протокол должен предоставить необходимую информацию Менеджеру приложений для передачи нужд QoS запрошенной услуги.

Таблица I.3/J.179 – Детали сообщения двухфазного резервирования ресурса для Сценария 1

Сообщение	Функция	Поля	Кандидат протокола	Комментарии
(2) Запрос правила	Менеджер приложений запрашивает установку QoS от имени клиента.	IPCablecom MM QoS Тип, IPCablecom MM Класс Сеанса, Параметры Полосы частот и Времени задержки, Классификатор трафика, Возможность скрытого Биллинга	Контроль Шлюза (COPS)	Сервер, обеспечивающий выполнение правил, использует правила, установленные оператором, для того чтобы позволить или не отклонить запрос.
(3) Установка Правила	Сервер, обеспечивающий выполнение правил, отправляет сообщение CMTS, назначая свое выполнение правила и запрашивая резервирование Потока услуг.	IPCablecom MM QoS Тип, IPCablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Возможность скрытого биллинга (для AM и PS)	Контроль Шлюза (COPS)	В случае применения двухфазовой модели, этот запрос предназначен для авторизации резервирования ресурсов QoS.
(4) Резервирование DOCSIS	CMTS устанавливает потоки услуг, расширенные QoS и помещает их в "подходящее" состояние.	CableModem Тип Планирования, Параметры Полосы частот и Времени задержки, Классификатор трафика	Механизмы сигнализации CableModem	Функции QoS здесь основаны на механизмах, определенных в спецификации РЧИ (RFC) CableModem. Зарезервированные ресурсы остаются неактивными и могут использоваться трафиком "Наилучший из возможных" на других потоках до тех пор, пока не будут запрошены.
(5) Событие QoS	CMTS создает надлежащее сообщение о событии, указывающее на резервацию QoS reservation и другие параметры биллинга.	IPCablecom MM QoS Тип, IPCablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Принятие решения о возможности скрытого биллинга (для AM и PS), данные использования Услуги, Время суток	Обмен сообщениями о событиях (RADIUS)	Это сообщение должно содержать необходимые конструкции, для того чтобы позволить преобразование события(й), сделанное в расчете на определенную услугу для поддержки и/или взаимодействия.
(6) Событие Правила	Сервер, обеспечивающий выполнение правил, создает надлежащее сообщение о событии, указывающее на Запрос правила и предпринятое действие.	IPCablecom MM QoS Тип, IPCablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Принятие решения о возможности скрытого биллинга (для AM и PS)	Обмен сообщениями о событиях (RADIUS)	Это сообщение должно содержать необходимые конструкции, для того чтобы позволить преобразование события(й), сделанное в расчете на определенную услугу для поддержки и/или взаимодействия.
(7) Обязательство QoS	AM сообщает о необходимости предоставить ресурсы QoS.	IPCablecom MM QoS Тип, IPCablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Идентификатор правила	Контроль Шлюза (COPS)	Обязательство AM может зависеть от дальнейшего обмена сообщениями с клиентом.

Таблица I.3/J.179 – Детали сообщения двухфазного резервирования ресурса для Сценария 1

Сообщение	Функция	Поля	Кандидат протокола	Комментарии
(8) Обязательство QoS (Удаленное)	Сервер, обеспечивающий выполнение правил, получает запрос АМ и перенаправляет его CMTS.	IPcablecom MM QoS Тип, IPcablecom MM Класс сеанса связи, Параметры Полосы связи и Времени задержки, Классификатор трафика, Идентификатор Правила	Контроль Шлюза (COPS)	Не смотря на то, что PS может принять правила во время фазы обязательства, в общем он допускает, что зарезервированная полоса частот может быть предоставлена в любое время Менеджером приложений (АМ).
(9) Обязательство DOCSIS	CMTS переводит Поток услуг в "активное" состояние.	CableModem Тип Планирования, Параметры Полосы частот и Времени задержки, Классификатор трафика, Идентификатор потока услуг	Механизм сигнализации CableModem	Функции QoS здесь основаны на механизмах, определенных в спецификации РЧИ (RFC) CableModem.
(10) Событие QoS (Обязательство)	CMTS создает надлежащее сообщение о событии, указывающее на использование QoS и другие параметры биллинга.	IPcablecom MM QoS Тип, IPcablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Принятие решения о возможности скрытого биллинга (для АМ и PS), Время суток	Обмен сообщениями о событии (RADIUS)	Это сообщение должно содержать необходимые конструкции, для того чтобы позволить преобразование события(й), сделанное в расчете на определенную услугу для поддержки и/или взаимодействия.
(11) Событие Обязательства	Сервер, обеспечивающий выполнение правил, создает надлежащее сообщение о событии, указывающее на Запрос правила и предпринятое действие.	IPcablecom MM QoS Тип, IPcablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика. Идентификатор Правила	Обмен сообщениями о событии (RADIUS)	Это сообщение должно содержать необходимые конструкции, для того чтобы позволить преобразование события(й), сделанное в расчете на определенную услугу для поддержки и/или взаимодействия.

После того, как ресурсы QoS были успешно авторизованы, зарезервированы и предоставлены в сеть доступа, эти ресурсы отслеживаются на предмет активности в Системе завершения вызова для кабельного модема (CMTS). В целом используется модель мягкого состояния, в которой периодически обновляемые сообщения требуются во время периода неактивности в потоках зарезервированных и предоставленных услуг. Если время таймеров активности истекло без обновления, соответствующие ресурсы могут быть восстановлены CMTS. Это приведет к устойчивости сети в случае отказа конечной точки.

Более стандартная последовательность восстановления ресурсов также обеспечивается под управлением этого сценария, при котором Менеджер приложений сообщает Серверу, обеспечивающему выполнение правил, когда сеанс связи услуги заканчивается. Сервер, обеспечивающий выполнение правил, отвечает созданием сообщения о событии, которое отправляет на

RKS, и выпуская указание Системе завершения вызова для кабельного модема (CMTS) освободить соответствующий(е) поток(и) услуг и возобновить соответствующие ресурсы. Вне зависимости от того закончилось ли время Потока услуг вследствие неактивности, или оно явно удалено, назначается надежный аудит, для наблюдения за фактическим использованием ресурса посредством сообщения о событии, создаваемом CMTS и отправляемом на RKS.

1.4.1 Пример: полоса частот, основанная на интернет-технологии, по требованию

Одним из примеров того, как механизмы в Сценарии 1 могут быть использованы для предоставления услуг, является вебсайт, на хосте оператора, который позволяет абонентам запрашивать резервирование полосы частот по требованию.

Допустим, к примеру, что стандартная услуга абонента ограничена по скорости до 128 Кбит/с входящего трафика и 128 Кбит/с исходящего трафика. Пока что этот уровень услуг может подходить для большинства случаев использования, но может случиться, что приложения, которые использует абонент, требуют большей пропускной способности или имеют отличные потребности QoS. Если пользователь решает использовать услугу полоса частот-по-требованию, для временного изменения стандартного уровня своих услуг, он должен просто зарегистрироваться на вебсайте оператора (Менеджер приложений) и запросить временную модернизацию услуги.

