МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

J.163

(11/2005)

СЕРИЯ J: КАБЕЛЬНЫЕ СЕТИ И ПЕРЕДАЧА СИГНАЛОВ ТЕЛЕВИЗИОННЫХ И ЗВУКОВЫХ ПРОГРАММ И ДРУГИХ МУЛЬТИМЕДИЙНЫХ СИГНАЛОВ

Проект IPCablecom

Динамическое качество обслуживания для обеспечения услуг режима реального времени по сетям кабельного телевидения с использованием кабельных модемов

Рекомендация МСЭ-Т J.163

Рекомендация МСЭ-Т J.163

Динамическое качество обслуживания для обеспечения услуг режима реального времени по сетям кабельного телевидения с использованием кабельных модемов

Резюме

В данной Рекомендации рассматриваются требования к устройству клиента для получения доступа к ресурсам сети. В частности, в ней определен комплексный механизм для того, чтобы устройство клиента могло запрашивать определенное Качество обслуживания (QoS) от сети DOCSIS. Использование данной Рекомендации иллюстрирует большое количество примеров. Сфера применения этой Рекомендации заключается в определении архитектуры QoS для части "доступ" сети IPCablecom, предоставляемую для запрашивающих приложений на основе каждого потока. Часть доступа сети определена как находящаяся между Адаптером медиатерминала (MTA) и Системой завершения кабельного модема (CMTS), включая сеть DOCSIS. Метод распределения QoS через магистральную линию в данной Рекомендации не рассмотрен. Интерфейс для управляемой магистральной линии IP и вопросы, связанные с многоадресной передачей IP, не входят в область применения данной Рекомендации. В этой Рекомендации также признается, что в пределах помещения пользователя может потребоваться резервирование на основе каждого потока, и разработанные протоколы учитывают эту потенциальную потребность.

Источник

Рекомендация МСЭ-Т J.163 была утверждена 29 ноября 2005 года 9-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.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 1 ВАСЭ.

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

ПРИМЕЧАНИЕ

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

Соблюдение положений данной Рекомендации 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/.

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 и соглашения по терминам	2
4.1	Сокращения	2
4.2	Соглашения по терминам	3
5	Технический обзор	3
5.1	Требования к архитектуре QoS проекта IPCablecom	4
5.2	Сетевые элементы доступа QoS проекта IPCablecom	6
5.3	Архитектура динамического QoS проекта IPCablecom	7
5.4	Интерфейсы QoS	8
5.5	Структура для QoS проекта IPCablecom	10
5.6	Требования к управлению ресурсами сети доступа	12
5.7	Теория функционирования	16
6	Протокол QoS для встроенного адаптера MTA – модема CM (pkt-q1)	22
6.1	Сочетание FlowSpecs протокола RSVP	23
6.2	Поддержка в DOCSIS резервирования ресурса	33
6.3	Использование интерфейса управляющей службы MAC сети DOCSIS	41
7	Описание интерфейса авторизации (pkt-q6)	45
7.1	Шлюзы: структура для управления QoS	45
7.2	Профиль COPS для проекта IPCablecom	50
7.3	Форматы сообщений в протоколе управления шлюзом	52
7.4	Работа протокола управления шлюзом	61
7.5	Использование CMS протокола шлюза	68
7.6	Координация шлюзов	68
Приложение A – Определения таймеров и их значения		70
Дополнения I – VIII и XI		72
Дополнение IX – Сценарии кражи услуг		72
IX.1	Сценарий № 1: Клиенты, сами устанавливающие соединения с высоким QoS	72
IX.2	Сценарий № 2: Клиенты, использующие предоставляемое QoS для неречевых приложений	73
IX.3	Сценарий № 3: Адаптер MTA, меняющий адрес пункта назначения в речевых пакетах	73
IX.4	Сценарий № 4: Использование половинных соединений	73
IX.5	Сценарий № 5: Раннее завершение, после которого осталось половинное соединение	73
IX.6	Сценарий № 6: Поддельные сообщения координации шлюза	73
IX.7	Сценарий № 7: Обман, направленный против нежелательных вызывающих пользователей	74

Стр.

Дополнение X – COPS (Общая открытая служба политики) 74
X.1 Процедуры и принципы COPS 74
X.2 Сравнение COPS и LDAP для политики 75
Дополнение XII – Анализ TCP 76
XII.1 Требования 76
XII.2 Рекомендуемые изменения 76
XII.3 Установление соединения TCP, воздействующее на задержку после набора номера 77
XII.4 Необходимость низкой задержки для пакетов между GC и CMTS, даже при потерях 78
XII.5 Блокирование заголовка строки 78
XII.6 Медленный старт протокола TCP 79
XII.7 Задержка пакетов: алгоритм Nagle 79
XII.8 Интерфейс без блокировки 79

Рекомендация МСЭ-Т J.163

Динамическое качество обслуживания для обеспечения услуг режима реального времени по сетям кабельного телевидения с использованием кабельных модемов

1 Сфера применения

В данной Рекомендации рассматриваются требования к устройству пользователя для получения доступа к ресурсам сети. В частности, в ней определен комплексный механизм для того, чтобы устройство пользователя могло запрашивать определенное качество обслуживания от сети DOCSIS. Использование данной Рекомендации иллюстрируют многочисленные примеры. Сфера применения этой Рекомендации заключается в определении архитектуры QoS для части "доступ" сети IPCablecom, предоставляемую для запрашивающих приложений на основе каждого потока. Часть доступа сети определена как находящаяся между Адаптером медиатерминала (MTA) и Системой завершения кабельного модема (CMTS), включая сеть DOCSIS. Метод распределения QoS через магистральную линию в данной Рекомендации не рассмотрен. Интерфейс к управляемой магистральной линии IP и вопросы, связанные с многоадресной передачей IP, не входят в область применения данной Рекомендации. В этой Рекомендации также признается, что в пределах помещения пользователя может потребоваться резервирование на основе каждого потока, и разработанные протоколы учитывают эту потенциальную потребность.

2 Справочные документы

2.1 Нормативные справочные документы

В перечисленных ниже Рекомендациях МСЭ-Т и другой справочной литературе содержатся положения, которые посредством ссылки на них в данном тексте составляют основные положения данной Рекомендации. На момент опубликования, действовали указанные редакции документов. Все Рекомендации и другая справочная литература являются предметом корректировки, и стороны пришли к договоренности основываться на этой Рекомендации и стараться изыскивать возможность для использования самых последних изданий Рекомендации и справочной литературы, перечисленной ниже. Регулярно публикуется перечень действующих Рекомендаций МСЭ-Т. Ссылка на документ в рамках этой Рекомендации не дает ему, как отдельному документу, статуса рекомендации.

- ITU-T Recommendation J.83 (1997), *Digital multi-programme systems for television, sound and data services for cable distribution*.
- ITU-T Recommendation J.112 (1998), *Transmission systems for interactive cable television services*.
- ITU-T Recommendation J.112 Annex A (2001), *Digital Video Broadcasting: DVB interaction channel for Cable TV (CATV) distribution systems*.
- ITU-T Recommendation J.112 Annex B (2004), *Data-over-cable service interface specifications: Radio-frequency interface specification*.
- ITU-T Recommendation J.160 (2005), *Architectural framework for the delivery of time-critical services over cable television networks using cable modems*.
- ITU-T Recommendation J.161 (2001), *Audio codec requirements for the provision of bidirectional audio service over cable television networks using cable modems*.
- IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol*.

2.2. Информативные справочные документы

- ITU-T Recommendation G.114 (2003), *One-way transmission time*.
- ITU-T Recommendation G.711 (1988), *Pulse code modulation (PCM) of voice frequencies*.

– ITU-T Recommendation G.726 (1990), *40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM)*.

– ITU-T Recommendation G.728 (1992), *Coding of speech at 16 kbit/s using low-delay code excited linear prediction*.

– ITU-T Recommendation G.729 Annex E (1998), *11.8 kbit/s CS-ACELP speech coding algorithm*.

– ITU-T Recommendation J.162 (2005), *Network call signalling protocol for the delivery of time-critical services over cable television networks using cable modems*.

– ITU-T Recommendation J.164 (2005), *Event message requirements for the support of real-time services over cable television networks using cable modems*.

– ITU-T Recommendation J.170 (2005), *IPCablecom security specification*.

– IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program – Protocol specification*.

– IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal control*.

– IETF RFC 2327 (1998), *SDP: Session Description Protocol*.

– IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

– IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control*.

3 Термины и определения

В данной Рекомендации определяются следующие термины:

3.1 кабельный модем: кабельный модем представляет собой оконечное устройство второго уровня, которое завершает соединение со стороны заказчика DOCSIS или J.122.

3.2 поток DOCSIS: Однонаправленный или двунаправленный поток пакетов данных, который является предметом сигнализации уровня MAC и присвоения QoS, соответствующих Рекомендации МСЭ-Т J.112 (или Рекомендации МСЭ-Т J.122).

3.3 IPCablecom: Проект МСЭ-Т, в который включены архитектура и серии Рекомендаций, делающие возможной поставку услуг в режиме реального времени по сетям кабельного телевидения с использованием кабельных модемов.

4 Сокращения и соглашения по терминам

4.1 Сокращения

В данной Рекомендации используются следующие сокращения:

CM	Cable Modem	Кабельный модем
CMTS	Cable Modem Termination System	Система завершения кабельного модема
COPS	Common Open Policy Service	Общая открытая служба политики
CPE	Customer Premises Equipment	Оборудование в помещении пользователя
DCS	Distributed Call Signalling	Распределенная сигнализация вызова
DSA	Dynamic Service Addition	Динамическое дополнение службы
DSC	Dynamic Service Change	Динамическое изменение службы
INA	Interactive Network Adapter	Диалоговый сетевой адаптер
IP	Internet Protocol	Протокол Интернет
MTA	Media Terminal Adaptor	Адаптер медиатерминала
NCS	Network-based Call Signalling	Сигнализация вызова, основанная на сети
PHS	Payload Header Suppression	Подавление заголовка полезной нагрузки

PSTN	Public Switched Telephone Network	Коммутируемая телефонная сеть общего пользования	КТСОП
QoS	Quality of Service	Качество обслуживания	
RAP	Resource Allocation Protocol	Протокол распределения ресурсов	
RSVP	Resource ReSerVation Protocol	Протокол резервирования ресурсов	
TLV	Type-Length-Value	Значение типа длины	
VAD	Voice Activity Detection	Обнаружение активности речи	

4.2 Соглашения по терминам

В тексте данной Рекомендации, слова, используемые для определения значимости специфических требований, выделяются прописными буквами. К таким словам относятся:

"ДОЛЖЕН" Это слово или глагол "ТРЕБУЕТСЯ" означает, что данное требование является абсолютным для данной Рекомендации.

"НЕ ДОЛЖЕН" Это выражение означает, что на данный аспект налагается абсолютный запрет в данной Рекомендации.

"ЖЕЛАТЕЛЬНО" Это слово или глагол "РЕКОМЕНДУЕТСЯ" означает, что в определенных обстоятельствах могут существовать веские причины, которые позволяют игнорировать данный аспект, но прежде чем принять данное решение должны в полной мере быть взвешены все последствия, а ситуация тщательно проанализирована.

"НЕЖЕЛАТЕЛЬНО" Это слово означает, что могут существовать веские причины, когда в определенных обстоятельствах, указанный образ действий допустим и даже полезен, но при осуществлении действия, отличного от рекомендованного, ситуация должна быть тщательно проанализирована, а последствия этого должны быть осознаны.

"МОЖНО" Это слово или наречие "НЕОБЯЗАТЕЛЬНО" означает, что данный аспект действительно не является обязательным. Конкретный продавец может рассматривать данный аспект как желательный в конкретных условиях рынка или в целях улучшения продукта, другие продавцы могут игнорировать данное требование.