Одной из возможных мотиваций такого запроса может быть желание получать от поставщика данных медиа-файлы на высокой битовой скорости. В таком случае абонент может явно запрашивать услугу минимальной зарезервированной скорости входящего трафика, равной 512 Кбит/с, в течение следующих трех часов. Напротив, точные потребности QoS приложения могут быть скрытыми для пользователя, который может просто запросить данный трехчасовой видеоклип (который без ведома для абонента был закодирован на скорости 512 Кбит/с). С другой стороны этот обмен представляет собой "Запрос услуги" абонента у Менеджера приложений.

В другом случае, Менеджер приложений отправит "Запрос правила" для услуги минимальной зарезервированной скорости, равной 512 Кбит/с, на три часа Серверу, обеспечивающему выполнение правил, от имени абонента. Сервер, обеспечивающий выполнение правил, тогда применит свой собственный критерий авторизации и, если запрос будет удовлетворен, запросит CMTS (посредством "Установки правила") о предоставлении полосы частот абоненту. CMTS в свою очередь произведет контроль внутреннего доступа и обеспечит QoS, используя обмен сообщениями CableModem, отслеживая данный процесс посредством сообщений о событии QoS.

1.4.2 Пример: игры онлайн через игровые консоли

В качестве альтернативы рассмотрим пример, в котором две игровые консоли хотят войти в контакт друг с другом посредством тоннеля сети. В этом примере два пользователя могут типично подключить свои консоли к сети, только если они располагаются в одном месте. Тем не менее, специальное программное обеспечение, установленное на персональном компьютере каждого пользователя, находящегося в одной локальной сети и служащего в качестве модуля доступа для удаленной консоли, дает возможность входа в сеть таким образом, что двум игровым консолям больше не требуется находиться рядом в одном месте. Единственной проблемой этого нестандартного подхода может быть то, что получившийся тоннель потребует достаточных QoS, так чтобы на игровых консолях можно было играть, таким образом, как если бы они находились в сети с высокой скоростью передачи данных.

В этом сценарии пользователь(и) смогут подсоединиться к Менеджеру приложений посредством PC, который передает свои пакеты по тоннелям. С помощью обмена сообщениями, особыми для приложения, они аутентифицируются и указывают на свой запрос для игры друг с другом. Менеджер приложений удовлетворяет запрос и создает "Запрос(ы) Правила" от имени пользователя(ей). Сервер, обеспечивающий выполнение правил, принимает свое решение и пересылает это сообщение как "Принятое решение" CMTS. CMTS осуществляет контроль доступа и открывает сеть доступа QoS между компьютерами для игрового тоннеля, используя обмен сообщениями CableModem. С этой точки зрения игровые консоли могут обмениваться пакетами без знания того, что они не находятся в одной сети. Следует заметить, что Обмен сообщениями о Событии был исключен из этого примера для простоты.

В этом гипотетическом примере, если пользователи находятся в отдельных узловых точках HFC, обязанностью оператора является удостовериться, что магистральная линия QoS к и от CMTS правильно управляется на таком уровне, который требуют их правила и соглашения об услугах. На Рисунке 1.6 дается графическое отображение этого примера для упрощенной модели, в которой оба пользователя получают услугу от одиночной Системы завершения вызова для кабельного модема (CMTS).

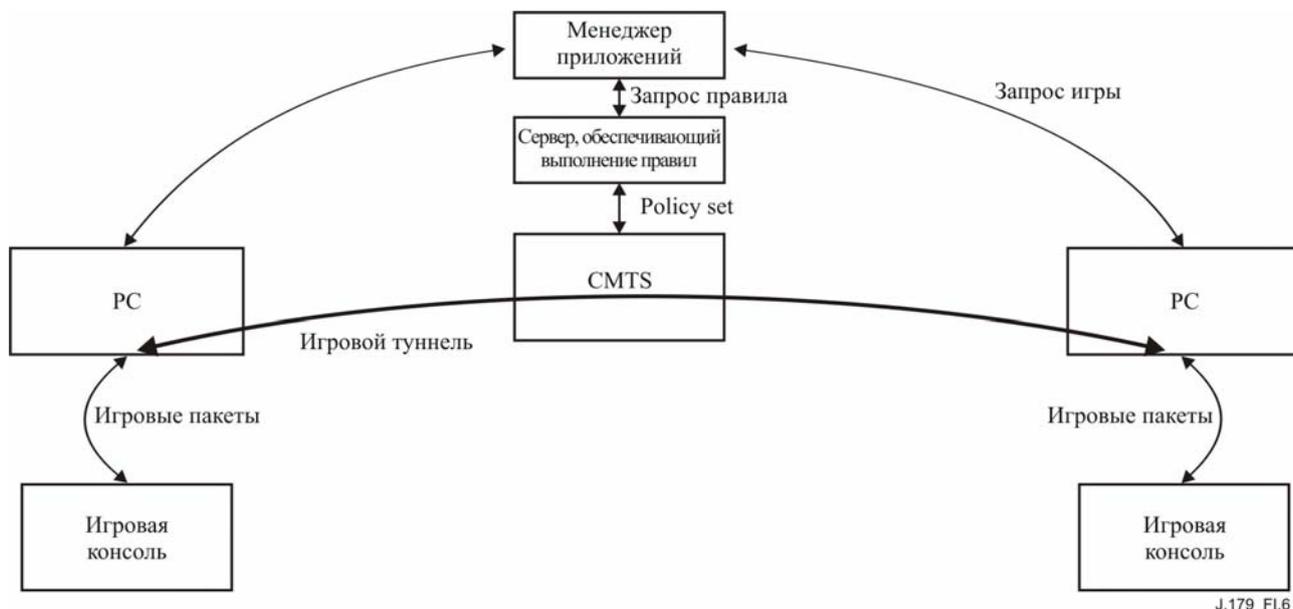


Рисунок I.6/J.179 – Игровые консоли, объединенные в сеть, посредством настроенного QoS IP туннеля

I.5 Запрошенное клиентом QoS с правилом активного опроса (Сценарий 2)

Модель Сценария 2 "Запрошенное клиентом QoS с правилом активного опроса" поддерживает Тип Клиента 2, который может сигнализировать и управлять своими ресурсами QoS, но требует предварительной авторизации этих запросов посредством Менеджера приложений. В этом сценарии модель авторизации правила и резервации QoS близко схожа с моделью телефонии IPcablecom-T, определенной в спецификации DQoS. Сервер, обеспечивающий выполнение правила, выполняет опрос на CMTS образом, схожим, с тем по которому Контроллер шлюза отправляет правило на CMTS посредством COPS. Тип Клиента 2 использует Механизм сигнализации DSx CableModem или обмен сообщениями RSVP+, схожий с устройствами MTA в IPcablecom-T.