5 Технический обзор

Для поддержки диалоговых мультимедийных приложений требуется улучшенное качество обслуживания (QoS). Ресурсы могут быть ограничены в сегментах сети, что требует распределения ресурсов в сети. Область применения этой Рекомендации состоит в определении архитектуры качества обслуживания для части "доступ" ("Access") сети проекта IPCablecom. Часть доступа сети определяется как находящаяся между Адаптером медиатерминала (MTA) и Системой оконечного устройства кабельного модема (CMTS), включая сеть DOCSIS. В этой Рекомендации также признается, что в пределах помещения пользователя может потребоваться резервирование на основе каждого потока, и протоколы, разработанные в Рекомендации, учитывают эту потенциальную потребность. Хотя некоторые сегменты магистральной сети могут требовать резервирования ресурсов, чтобы обеспечивать соответствующее качество обслуживания, здесь учитывается, что протоколы для управления магистральными ресурсами выходят за рамки этой Рекомендации.

В сети DOCSIS ресурсы распределяются для индивидуальных потоков, связанных с каждым сеансом приложения на каждого абонента, на основе авторизации и аутентификации. Сеанс DQoS, или просто сеанс, определяется этой Рекомендацией как отдельный двунаправленный поток данных между двумя пользователями. Когда мультимедийное приложение нуждается в многократных двунаправленных потоках данных (например, один для голоса и отдельный для видео), то устанавливаются отдельные сеансы DQOS для каждого из видов информации. Приложения могут использовать только половину двунаправленного потока данных сеанса, таким образом, обеспечивая услуги только передачи или только приема. Например, в типичном приложении голосовой связи

простая связь между двумя участниками осуществляется посредством отдельного сеанса, а комплексная связь с множеством участников (например, "вызовы конференц-связи") – посредством нескольких одновременных сеансов.

Сигнализация вызова на основе сети (Рекомендация МСЭ-Т J.162) является определенным протоколом сигнализации вызовов IPCablecom. Эта спецификация динамического качества QoS является основной структурой QoS для этого протокола сигнализации вызова. Качество QoS распределяется для потоков, связанных с сеансом, совместно с протоколом сигнализации.

Эта Рекомендация вводит понятие структуры посегментного качества QoS. Она использует информацию, доступную от протоколов сигнализации, чтобы осуществить назначение QoS как на "местном" сегменте (на участке сети DOCSIS, приближенном к исходящему участнику), так и на "удаленном" сегменте (на участке сети DOCSIS, приближенном к завершающему участнику). Таким образом, эта Рекомендация позволяет различным поставщикам использовать наиболее подходящие механизмы для сегмента, которым они управляют. Используя связь сегментов с качеством QoS, предоставляют сквозную гарантию качества QoS для сеанса.

Спецификация динамического качества QoS включает протоколы, которые дают возможность поставщикам услуг речевой пакетной связи с использованием структуры IPCablecom применять различные модели тарификации, включая как тарификацию на основе фиксированной ставки, так и тарификацию, зависящую от использования. Намерение этой Рекомендации состоит в том, чтобы гарантировать, что расширенное качество QoS обеспечивается только уполномоченным и заверенным пользователям. Конкретные методы, использованные для авторизации и опознавания пользователя, выходят за рамки этой Рекомендации.

Эта спецификация динамического качества QoS признает требования коммерчески жизнеспособной услуги голосовой связи, аналогичной той, что предлагается посредством коммутируемой телефонной сети общего пользования. Важно гарантировать, чтобы ресурсы были доступны перед тем, как оба участника приглашаются для осуществления связи. Таким образом, ресурсы резервируются прежде, чем получатель услуги связи уведомляется о том, что кто-то пытается инициировать связь. Если для сеанса нет достаточных ресурсов, то сеанс блокируется.

В протоколах, разработанных в этой Рекомендации, четко признается необходимость гарантировать, что нет возможности для подделки или кражи услуги пользователями в точках завершения, которые не желают сотрудничать с сигнализацией вызова и протоколами сигнализации QoS с намерением избежать тарификации за использование. Эта Рекомендация вводит понятие двухфазного резервирования ресурса (зарезервировать и зафиксировать). Эти две фазы позволяют поставщику распределять ресурсы только тогда, когда они требуются (когда просекается голосовой тракт), что может использоваться для составления счета. Более того, поскольку вторая фаза для фиксации ресурсов требует явного запроса от адаптера MTA, она дает возможность поставщику предотвратить мошенничество и кражу услуги

Эта Рекомендация технически совместима с соответствующим документом PacketCable CableLabs: *PacketCable Dynamic Quality-of-Service Specification* PKT-SP-DQOSI 5 I01.

5.1 Требования к архитектуре QoS проекта IPCablecom

В следующем ниже перечне представлены требования QoS для поддержки мультимедийных приложений по сетям проекта IPCablecom.

1) *Обеспечить ведение учета IPCablecom для ресурсов QoS на основе каждого сеанса*

   Ожидается, что с точки зрения выписки счетов, один из ресурсов, который должен учитываться, представляет собой использование качества QoS в сети DOCSIS. Таким образом, информация нуждается в том, чтобы быть идентифицированной и отслеживаемой, что позволяет согласовывать использование ресурсов QoS DOCSIS с деятельностью сеанса IPCablecom.

2) *Наличие как двухфазной модели активации QoS (зарезервировать–зафиксировать), так и однофазной модели активации QoS (зафиксировать)*

   Под управлением приложения должно быть возможным использование либо двухфазной, либо однофазной модели активации QoS. В двухфазной модели приложение резервирует ресурс, а затем позднее фиксирует его. В однофазной модели как резервирование, так и

фиксация происходят в качестве отдельной автономной операции. Аналогично модели DOCSIS, ресурсы, которые зарезервированы, но еще не зафиксированы, являются доступными для временного назначения другим обслуживающим потокам DOCSIS (например, лучшее усилие). Эта Рекомендация предоставляет механизмы как для двухфазной, так и для однофазной активации для встроенных адаптеров MTA.

3) *Обеспечить политики, определенные проектом IPCablecom, чтобы управлять качеством QoS как в сети DOCSIS, так и в магистральной сети IP*

Для различных типов сеансов должно быть возможным иметь различные характеристики QoS. Например, сеансы в пределах области (домена) поставщика единственного оператора кабельной сети могут получать различные значения QoS, в отличие от сеансов вне пределов области (например, международные сеансы, включая связи к сети КТСОП). Эта спецификация динамического QoS позволяет оператору кабельной сети обеспечивать различные значения QoS для различных типов клиентов (например, более высокое качество QoS для абонентов делового обслуживания в определенные моменты дня по сравнению с клиентами-жильцами) или для различных типов приложений для одного клиента.

4) *Предотвратить (свести к минимуму) злоупотребляющее использование QoS*

Определены два типа злоупотребляющего использования QoS: то, на которое точно выставляется счет, но которое приводит к отказу другим клиентам в обслуживании, и то, на которое счет точно не выставляется и которое приводит к краже услуги. Абонентские приложения и приложения IPCablecom (либо встроенные, либо на основе персонального компьютера ПК) могут неосторожно или преднамеренно злоупотреблять своими привилегиями QoS [например, использовать расширенное качество QoS, которое поставщик хочет ограничить голосовыми приложениями, приложением протокола передачи файлов (FTP)]. Даже при том, что сеть DOCSIS, как ожидается, будет навязывать абонентский доступ к QoS, должны существовать богатая пакетная классификация и механизмы управления сигнализацией, чтобы охранять абонента (и абонентские устройства) от мошеннического использования QoS. Следует использовать процедуры управления доступом, чтобы уменьшить атаки типа "отказ в обслуживании".

5) *Обеспечивать механизмы управления доступом как для восходящего, так и для нисходящего потока в сети DOCSIS*

Качеству QoS как восходящего, так и нисходящего потока следует быть предметом управления доступом на основе каждого сеанса.

6) *QoS для DOCSIS*

Должно быть возможным осуществлять наблюдение (определяемое как маркирование, удаление или задержка пакетов) за всеми аспектами QoS, определенными в обслуживании на системе CMTS, используя механизмы QoS DOCSIS. Кроме того, должно быть возможным поддерживать модели преобразования многократных потоков: связывать единственный сеанс IPCablecom с единственным обслуживающим потоком и многократные сеансы IPCablecom – с единственным обслуживающим потоком.

7) *Политика предписана CMTS*

Окончательное управление политикой поручается CMTS. Доктрина состоит в том, что любой клиент может сделать запрос на любое качество QoS, но CMTS (или объект после CMTS) является единственным объектом, которому поручено предоставлять или отклонять запросы по качеству QoS.

8) *Объекты IPCablecom, насколько это возможно, не должны быть осведомлены об особых примитивах и параметрах QoS DOCSIS*

Для проекта IPCablecom, подобно любому другому приложению, которое использует IP-сеть, цель проектирования состоит в том, чтобы свести к минимуму количество сведений, характерных для звеньев доступа в прикладном уровне. Чем меньше сведений о связях доступа в прикладном уровне, тем больше приложений будет доступно для разработки и развертывания, и тем меньше будет проблем по испытаниям и поддержке.

9) *Повторное использование ресурсов QoS для недействующих/устаревших сеансов*

Необходимо использовать и перераспределять драгоценные ресурсы QoS, принадлежащие сеансам, которые больше не являются активными, но не были должным образом отсечены.

Не следует иметь "утечек" ресурсов в звене DOCSIS. Например, если модуль клиента IPCablecom работает неисправно посреди сеанса IPCablecom, то все ресурсы QoS DOCSIS, используемые сеансом, следует освободить в пределах приемлемого промежутка времени.

10) *Динамическое изменение политики QoS*

Желательно динамически изменять политику QoS для абонентов. Например, это требование обращается к способности изменять уровень обслуживания клиента (например, расширенный от "бронзового" обслуживания до "золотого" обслуживания) на ходу, без переустановки модема CM.

11) *Абсолютное минимальное время задержки при установлении сеанса и после поднятия трубки*

Для потребителя сеть IPCablecom должна позволять эмуляцию и расширение опыта сети КТСОП, а также должна быть одинаково доброжелательной, если не лучше, в измерениях задержки при установлении сеанса и после снятия трубки.

12) *Многократные одновременные сеансы*

Желательно распределять ресурсы QoS (например, полосу пропускания) не только для индивидуальных двухточечных сеансов, но также и для многократных двухточечных сеансов (например, вызовы конференцсвязи, составные вызовы аудио/видео).

13) *Динамическая подстройка параметров QoS в середине сеансов IPCablecom*

Для услуги IPCablecom должна существовать возможность изменения QoS в середине сеанса, например, осуществление на всей сети настройки ресурсов или создание совместимых параметров КОДЕКА (требующих изменения QoS), или наличие определяемой пользователем характеристики для изменения уровней QoS, или обнаружение потоков данных факсимильных аппаратов или модемов (требующее изменения метода сжатия КОДЕКА по сравнению с Рекомендацией МСЭ-Т G.711).

14) *Поддерживать модели управления многократными QoS*

Могут быть исполнены крайние случаи для инициации сигнализации QoS как от абонентской стороны, так и от сетевой стороны. В сигнализации от абонентской стороны приложение может инициализировать свой запрос на качество QoS немедленно, когда приложение считает, что оно нуждается в QoS. Кроме того, сигнализация от абонентской стороны поддерживает прикладные модели, которые являются равноправными. В сигнализации от сетевой стороны реализация приложения конечной точки может не иметь полного представления о качестве QoS (особенно в сети DOCSIS). Сигнализация от сетевой стороны поддерживает прикладные модели, которые построены по принципу "клиент-сервер" (с сервером, которому доверяют). Ожидается, что в сетях IPCablecom (и в другом приложении) будут присутствовать обе модели. Эта Рекомендация предназначена только для сигнализации от абонентской стороны.