Обзор высокого уровня Сценария 2 иллюстрируется на Рисунке I.7. Следует заметить схожесть со структурой авторизации, описанной для Сценария 1. Здесь снова клиент запрашивает услугу, особую для приложения, отправляя "Запрос услуги" на Менеджер приложений. Менеджер приложений затем определяет потребность QoS в запрашиваемой услуге и отправляет "Запрос правила" на Сервер, обеспечивающий выполнение правил. "Запрос правила" содержит "авторизованный формат" или максимальное QoS, позволенное этому клиенту. Сервер, обеспечивающий выполнение правил, в свою очередь подтверждает "Запрос правила" по отношению к правилам, назначенным оператором, и, если решение положительное, отправляет "Принятое решение" на CMTS. CMTS осуществляет контроль допуска в отношении запрошенного QoS и устанавливает авторизацию правила. Так же, как и в Сценарии 1, Сообщения о событиях создаются Сервером, обеспечивающим выполнение правил, и CMTS и отправляются на RKS. Сервер, обеспечивающий выполнение правил, записывает событие всякий раз, как принимает решение или обновляет его состояние, а CMTS отслеживает поддержку и использование ресурса QoS.

В Сценарии 2 и в отличие от Сценария 1, существует прямое сообщение между Клиентом и CMTS с целью создания, изменения и удаления резервирования ресурсов. После того, как CMTS получает сообщение "Принятое решение" от Сервера, обеспечивающего выполнение правил, Клиент может запросить QoS напрямую от CMTS, используя механизмы сигнализации, описанные выше. Клиент может также изменять QoS динамически до тех пор, пока запрошенное QoS находится внутри "авторизованного формата", утвержденного Сервером, обеспечивающим выполнение правил. Преимущество этого метода состоит в том, что Менеджер приложений не должен иметь дел с использованием полосы частот Клиентом, что является очень важным фактором, когда потребности QoS Клиента изменяются динамически.

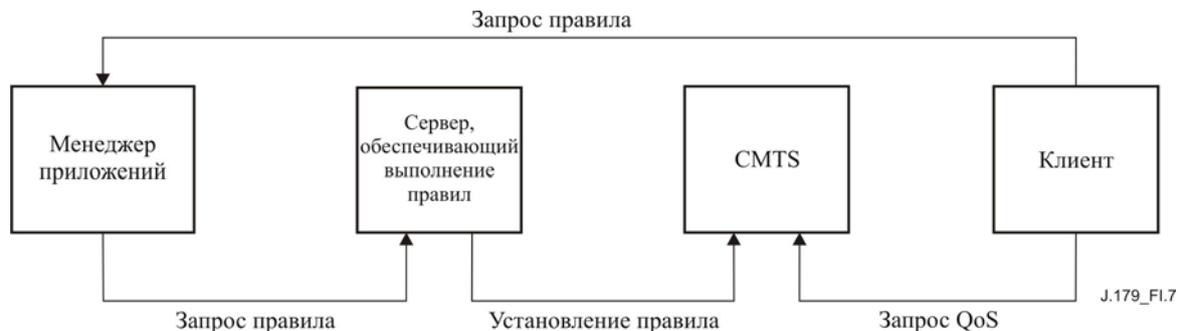


Рисунок I.7/J.179 – Структура авторизации для Сценария 2

Так же, как и предыдущий сценарий, Сценарий 2 (как показывается на Рисунке I.8) поддерживает однофазную модель резервирования ресурсов для установления возможности немедленной активирования и использования ресурсов сети доступа клиентом.

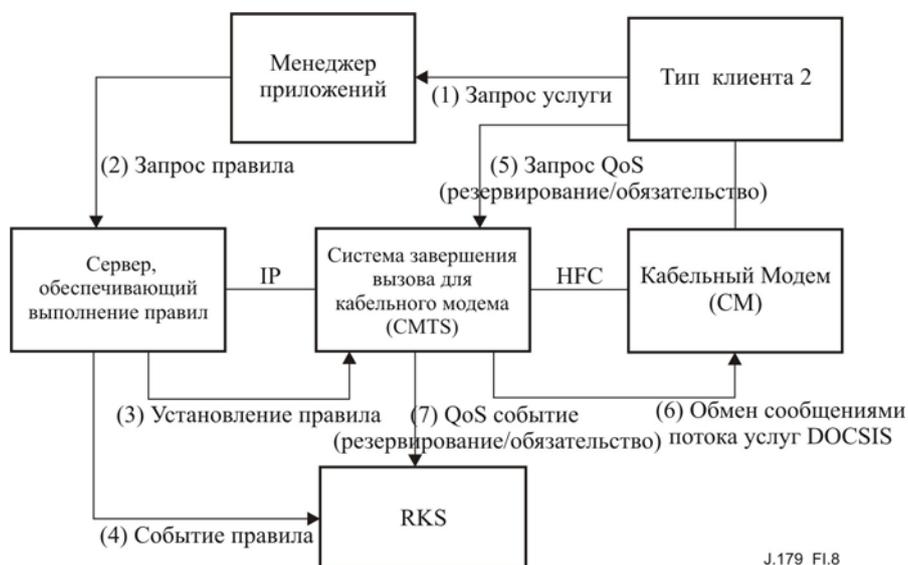


Рисунок I.8/J.179 – Однофазная модель резервирования ресурсов для Сценария 2

На основе этой однофазной последовательности обмена сообщениями, в Таблице I.4 предоставляется описание высокого уровня для каждого из этих сообщений.

Таблица I.4/J.179 – Детали сообщения однофазного резервирования для Сценария 2

Сообщение	Функция	Поля	Кандидат протокола	Комментарий
(1) Запрос услуги	Клиент запрашивает услугу от Менеджера приложений.	<нет>	Вне рассмотрения мультимедийной сети IP-Cablecom	Этот протокол должен поддерживать аутентификацию Клиента и Менеджера приложений. Также протокол должен обеспечивать Менеджер приложений необходимой информацией для передачи нужд QoS запрошенной услуги.
(2) Запрос правила	Менеджер приложений запрашивает авторизацию QoS от имени Клиента.	IP-Cablecom MM QoS Тип, IP-Cablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Возможность скрытого биллинга	Контроль Шлюза (COPS)	Сервер, обеспечивающий выполнение правил, использует правила, установленные оператором, для того чтобы позволить или отклонить запрос.
(3) Принятое решение	Сервер, обеспечивающий выполнение правила, отправляет сообщение CMTS, назначая свое Принятие решения.	IP-Cablecom MM QoS Тип, IP-Cablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Возможность скрытого биллинга (для AM и PS)	Контроль Шлюза (COPS)	В этом сценарии этот запрос используется только для авторизации.
(4) Событие Правила	Сервер, обеспечивающий выполнение правила, создает надлежащее сообщение о событии, указывая на Запрос правила и предпринятое действие.	IP-Cablecom MM QoS Тип, IP-Cablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Принятие решения о возможности скрытого биллинга (для AM и PS)	Обмен сообщениями о событии (RADIUS)	Это сообщение должно содержать необходимые конструкции, для того чтобы позволить преобразование события(й) и решения(й), сделанных в расчете на определенную услугу для поддержки и/или сообщения.
(5) Запрос QoS (Резервирование/ Обязательство)	Клиент запрашивает ресурсы QoS, которые были зарезервированы и немедленно предоставлены для использования.	Параметры Полосы частот и Времени задержки, Классификатор трафика	Механизм сигнализации (DSx) CableModem или RSVP+	Клиент может напрямую устанавливать потоки сообщений CableModem посредством механизмов сигнализации или может создавать сообщения RSVP+ для создания таких потоков.

Таблица I.4/J.179 – Детали сообщения однофазного резервирования для Сценария 2

Сообщение	Функция	Поля	Кандидат протокола	Комментарий
(6) Обмен сообщениями DOCSIS	CMTS создает потоки услуг, исправленные QoS, и устанавливает их в активное состояние.	Тип Планирования CableModem, Параметры Полосы частот и Времени задержки, Классификатор трафика	Механизм сигнализации (DSx) CableModem	Этот этап нужен только в том случае, когда сигнализация RSVP+ была обеспечена для CMTS для предыдущего сообщения, в противном случае потоки услуг уже были настроены и активированы посредством обмена сообщениями механизмов сигнализации (DSx) CableModem. Функции QoS здесь основаны на механизмах, определенных в Рекомендациях.
(7) Событие QoS	CMTS создает надлежащее сообщение о событии, указывая на использование QoS и другие параметры биллинга.	IPCablecom MM QoS Тип, IPCablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Принятие решения о возможности скрытого биллинга (для AM и PS), данные использования услуги. Время суток	Обмен сообщениями о событии (RADIUS)	Это сообщение должно содержать необходимые конструкции, для того чтобы позволить преобразование события(й) и решения(й), сделанных в расчете на определенную услугу для поддержки и/или сообщения.

CMTS также поддерживает двухфазную модель резервации ресурсов, как иллюстрируется на Рисунке I.9. В этой модели Клиент сначала требует, чтобы ресурсы QoS сети доступа были зарезервированы. После того, как ресурсы были зарезервированы, Клиент запрашивает предоставление этих ресурсов QoS. Двухфазная модель резервирования/обязательства гарантирует, что ресурсы сети доступа доступны, перед тем, как предлагать услугу клиенту.



Рисунок I.9/J.179 – Двухфазная модель резервирования ресурсов для Сценария 2

Таблица I.5/J.179 – Детали сообщения двухфазного резервирования для Сценария 2

Сообщение	Функция	Поля	Кандидат протокола	Комментарий
(1) Запрос услуги	Клиент запрашивает услуги от Менеджера приложений.	<нет>	Вне рассмотрения мультимедийной сети IP/Cablecom	Этот протокол должен поддерживать аутентификацию Клиента и Менеджера приложений. Также протокол должен обеспечивать Менеджеру приложений необходимую информацию для передачи нужд QoS запрошенной услуги.
(2) Запрос правила	Менеджер приложений запрашивает авторизацию QoS от имени Клиента.	IP/Cablecom MM QoS Тип, IP/Cablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, классификатор трафика, Возможность скрытого Биллинга	Контроль Шлюза (COPS)	Сервер, обеспечивающий выполнение правил, использует правила, назначенные оператором, для того чтобы позволять или отвергать запрос.
(3) Принятое решение	Сервер, обеспечивающий выполнение правил, отправляет сообщение CMTS, назначая свое выполнение правила.	IP/Cablecom MM QoS Тип, IP/Cablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Возможность скрытого биллинга (для AM и PS)	Контроль Шлюза (COPS)	В этом сценарии данный запрос используется только для авторизации.

Таблица I.5/J.179 – Детали сообщения двухфазного резервирования для Сценария 2

Сообщение	Функция	Поля	Кандидат протокола	Комментарий
(4) Событие правила	Сервер, обеспечивающий выполнение правил, создает надлежащее сообщение о событии, указывая на Запрос правила и предпринятое действие.	IPCablecom MM QoS Тип, IPCablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Принятие решения о возможности скрытого биллинга (для AM и PS)	Обмен сообщениями о событии (RADIUS)	Это сообщение должно содержать необходимые конструкции, для того чтобы позволить преобразование события(й) и решения(й), сделанных в расчете на определенную услугу для поддержки и/или сообщения.
(5) Запрос QoS (Резервирование)	Клиент запрашивает зарезервированные ресурсы QoS.	Параметры Полосы частот и Времени задержки, Классификатор трафика	Механизм сигнализации (DSx) CableModem или RSVP+	Клиент может напрямую устанавливать потоки сообщений CableModem посредством механизмов сигнализации или может создавать сообщения RSVP+ для создания таких потоков.
(6) DOCSIS (Резервирование)	CMTS создает потоки услуг, исправленные QoS, и устанавливает их в допустимое состояние.	Тип Планирования CableModem, Параметры Полосы частот и Времени задержки, Классификатор трафика	Механизм сигнализации (DSx) CableModem	Этот этап нужен только в том случае, когда сигнализация RSVP+ была обеспечена для CMTS для предыдущего сообщения, в противном случае потоки услуг уже были настроены и активированы посредством обмена сообщениями механизмов сигнализации (DSx) CableModem. Функции QoS здесь основаны на механизмах, определенных в Рекомендациях.
(7) Событие QoS (Резервирование)	CMTS создает надлежащее сообщение о событии, указывающее на использование QoS и другие параметры биллинга.	IPCablecom MM QoS Тип, IPCablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Принятие решения о возможности скрытого биллинга (для AM и PS), данные использования Услуги, Время суток	Обмен сообщениями о событии (RADIUS)	Это сообщение должно содержать необходимые конструкции, для того чтобы позволить преобразование события(й) и решения(й), сделанных в расчете на определенную услугу для поддержки и/или сообщения.

Таблица I.5/J.179 – Детали сообщения двухфазного резервирования для Сценария 2

Сообщение	Функция	Поля	Кандидат протокола	Комментарий
(8) Запрос QoS (Обязательство)	Клиент запрашивает ресурсы QoS, которые были переданы.	Параметры Полосы частот и Времени задержки, Классификатор трафика	Механизм сигнализации (DSx) CableModem или RSVP+	Клиент может напрямую устанавливать потоки сообщений CableModem посредством механизмов сигнализации или может создавать сообщения RSVP+ для создания таких потоков.
(9) DOCSIS (Обязательство)	CMTS переводит потоки услуг в "активное" состояние.	Тип Планирования CableModem, Параметры Полосы частот и Времени задержки, Классификатор трафика, Идентификатор потока услуг	Механизм сигнализации (DSx) CableModem	Этот этап нужен только в том случае, когда сигнализация RSVP+ была обеспечена для CMTS для предыдущего сообщения, в противном случае потоки услуг уже были настроены и активированы посредством обмена сообщениями механизмов сигнализации (DSx) CableModem. Функции QoS здесь основаны на механизмах, определенных в Рекомендациях.
(10) Сообщение QoS (Обязательство)	CMTS создает надлежащее сообщение о событии, указывая на использование QoS и другие параметры биллинга.	IPCablecom MM QoS Тип, IPCablecom MM Класс сеанса связи, Параметры Полосы частот и Времени задержки, Классификатор трафика, Принятие решения о возможности скрытого биллинга (для AM и PS), данные использования Услуги, Время суток	Event Messaging (RADIUS)	Это сообщение должно содержать необходимые конструкции, для того чтобы позволить преобразование события(й) и решения(й), сделанных в расчете на определенную услугу для поддержки и/или сообщения.

Так же, как и в предыдущем Сценарии, возможны две альтернативы относительно освобождения канала ресурсов QoS и восстановления. Время использования ресурсов может истечь (как определяется CMTS) вследствие неактивности без указанного обновления таймера, или они могут быть явно удалены Клиентом в заключение сеанса связи услуги. Механизм обеспечения явного удаления сигнала Потока услуг является компонентом протокола QoS, назначенного для Устройства Клиента 2. Единственным различием между последовательностью восстановления ресурсов, назначенной для Сценария 1 и Сценария 2, является то, что удаление Потока услуг указывается напрямую через Клиента вместо того, чтобы проводиться удаленно через Менеджер приложений во втором сценарии.