15) *Поддержка сигнализации QoS как от встроенного адаптера MTA, так и от автономного адаптера MTA*

Следует иметь возможность сообщать о качестве QoS как от встроенного адаптера MTA, так и от автономного адаптера MTA. Данная Рекомендация относится только ко встроенным адаптерам, использующим прямой доступ к сигнализации MAC DOCSIS.

5.2 Сетевые элементы доступа QoS проекта IPCablecom

Для поддержки QoS в сетях IPCablecom используются следующие сетевые элементы.

5.2.1 Адаптер мультимедийного терминала (MTA)

Сетевым клиентским устройством IPCablecom (т. е. адаптером MTA) может быть одно из следующих устройств. Эти устройства постоянно находятся в помещении клиента и через канал DOCSIS соединены с сетью. Предполагается, что все адаптеры MTA должны осуществлять некоторый протокол сигнализации мультимедиа, например, типа J.162. Адаптер MTA может быть либо устройством со стандартным двухпроводным телефонным аппаратом в конфигурации MTA-1, или может добавлять возможности ввода/выхода видео в конфигурации MTA-2. Он может иметь минимальные возможности или может осуществлять эти функциональные возможности на мультимедийном персональном компьютере и иметь в своем распоряжении все возможности персонального компьютера.

С точки зрения качества QoS имеются два типа адаптеров MTA.

1) **Встроенный/интегрированный адаптер MTA**. Это мультимедийный терминал клиента, который включает в себя интерфейс MAC-уровня DOCSIS к сети DOCSIS.

2) **Автономный адаптер MTA**. Это клиент, который осуществляет мультимедийные функциональные возможности без включения в состав интерфейса MAC-уровня DOCSIS. Автономный адаптер MTA будет обычно использовать Ethernet, USB, (универсальную последовательную шину) или устройство по стандарту IEEE 1394 в качестве физического присоединения к модему CM. Автономный адаптер MTA может быть подсоединен к сети клиента и использовать транспортные средства сети клиента (возможно, включая промежуточные маршрутизаторы IP), чтобы устанавливать сеансы через сеть DOCSIS.

5.2.2 Кабельный модем (CM)

Это сетевой элемент IPCablecom, как определено Рекомендацией Рек. МСЭ-Т J.112 или Рекомендацией МСЭ-Т J.122. Кабельный модем (CM) отвечает за классификацию, осуществление наблюдения и маркирование пакетов, как только протоколами сигнализации, описанными здесь, устанавливаются потоки трафика.

5.2.3 Система оконечного устройства кабельного модема (CMTS)

CMTS отвечает за распределение и планирование ширины полосы для восходящего и нисходящего потоков в соответствии с запросами MTA и авторизациями качества QoS, установленными администратором сети. CMTS действует как точка осуществления политики (PEP) на каждую структуру протокола распределения ресурсов (RAP) IETF (RFC 2753).

CMTS осуществляет "шлюз динамического качества QoS проекта IPCablecom" (здесь и далее называемый просто "шлюзом") между сетью DOCSIS и магистральной сетью IP. Шлюз реализуется с использованием пакетной классификации и функций фильтрации, определенных в Рекомендациях Рек. МСЭ-Т J.112 и J.122.

CMTS может быть или может не быть также конфигурирован в качестве объекта "Граница IS-DS". Граница IS-DS осуществляет стык между сетями, используя модель интегрированной услуги (IntServ) управления качеством QoS и некоторую другую модель, например дифференцированные услуги (DiffServ).

5.2.4 Сервер управления вызовом (CMS) и контроллер шлюза (GC)

Объект сервера управления вызовом IPCablecom (CMS) выполняет обслуживание, которое разрешают адаптерам MTA устанавливать мультимедийные сеансы (включая такие приложения голосовой связи, как "IP-телефония" или "VoIP"). Термин "контроллер шлюза" (GC) используется для того, чтобы сослаться на часть любого типа сервера CMS, который осуществляет функции, относящиеся к качеству обслуживания.

В модели динамического качества QoS проекта IPCablecom контроллер шлюза управляет операцией шлюзов, осуществленных на CMTS. Контроллер GC действует в качестве точки решения политики (*PDP*) согласно структуре протокола распределения ресурса (RAP) IETF (RFC 2753).

5.2.5 Сервер хранения записей (RKS)

Сервер хранения записей (RKS) является сетевым элементом IPCablecom, который только получает информацию от элементов IPCablecom, описанных в этой Рекомендации. Сервер RKS можно использовать в качестве сервера начисления оплаты, диагностического инструмента и пр.

5.3 Архитектура динамического QoS проекта IPCablecom

Архитектура QoS проекта IPCablecom основывается на Рекомендации МСЭ-Т J.112, протоколе RSVP IETF и гарантированном качестве QoS интегрированных услуг IETF.

Более точно архитектура QoS проекта IPCablecom использует протокол в пределах сети кабельного телевидения так, как определено в Рекомендации МСЭ-Т J.112. Эти сообщения поддерживают статическую и динамическую установку пакетных классификаторов (т. е. Filter-Specs) и механизмы планирования потока (т. е. flowSpecs), чтобы доставить улучшенное качество обслуживания. Качество QoS из DOCSIS основано на объектах, которые описывают спецификации трафика и потока, подобно объектам TSpec и RSpec, как определено в протоколе резервирования ресурса

(RSVP, Resource reSerVation Protocol) IETF. Это позволяет определять резервирование ресурса QoS на основе каждого потока.