I.5.1 Пример: игра в онлайн посредством консолей, объединенных в сеть

Пример сетевой игры посредством консолей, описанный для Сценария 1 в пункте I.4.2, легко может быть изменен для поддержки модели управления ресурсами QoS, представленными в Сценарии 2. В этом случае консоли по-прежнему будут координироваться Менеджером приложений с целью определения их положения друг относительно друга и установления сигнализации, требуемой для приложения. Вдобавок Менеджер приложений предоставит Запрос Ресурса Серверу, обеспечивающему выполнение правил, запрашивая авторизацию для необходимых ресурсов QoS. Однако после успешного воплощения этого решения об авторизации на CMTS, Менеджер приложений просто отправит обратно положительное подтверждение, содержащее признак авторизации, на каждый модуль доступа ПК. Этот признак затем может использоваться компьютерами в их сигнализации QoS на Системе завершения вызова для кабельного модема (CMTS) с целью резервирования, предоставления и удаления потоков услуг, запрашиваемых туннелем игры.

I.6 Запрашиваемое клиентом QoS с получением правила (Сценарий 3)

Третий сценарий, с его моделью авторизации "запрашиваемого клиентом QoS с извлечением правила" поддерживает Тип Клиента 3. Сценарий 3 определяет модель, при которой правила принятия авторизации не установлены заранее и передаются на CMTS посредством механизмов Менеджера приложений и Сервера, обеспечивающего выполнение правил. Эти правила описаны в предыдущих сценариях, но запрашиваются по требованию CMTS от Сервера, обеспечивающего выполнение правил, как предписание запросов входящих резервирований. Это позволяет реализовать очень гибкую и динамичную модель резервирования ресурсов, стимулируемую Клиентом, и одновременно поддерживать контроль оператора над всеми запросами ресурсов в центральном блоке управления.

В этом сценарии CMTS получает запрос QoS от Клиента раньше принятия решения, Сервером, обеспечивающим выполнение правил. Вместе с этим запросом QoS включаются мандаты, дающие право клиенту на аутентификацию. CMTS создает Запрос правила, который он отправляет на Сервер, обеспечивающий выполнение правил. На Сервере, обеспечивающем выполнение правил, запрос аутентифицируется, и создается правило аутентификации на основе критериев, определенных оператором, (к примеру, доступность ресурса, профиль клиента, оценка кредита, класс услуги, взаимодействие с другими элементами сети и т. д.). Если авторизация правила прошла успешно, разрешается продолжить резервирование ресурсов на CMTS, и на основе запрошенного QoS создается подходящий Поток услуг. Интерфейсы мультимедийной сети IP-Cablecom (определенные в пункте I.3.1), используемые при этом взаимодействии, включают в себя: pkt-mm-1, pkt-mm-2, pkt-mm-4, pkt-mm-5, pkt-mm-6, и mm-9. Интерфейс pkt-mm-3 может использоваться так же, как и предписание требований сигнализации приложения, но не допускается к использованию.

Рисунок I.10 иллюстрирует поток информации между центром элементов сети доступа для Сценария 3. В Таблице I.6, следующей за Рисунком I.10, представлено более подробное описание каждого сообщения. В примере, представленном ниже, заданное значение QoS установлено в восходящем направлении между CM и CMTS. Аналогичный поток потребуется для установления симметричного нисходящего потока QoS.

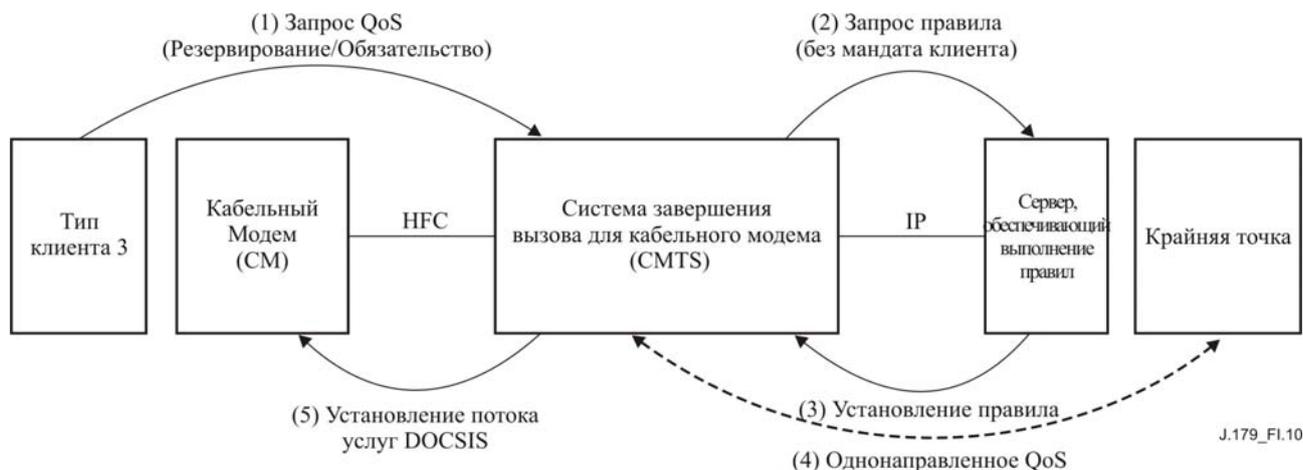


Рисунок I.10/J.179 – Структура авторизации для Сценария 3

Таблица I.6/J.179 – Детали сообщения для Сценария 3

Сообщение	Функция	Поля	Кандидат протокола	Комментарий
(1) Запрос QoS (Резервирование/ Обязательство)	Клиент запрашивает резервирование ресурсов у CMTS.	Параметры Полосы частот и Времени задержки, Классификатор трафика, Мандат Аутентификации	RSVP	Этот сценарий допускает способности RFC 2205, существующие для клиента.
(2) Запрос правила	CMTS запрашивает решение по авторизации правила от Сервера, обеспечивающего выполнение правила.	Параметры Полосы частот и Времени задержки, Классификатор трафика, Мандат Аутентификации	COPS	RFC 2748
(3) Принятое решение	Сервер, обеспечивающий выполнение правил, устанавливает авторизацию в CMTS.	Параметры Полосы частот и Времени задержки, Классификатор трафика	COPS	RFC 2748
(4) Однонаправленное QoS	CMTS ускоряет RSVP сигнализацию дальнего конца.	Параметры Полосы частот и Времени задержки, Классификатор трафика, Мандат Аутентификации	RSVP	RFC 2205
(5) Установление Потока услуг CableModem	CMTS обсуждает установление запланированного Потока услуг CableModem с CM.	Тип Планирования CableModem, Параметры Полосы частот и Времени задержки, Классификатор трафика, Идентификатор потока услуг	Механизм обмена сообщениями CableModem DSx	Функции QoS здесь основаны на механизмах, определенных в Рекомендациях CableModem.

Одной из основных отличительных характеристик этого сценария является поддержка RSVP, стандартный механизм сигнализации QoS. Поскольку Сценарий 1 предназначен для Клиентов без "врожденных" способностей к сигнализации QoS, а Сценарий 2 определяет специфический для сети IP-Cablecom механизм сигнализации QoS (основанный на RSVP, но включающий в себя частные расширения), этот сценарий основан на стандарте IETF как таковой. Это приведет к взаимодействию на стандартной основе с Клиентами, которые подписались на услуги QoS оператора и имеют значение безопасной аутентификации сами по себе в сети доступа. Он также не требует от приложений проталкивания решений раньше времени, и потому не помещает принуждения архитектуры на сигнализацию приложений.

Сценарий 3 допускает, что обмен сообщениями RSVP происходит между Клиентом и дальним концом. Однако следует заметить, что не требуется, чтобы все элементы сети между Клиентом и дальним концом должны были поддерживать RSVP, или не предполагается использование общих услуг (IntServ [13]) стратегии сквозного QoS. К примеру, различаемые услуги (DiffServ [16]) или другая схема QoS может использоваться вне CMTS. Также промежуточные маршрутизаторы, не желающие поддерживать RSVP могут просто пропускать сообщения RSVP без их обработки. Напротив, если гарантии QoS могут применяться в других значениях, такие маршрутизаторы могут быть определены как районы скопления и потому явно пропускать сообщения RSVP, как указано в RFC 3175 [20].

ПРИМЕЧАНИЕ. – RFC 3175 требует выполнения этих функций скопления на маршрутизаторах как ближнего, так и дальнего конца.

Более того, следует заметить, что использование RSVP в этом сценарии близко соответствует стандарту (к примеру, RFC 2205) операций RSVP и потому резервирование ресурсов в сети доступа

однаправлено. Таким образом Клиент резервирует ресурсы восходящего потока, и дальняя точка отвечает за резервирование ресурсов восходящего потока.

Успешное резервирование ресурсов поддерживается схожим образом с резервированием при других сценариях посредством обновления состояния программных средств. Клиенты RSVP должны периодически отправлять сообщения для подтверждения своего резервирования, в противном случае его время истечет и будет возвращено CMTS.

Наконец особые механизмы включены в протокол RSVP, для того чтобы позволить либо передающей, либо принимающей конечной точке сигнализировать об окончании и освобождении канала Потока услуг. Основываясь на однонаправленной природе резервирования RSVP, конечная точка, поддерживающая множественные потоки услуг, отвечает за явное удаление каждого из таких потоков при завершении сеанса связи услуг.

Отталкиваясь от этой модели, аутентификация запроса дальней точки, с целью позволить резервирование ресурсов нисходящего потока данных, требует особого обсуждения. Одним из решений проблемы может быть требование того, чтобы Сервер, обеспечивающий выполнение правил, мог аутентифицировать Клиентов, как ближней точки, так и дальней точки. Другие решения возможны, как таковые, но привлечение безопасности и, в частности, возможность для кражи услуг, следует рассматривать очень внимательно.

I.6.1 Пример: игра в онлайн посредством "родной" сигнализации QoS

Одной из потенциальных услуг, которая может использовать преимущества Сценария 3, является игра в онлайн. В этом примере все, что может понадобиться – это интегрированная стандартная RSVP поддержка Клиента. Так что игра в онлайн может быть настроена для работы либо совместно, либо без Менеджера приложений.

Когда Клиент хочет присоединиться к игре, ему просто нужно отправить особое для приложения сообщение на дальнюю точку, а затем продолжить в сети запроса QoS, посылая сообщение RSVP, снова адресуясь на удаленную конечную точку. Когда CMTS получает данное сообщение, она должна послать запрос на Сервер, обеспечивающий выполнение правил, с целью аутентификации Клиента и решения того, следует ли допустить QoS или нет. Успешная авторизация приведет к однонаправленному резервированию QoS.

Схожим образом дальняя точка отправит сообщение RSVP, адресуясь к Клиенту. Кроме того, когда CMTS получает такое сообщение, она отправляет его на Сервер, обеспечивающий выполнение правил, для того чтобы определить, должно ли быть удовлетворено QoS. После успешных авторизации и обслуживания, Клиент затем получит QoS в обоих направлениях и сможет продолжить игру в онлайн.

I.7 Сравнение сети IP-Cablecom-T и мультимедийной сети IP-Cablecom

Этот раздел описывает, на высоком уровне, главное различие между архитектурой сети IP-Cablecom-T и мультимедийной сети IP-Cablecom. Следует учесть, что большинство особых характеристик протокола и функциональных деталей мультимедийной сети IP-Cablecom должно быть еще определено в данном описании. В Таблице I.7 представляются известные различия для быстрого рассмотрения.

Таблица I.7/J.179 – Различия между сетью IP-Cablecom-T и мультимедийной сетью IP-Cablecom

	Сеть IP-Cablecom-T	Мультимедийная сеть IP-Cablecom
Поддерживаемые Услуги	Резидентная Телефония Основные свойства резидентной телефонии Расширенные свойства телефонии	Мультимедийные услуги На базе клиента (соединение равноправных узлов ЛВС) На базе сервера
Обмен сообщениями о событиях	Надежный аудит следа для всех правил и события QoS Поддержка модели биллинга PSTN (Телефонной сети общего пользования)	Надежный аудит следа для всех правил и события QoS Поддержка расчета на основе QoS Поддержка расчета по времени и объема

Таблица I.7/J.179 – Различие между сетью IPСablecom-Т и мультимедийной сетью IPСablecom

	Сеть IPСablecom-Т	Мультимедийная сеть IPСablecom
Возможности QoS	<p>Алгоритмы планирования QoS сети CableModem</p> <p>Услуга Услуги без запроса разрешения</p> <p>Услуга Услуги без запроса разрешения с выявлением активности</p> <p>Характеристики Полосы частот</p> <p>Постоянная Скорость битов</p> <p>Симметричные восходящие/нисходящие потоки данных</p> <p>Уровень Гарантированных QoS Клиент-к-Клиенту (т. е. сквозной посредством сегментированной модели)</p>	<p>Алгоритмы планирования QoS сети CableModem</p> <p>Услуга Услуги без запроса разрешения</p> <p>Услуга Услуги без запроса разрешения с выявлением активности</p> <ul style="list-style-type: none"> • Опрос в реальном времени • Опрос не в реальном времени • "Наилучший из возможных" с или без Приоритета <p>Характеристики Полосы частот:</p> <ul style="list-style-type: none"> • Постоянная скорость битов • Варьируемая скорость битов • Симметричные восходящие/нисходящие потоки данных • Ассиметричные восходящие/нисходящие потоки данных <p>Уровень Гарантированных QoS:</p> <ul style="list-style-type: none"> • CMTS-на-СМ (т. е. сеть доступа)
Безопасность	<p>Сигнализация безопасности и средства связи</p> <p>Предоставление устройств безопасности и управление настройкой</p>	<p>COPS и RADIUS охраняемые посредством IPsec; управление ключами посредством IKE с аутентификацией ключей с заранее обеспеченным общим доступом (IKE с сертификатами или Управление ключами на базе системы Kerberos являются дополнительными).</p> <p>Сигнализация Клиента находится вне рассмотрения данного приложения, и потому не существует определенной системы безопасности для интерфейса сигнализации клиента.</p>

I.7.1 DQoS (Динамическое Качество обслуживания)

Основная зона рассмотрения сети IPСablecom-Т это услуги резидентной телефонии. Спецификация Динамического Качества Обслуживания (DQoS) была развита, как часть этой попытки, определяя механизмы, необходимые для поставки QoS на узлы доступа на базе CableModem IP сети. Так что сеть IPСablecom-Т принимает сегментный подход (разделяющий сквозные средства связи и путь сигнализации на сетевые RKS ближнего и дальнего доступа, объединенные опорной сетью), при котором DQoS особым образом адресует резервирование ресурсов на сегменте доступа, а не в опорной сети или сквозном QoS.