В архитектуре QoS из DOCSIS потоки трафика рассматриваются как однонаправленные, таким образом интерактивный сеанс включает два потока, которые являются предметом операций, показанных ниже. Для каждого (однонаправленного) потока:

Модем CM, где трафик входит в кабельную сеть с качеством IP QoS, является ответственным за:

- Классификацию трафика IP в потоках IP QoS, основанную на определяемых спецификациях фильтра.
- Осуществление формирования трафика и осуществление контроля, как требуется спецификацией потока.
- Поддержание состояния для активных потоков.
- Изменение поля TOS в заголовках IP восходящего потока, основанное на политике сетевого оператора.
- Получение требуемого качества QoS от CMTS.
- Применение механизмов QoS DOCSIS должным образом.

CMTS является ответственным за:

- Предоставление требуемого QoS модему CM, основанного на конфигурации политики.
- Распределение полосы пропускания восходящего потока в соответствии с запросами модема CM и сетевыми политиками QoS.
- Классификацию каждого прибывающего пакета от интерфейса сетевой стороны и за назначение ему уровня QoS, основанного на определенных фильтром спецификациях.
- Осуществление наблюдения за полем TOS в пакетах, полученных от кабельной сети чтобы навязывать установки полей TOS согласно политике каждого сетевого оператора.
- Изменение поля TOS в заголовках IP нисходящего потока, основанное на политике сетевого оператора.
- Осуществление формирования трафика и осуществление контроля, как требуется спецификацией потока.
- Перенаправление пакетов нисходящего потока к сети DOCSIS, используя назначенное качество QoS.
- Перенаправление пакетов восходящего потока к устройствам магистральной сети, используя назначенное качество QoS.
- Поддержание состояния для активных потоков.

Магистральная сеть может использовать либо механизмы, основанные на интегрированных услугах IETF, либо использовать механизмы дифференцированных услуг IETF. В магистральной услуге DiffServ сетевые маршрутизаторы направляют пакет, обеспечивая соответственное качество QoS IP, основанное на установке поля TOS. В магистральной услуге DiffServ требуется состояние по каждому потоку в устройствах магистральной сети.

5.4 Интерфейсы QoS

Интерфейсы сигнализации о качестве обслуживания определяются между многими из компонентов сети IPCablecom, как показано на рисунке 1. Сигнализация включает в себя процесс передачи информации о требованиях QoS на прикладном уровне (например, параметры SDP), на сетевом уровне (например, RSVP) и на уровне звена передачи данных (например, QoS DOCSIS). Кроме того, требование для осуществления политики и связей систем между обеспечением абонента OSS, управлением доступом в пределах управляемой магистральной сети IP и управлением доступом в пределах сети DOCSIS создает потребность в дополнительных интерфейсах между компонентами в сети IPCablecom .

Расширенное объяснение архитектурной структуры QoS содержится в архитектурной структуре IPCablecom, Рекомендации МСЭ-T J.160 и показано на рисунке 1

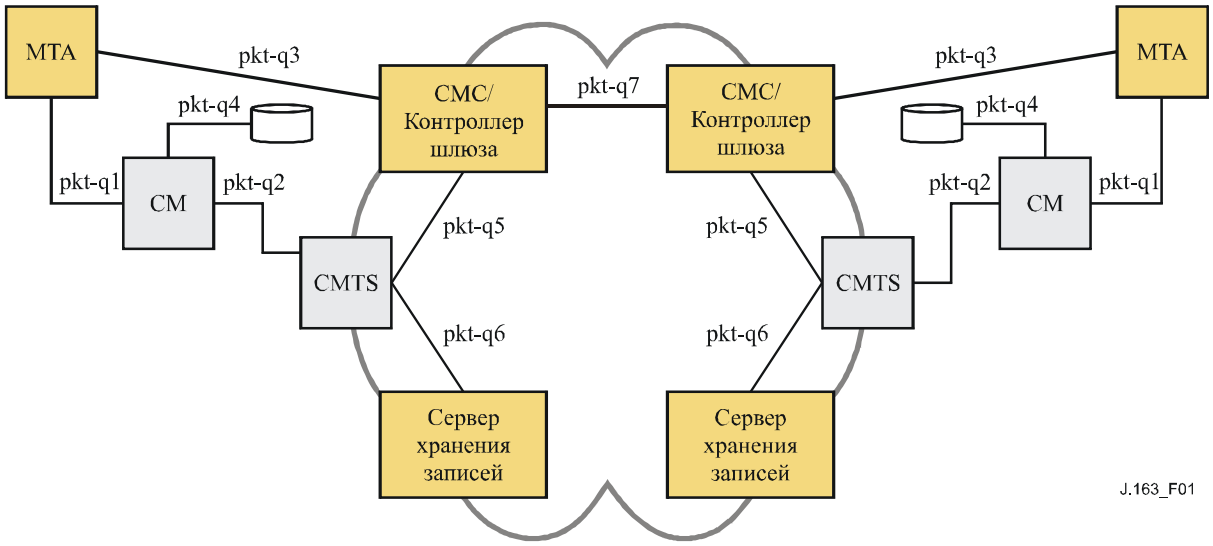


Рисунок 1/J.163 – Интерфейсы сигнализации QoS в сети IPCablecom

Интерфейсы от pkt-q1 до pkt-q7 доступны для управления и обработки QoS. Не все интерфейсы используются во всех конфигурациях и вариантах протоколов. Все интерфейсы, кроме интерфейса pkt-q5, используются системой DQOS. В таблице 1 кратко определен каждый интерфейс и то, как каждый интерфейс используется в этой спецификации динамического качества QoS (DQoS, Dynamic QoS).