Мультимедийная сеть IPСablecom направлена на более общие мультимедийные приложения, которые выходят за пределы поддержки голоса. Однако она основывается на некоторых механизмах DQoS сети IPСablecom-Т с целью обеспечения расширенных QoS услуг для таких приложений.

I.7.1.1 Элементы сети доступа

Сеть IPСablecom-Т поддерживает следующие элементы сети: MTA, СМ, CMTS, CMS (логически состоящий из Агента Вызова и Контроллера шлюза) и RKS. В архитектуре мультимедийной сети IPСablecom Агент Вызова функционально может быть преобразован в Менеджер приложений, а Контроллер шлюза – в Сервер, обеспечивающий выполнение правил. Дополнительные элементы сети могут быть введены в архитектуру мультимедийной сети IPСablecom, включая, к примеру, Мультимедийный Сервер. Менеджер приложений и Мультимедийный Сервер физически могут располагаться в одном и том же оборудовании, или могут использоваться раздельно.

I.7.1.2 Архитектура DQoS

Архитектура DQoS [9] сети IPCom базирется на CableModem, RSVP+, и правилах QoS, установленных на CMTS Сервером управления вызовами (CMS) (Контроллер шлюза).

Как описывалось в данной Рекомендации, архитектура мультимедийной сети IPCom также базирется на этих технологиях. Вдобавок, попытка мультимедиа имеет целью поддерживать более стандартную RSVP модель сигнализации (Сценарий 3) с намерением того, что эта способность сделает услуги, расширенные QoS, доступной для большей базы пользователей.

CMTS в архитектуре DQoS сети IPCom-T выступает, как точка усиления правила для правил QoS. CMTS будет исполнять схожую функцию в архитектуре мультимедийной сети IPCom. Вдобавок к служебным запросам QoS, побуждаемым клиентами, CMTS также может получать удаленные запросы от Сервера, обеспечивающего выполнение правил (Сценарий 1). Это отличается от архитектуры DQoS сети IPCom-T, где только автономный MTA или встроенный MTA может инициировать активацию QoS.

I.7.1.3 Интерфейсы QoS

В архитектуре сети IPCom-T интерфейсы сигнализации были заданы для всех элементов сети, так же, как в Системах завершения вызова для кабельного модема (CMTS) для внутрисетевых звонков, поддерживающих Координацию Шлюза. В заключении основным протоколом сигнализации между MTA и Агентом Вызова является Узел управления сетью (NCS), между встроенным MTA и CMTS – CableModem, и между автономным MTA и CMTS – RSVP+. Сигнализацией от игрового компьютера (GC) к CMTS является обмен сообщениями Контроля Шлюза на базе COPS.

Мультимедийная сеть IPCom построена на этих сигнальных интерфейсах и дополнительно поддерживает интерфейсы сигнализации между Менеджером приложений и Сервером, обеспечивающим выполнение правил. Следует напомнить, что любая сигнализация, особая для приложения, и происходящая между Менеджером приложений и его клиентами, находится вне рассмотрения данной архитектуры.

I.7.1.4 Структура для QoS сети IPCom

В архитектуре QoS сети IPCom-T "определенная QoS конструкция, называемая Шлюзом, обеспечивает контрольную точку для присоединения сетевых RKS доступа к услуге широкополосной сети передачи данных высокого качества" (Смотри спецификацию DQoS [14].) Шлюз представляет собой авторизацию QoS, которая установлена на CMTS для целей усиления правила. Мультимедийная сеть IPCom определяет схожую конструкцию правила QoS и ожидается, что конструкция Шлюза DQoS IPCom-T будет использоваться для обеспечения функции правила в мультимедийной сети IPCom. Изменения в существующих механизмах Контроля Шлюза сети IPCom-T могут потребоваться для обеспечения ослабленного контроля QoS (к примеру, для поддержки Сценария 1).

I.7.1.5 Требования к управлению ресурсами сети доступа

Архитектура сети IPCom-T "нацелена на обеспечение высокой степени всеобщности с намерением предоставить доступ к новым услугам и будущему развитию архитектуры сетей". Целью являются несколько требований к жизнеспособной архитектуре QoS в следующих областях (следует заметить, что каждая из этих способностей, относящихся к QoS, четко определена и обсуждена в спецификации DQoS сети IPCom):

- Изменения ресурсов во время сеанса связи;
- Динамическое связывание ресурсов;
- Класс сеанса связи (обозначение приоритета);
- Двухфазная передача ресурсов;
- Сегментное назначение ресурсов;
- Поддержка магистральной линии связи QoS;
- Предотвращение кражи услуги.

Архитектура мультимедийной сети IPCom также поддерживает однофазную модель резервирования ресурсов. В начале мультимедийная архитектура не предназначена для поддержки магистральной линии связи QoS, хотя данные функциональные средства могут формально адресоваться в соответствии с нуждами оператора. Для более подробной информации о существующих требованиях DQoS сети IPCom-T, пожалуйста, обратитесь к спецификации [14] DQoS сети IPCom-T.

I.7.1.6 Теория операции

DQoS сети IPCom-T включают в себя особое резервирование и фазы обязательства для получения ресурсов сети доступа. В конце фазы резервирования ресурсы установлены в стороне, но еще не активны или доступны для MTA. В конце второй фазы ресурсы предоставлены и доступны для использования. В традиционной модели телефонии биллинг начинается во время фазы обязательства.

В модели со встроенным MTA RSVP+ не требуется между MTA и Системой завершения вызова для кабельного модема (CMTS). Вместо этого E-MTA может сигнализировать о резервировании ресурсов и предоставлении посредством обмена сообщениями DSx CableModem. В модели с автономным MTA обмен сообщениями RSVP+ используется для воплощения этих этапов. CM и CMTS затем координируются посредством обмена сообщениями DSx CableModem для планирования, необходимого потока услуг в сети доступа.

Как указывается в данном приложении, мультимедийная сеть IPCom поддерживает модель, схожую с IPCom-T, и дополнительно поддерживает более стандартное использование RSVP. Она также предлагает удаленную модель запроса QoS, где Менеджер приложений управляет QoS от имени Клиента. Эти модели разобраны в разделах сценариев данного приложения. Существующая модель сети IPCom-T отображает Сценарий 2. Две другие модели поддерживаются в архитектуре мультимедийной сети IPCom для обеспечения большей гибкости там, где мультимедийные услуги могут использоваться в сети оператора.

I.7.2 Сообщение о событиях для биллинга

Сообщения о событиях сети IPCom предназначены, для того чтобы быть легко приспособляемыми и расширяемыми с целью предоставления информации об использовании сети для множества вариантов услуг, предоставляемых посредством архитектуры IPCom. Спецификация сообщений о событиях сети IPCom-T определяет общую архитектуру Сообщения о событии так же, как и особые требования для поддержки голосовые услуги сети IPCom-T. Спецификация сообщения о событии сети IPCom (Рекомендация МСЭ-T J.164) подробно описывает транспортировку независимого от протокола TLV формата сообщения о событии, формата файла сообщения о событии, а также обязательные и дополнительные протоколы транспортировки.

Данные сообщения содержат достаточную информацию по каждому сеансу связи для поддержки биллинга пользователя для услуги. Информация, содержащаяся в сообщениях о событиях, поддерживает множество вариантов биллинга и моделей расчета. Сеть IPCom не дает полномочий на использование особых моделей биллинга или расчета, так как данные модели определены и базируются на особых требованиях бизнеса индивидуального кабельного оператора. Сеть IPCom ни не дает полномочий, ни препятствует использованию расчетной палаты для расчетов.

Сообщения о событиях сети IPCom основаны на модели, где сеанс связи или услуга разделены на начинающую половину и завершающую половину. Начинаящий CMS или MGC должен создавать уникальный Идентификатор Корреляции биллинга (BCID) для идентификации всех Сообщений о событиях, относящихся к начинающей половине сеанса связи. Завершающий CMS или MGC должен создавать уникальный BCID для идентификации всех Сообщений о событиях, относящихся к завершающей половине сеанса связи. Для каждой из этих половин сеансов связи. Группа элементов сети IPCom, которая создает Сообщение о событии (CMS, MGC, CMTS) должна предоставить всю необходимую информацию, требуемую для биллинга и/или расчетов как соответствующие, базирующиеся услуге. Информация, создаваемая начинающей половиной, должна отправляться на RKS, поддерживающий начинающую половину. Информация, создаваемая завершающей половиной, должна отправляться на RKS, поддерживающий завершающую половину.

Ограниченная группа сообщений о событиях требуется для услуг мультимедийной сети IP-Cablecom. Эти сообщения включают в себя:

- Signal_Start (Сигнал Старта) для "расширенной QoS услуги", создаваемое Сервером, обеспечивающим выполнение правил, указывающим время, в которое Сервер, обеспечивающий выполнение правил, получает запрос для QoS сети доступа;
- Signal_Stop (Сигнал Остановки) для "расширенной QoS услуги", создаваемое Сервером, обеспечивающим выполнение правил, указывающим время, в которое Сервер, обеспечивающий выполнение правил, получает замечание о том, что использование QoS сети было завершено;
- QoS_Reserve, QoS_Commit, QoS_Stop, создаваемые Системой завершения вызова для кабельного модема (CMTS). Эти сообщения указывают время, в которое CMTS резервирует, предоставляет или освобождает QoS сети доступа.

I.7.3 Безопасность

Архитектура безопасности сети IP-Cablecom-T назначает механизмы, алгоритмы и протоколы, которые отвечают сервисным требованиям безопасности. Интерфейсы мультимедийной сети IP-Cablecom охраняются с использованием идентичных механизмов для соответствующих интерфейсов.

Приложение II

Рекомендации для назначения номера версии

Взаимодействие между разными версиями протокола основывается на следующих принципах:

Принцип устойчивости к ошибкам:

RFC 791 определяет основной "принцип устойчивости к ошибкам" для Протокола Интернета следующим образом:

- "Осуществление должно быть консервативным в плане отправления линии поведения и либеральным в плане получения линии поведения".
- Следуя такому принципу устойчивости к ошибкам, возможно разрешение незначительных изменений в протоколе с поддержанием обратной совместимости.

Основное правило для нумерации версии протокола внутри Протокола Контроля Шлюза мультимедийной сети PacketCable должно отвечать следующим требованиям:

- Версии протокола в пределах одного и того же номера старшей версии ДОЛЖНЫ быть обратно совместимы. Версии с разными Номерами Старшей Версии могут не быть обратно совместимыми.
- Критично, чтобы группа Спецификации мультимедийной сети PacketCable изучала все изменения протокола с целью включения в новую версию этого протокола и выбирала номер версии протокола, основываясь на изменении с наибольшим влиянием. Если любое из этих изменений отвечает критерию изменения старшей версии протокола, тогда старшая версия должна быть увеличена.

Примеры изменений протокола, которые могут привести к изменению номер младшей версии:

- Введение нового дополнительного объекта так долго, что включение нового объекта в сообщение не приводит к введению новых обязательных функциональных требований для элемента сети, получающего данное сообщение, так что данный объект может быть безопасно игнорирован.
- Неодобрение дополнительного объекта.

Примеры изменений протокола, которые могут привести к изменению номер старшей версии:

- Введение нового сообщения.
- Изменение в формате данного объекта.
- Грамматическое изменение, которое запретило включение данного объекта в данное сообщение.
- Грамматическое изменение, которое сделало объект обязательным в данном сообщении.
- Грамматическое сообщение, которое сделало объект дополнительным в сообщении, в котором он ранее был обязательным.
- Введение нового дополнительного объекта, который, будучи включенным в сообщение, вводит новые обязательные функциональные требования для элемента сети, получающего это сообщение, так что объект не может быть безопасно игнорирован.
- Семантическое изменение в протоколе, связанное с алгоритмами или состоянием (таким, как машина состояния шлюза), которое может привести к несовместимости состояния между устройствами, использующими старую и новую версии протокола.

Некоторые изменения, к примеру, такие, которые вводят новые функциональные средства, трудно поддаются классификации. Например, можно представить изменение, которое вводит новый объект и функциональные требования для элемента сети, получающего объект в сообщении. Если элемент сети, получающий объект, работал с младшей версией протокола, в которой новый объект не был определен, тогда линия поведения по умолчанию будет такой, что объект будет игнорироваться, и, следовательно, линия поведения, предложенная новым объектом, не будет работать. Если новая линия поведения, которая не работает вследствие того, что объект игнорируется, была локальной по отношению к принимающему элементу сети, можно поспорить, что в таком случае два элемента сети успешно взаимодействуют при младшей версии протокола. Если, с другой стороны, присутствие нового объекта в сообщении требует от принимающего элемента сети отправить новый запрос или видоизменить существующий ответ, основанный на новом объекте, тогда игнорирование нового объекта может предотвратить взаимодействие. В последнем случае может понадобиться изменение старшей версии.

Другие изменения, такие, которые изменяют состояние объекта внутри сообщения от обязательного до дополнительного или наоборот, могут привести к осуществлению взаимодействия на основе линии поведения отправителя. Тем не менее, так как линия поведения отправителя с учетом дополнительных параметров не может быть гарантировано, такие изменения должны классифицироваться как старшие изменения.

Учитывая, что много типов изменений протокола потребуют изменения старшей версии протокола, имеет смысл сгруппировать изменения в протоколе таким образом, что изменения старшей версии будут встречаться нечасто, а новые версии будут иметь важное значение, которое оправдывало бы их воплощение.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	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	Качество телефонной передачи, телефонные установки, сети местных линий
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 телекоммуникации