Таблица 1/J.163 – Интерфейсы DQoS

Интерфейс	Описание	Встроенный адаптер MTA DQoS (дополнительный)
pkt-q1	MTA-CM	Интерфейс службы управления MAC E-MTA
pkt-q2	CM-CMTS	QoS DOCSIS, инициированный модемом CM
pkt-q3	MTA-GC/CMC	NCS
pkt-q4	Сервер подготовки к работе CM	N/A
pkt-q5	GC-CMTS	Управление шлюзом
pkt-q6	CMTS-RKS	Выписка счетов
pkt-q7	CMC-CMC	Сигнализация от CMC к CMC

pkt-q1: Интерфейс между адаптером MTA и модемом CM

Этот интерфейс определяется только для встроенного адаптера MTA. Интерфейс раскладывается на три вспомогательных интерфейса (подинтерфейса):

- Управление: используется для управления обслуживающими потоками DOCSIS и их связанными параметрами трафика QoS и правилами классификации.
- Синхронизация: используется для того, чтобы синхронизировать пакетизацию, и для планирования минимальной задержки и дрожания.
- Транспорт: используется для обработки пакетов в потоке носителя информации и выполнения соответствующей обработки QoS по каждому пакету.

Этот интерфейс концептуально определен в Рек. МСЭ-Т J.112. Для автономных адаптеров MTA образец такого интерфейса не определяется.

pkt-q2: Интерфейс QoS DOCSIS между модемом CM и CMTS

Это интерфейс QoS сети DOCSIS (управление, планирование и транспорт). Функции управления могут быть инициированы либо модемом CM, либо CMTS. Однако CMTS является окончательным

арбитром политики и предоставляет ресурсы путем выполнения управления доступом для сети DOCSIS. Этот интерфейс определен в Рекомендации МСЭ-Т J.112.

pkt-q3: Сигнализация прикладного уровня между GC/CMC и адаптером MTA

Через этот интерфейс сигнализирует множество таких параметров, как поток среды передачи, адреса IP, номера портов и выбор характеристик кодека и пакетизации. Сигнализации DCS и NCS являются двумя примерами сигнализации прикладного уровня.

pkt-q4: Сигнализация от DOCSIS/Обеспечение из IPCablecom для модема CM

Этот интерфейс не используется для сигнализации QoS в DQoS.

pkt-q5: Интерфейс между GC/CMC и терминалами CMTS

Этот интерфейс используется для управления динамическими шлюзами для сеансов потоков среды передачи. Этот интерфейс дает возможность сети IPCablecom запрашивать и авторизовать качество QoS.

pkt-q6: Между CMTS и сервером хранения записей

Этот интерфейс используется CMTS, чтобы сигнализировать серверу RKS обо всех изменениях в авторизации и использовании сеанса.

pkt-q7: Интерфейс между терминалами CMTS

Этот интерфейс используется для управления сеансом и координации ресурсов между двумя CMC.

5.5 Структура для QoS проекта IPCablecom

Чтобы оправдать свои затраты к конечному пользователю, коммерческая мультимедийная услуга (например, возможность осуществления голосовой связи) может потребовать высокий уровень показателей качества транспорта и сигнализации, включая:

- Низкую задержку: сквозная задержка пакета должна быть достаточно малой, чтобы это не мешало нормальным мультимедийным взаимодействиям. Для нормальной телефонной услуги, использующей сеть КТСОП, МСЭ-Т рекомендует задержку сигнала туда и обратно не более 300 мс[1]. Задаваясь тем, что сквозная задержка распространения по магистральной сети может вобрать в себя существенное количество этого запаса задержки, важно управлять задержкой на канале доступа, по крайней мере, для дальних вызовов.
- Низкую потерю пакета: потеря пакета должна быть достаточно малой, чтобы качество речи или показатели качества факсимильных аппаратов и модемов голосовой ширины полосы ощутимо не повреждались. В то время как для воспроизведения понятной речи даже с высокими коэффициентами потерь могут использоваться алгоритмы сокрытия потерь, результирующее действие не может считаться адекватным для замены существующей телефонной службы с коммутацией каналов. Требования по потерям для приемлемого действия модемов голосовой ширины полосы являются даже более строгими, чем требования для голоса.
- Короткую задержку после набора номера: задержка между пользователем, сообщающим о запросе соединения, и принимаемым положительным подтверждением от сети должна быть достаточно короткой, чтобы пользователи не воспринимали разность от задержки после набора номера, к которой они привыкли в сети с коммутацией каналов, и не предполагали, что сеть потерпела неудачу. Эта задержка составляет порядка одной секунды.
- Короткую задержку после поднятия трубки: задержка между поднятием пользователем трубки звонящего телефона и просечкой голосового тракта должна быть достаточно

[1] В Рек. МСЭ-Т G.114 установлено, что задержка в одном направлении порядка 150 мс является приемлемой для большинства приложений пользователей. Однако приложения голоса и передачи данных с высокой степенью диалога могут ощущать ухудшение даже в том случае, если задержки составляют менее 150 мс. Поэтому следует препятствовать любому увеличению задержки обработки (даже на соединениях со временем передачи значительно ниже 150 мс), если нет явных выгод для услуги и приложения.

короткой, чтобы приветствие "алло" не было отсечено. Этой задержке следует быть не более нескольких сотен миллисекунд (в идеальном случае меньше, чем 100 мс).

Ключевым вкладом структуры динамического качества QoS является распознавание потребности в координации между сигнализацией, которая управляет доступом к конкретным прикладным услугам, и управлением ресурсами, которое управляет доступом к ресурсам сетевого уровня. Эта координация обеспечивает ряд критических функций. Это гарантирует, что подлинности пользователей установлены и им даны полномочия перед получением доступа к расширенному качеству QoS, связанному с услугой. Это гарантирует, что сквозные сетевые ресурсы будут доступны перед приведением в готовность адаптера MTA пункта назначения. Наконец, это гарантирует, что использование ресурсов рассчитано должным образом, совместимым с соглашениями по традиционному телефонному обслуживанию (которому некоторые услуги IPCablecom подобны с точки зрения клиента), в котором начисление оплаты происходит только после того, как участник, получающий связь, снимает трубку.

Чтобы поддерживать вышеуказанные требования, протоколы QoS обеспечивают, что все ресурсы фиксируются для всех транспортных сегментов перед тем, как протоколы сигнализации приведут в готовность пункт назначения. Аналогично, во время разрыва сеанса, протоколы QoS включают в себя меры для обеспечения того, чтобы все ресурсы, выделенные исключительно сеансу, были освобождены. Без этой координации между двумя направлениями потоков данных для пользователей было бы возможным разрушать управление качеством QoS и получать бесплатное обслуживание. Например, если платящий клиент завершает сеанс, а неплатящий клиент этого не делает, то остается "половинный канал", который можно использовать для мошеннического переноса данных в одном направлении. Протоколы QoS аппроксимируют семантику транзакции "все или ничего" для создания и разрушения сеанса.

Желательно, чтобы механизмы, используемые для осуществления сеанса, основывались на существующих стандартах и практике, а также чтобы результаты этой работы были пригодны для поддержки альтернативных моделей вызовов. Эти пожелания должны привести к использованию протокола реального времени IETF (RTP), чтобы переносить мультимедийные данные, транспортируемые с помощью протокола пользовательских дейтаграмм (UDP) IETF. Сигнализация в полосе рабочих частот для установления качества обслуживания осуществляется с использованием сообщений DOCSIS с динамическим качеством QoS.

Архитектуре QoS следует обеспечивать поддержку новых возникающих приложений, которые зависят от доставки многоадресных данных. Хотя это не является строгим требованием в архитектуре QoS, предоставление поддержки для многоадресной передачи обеспечит будущее развитие богатого набора мультимедийных приложений. Еще не исследовано, будут ли бесшовно поддерживать или нет многоадресную передачу введенные здесь расширения управления ресурсами.

Для целей управления качеством обслуживания несущий канал для сеанса управляется как три отличающихся сегмента: сеть доступа для исходящей стороны сеанса, магистральная сеть и сеть доступа для завершающей стороны сеанса. Сетевые ресурсы DOCSIS управляются как пара динамических обслуживающих потоков, используя механизмы, определенные в Рекомендации МСЭ-Т J.112. Магистральными ресурсами можно управлять либо на основе каждого потока, либо, более вероятно, с помощью механизма группового качества обслуживания. Управление магистральными ресурсами выходит за рамки этой Рекомендации.

Конструкция, определенная с помощью QoS, называемая *шлюзом,* предоставляет точку управления для подсоединения сетей доступа к магистральной услуге высокого качества. Шлюз реализуется с помощью системы CMTS и состоит из пакетного классификатора, наблюдателя за трафиком и интерфейса к объекту, который собирает статистические данные и события (все из этих компонентов существуют в сети DOCSIS). Шлюз может гарантировать, что только те сеансы, которые были авторизованы поставщиком услуг, получают услугу высокого качества. Шлюзы управляются выборочно для потока. Что касается услуг голосовой связи, основанных на IPCablecom, то они открыты для индивидуальных вызовов. Открытие шлюза включает в себя проверку управления доступом, которая выполняется тогда, когда от клиента принимается запрос на управление ресурсами для индивидуального сеанса, и в случае необходимости это может включать в себя резервирование ресурсов в сети для сеанса. Фильтр пакета восходящего потока в шлюзе позволяет потоку пакетов получать расширенное качество QoS для сеанса от определенного адреса источника IP и номера порта к определенному адресу пункта назначения IP и номеру порта. Фильтр нисходящего пакета в

шлюзе позволяет потоку пакетов получать расширенное качество QoS для сеанса от определенного адреса источника IP к определенному адресу пункта назначения IP и номеру порта.

Шлюз является логическим объектом, который постоянно находится в системе CMTS. Идентификатор GateID связан с индивидуальным сеансом и поддается интерпретации в шлюзе; GateID является идентификатором, который будет уникальным на местной основе в терминалах CMTS и назначается этой CMTS. Шлюз по своей природе является однонаправленным. Если шлюз "закрыт", то данные, идущие в нисходящем/восходящем потоках на сеть доступа DOCSIS, могут быть либо отброшены, либо могут обеспечивать услугу наилучшего усилия. Выбор отбрасывания пакетов или их обслуживания на основе наилучшего усилия является выбором политики поставщика.

Контроллер шлюза является ответственным за политику решения того, следует ли и когда открывать шлюз. Шлюз заранее устанавливается по запросу управления ресурсами. Это позволяет функции политики, которая располагается в контроллере шлюза, быть "без состояния", в том смысле, что она не нуждается в знании о состоянии сеансов, которые уже выполняются.

В то время как шлюз управляет потоком гарантированного качества QoS, другие потоки, такие как RTCP или сообщения сигнализации, не контролируются шлюзом. Поддержание улучшенного качества QoS для сообщений сигнализации может играть очень важную роль, в случае, если кабельная система использует высокий трафик с наибольшим усилием. Для достижения целей эффективной сигнализации, описанных в начале данного раздела, может оказаться решающим использование выделенного канала сигнализации с правильными конструкциями, определенными QoS. Необходимо отметить еще, что точная природа QoS, данного канала зависит от трафика и конструкции CMTS и оставляется на усмотрение продавца.

5.6 Требования к управлению ресурсами сети доступа

Обеспечение услуги голосовой связи по сетям IP с тем же самым уровнем качества, какой доступен на сети КТСОП, устанавливает границы на метрику задержки и потерь для голосовых пакетов и требует активного управления ресурсами как в сети доступа, так и в магистральной сети. Поставщик услуг должен быть способен управлять доступом к сетевым ресурсам, чтобы гарантировать, что адекватная пропускная способность доступна на сквозной основе, даже при необычном состоянии или состоянии перегрузки. Поставщик услуг может добиваться дополнительного дохода за обеспечение услуг голосовой связи с этими улучшенными характеристиками качества (т. е. качество кроме того, что получено при обслуживании по методу "наилучшего усилия"). Механизмы, предоставляемые здесь для управляемого доступа к улучшенному качеству QoS, дают возможность поставщику услуг гарантировать, что доступ обеспечивается только для уполномоченных и опознанных пользователей на посеансовой основе, и нет кражи такой услуги.

Клиенты услуги сообщают о своих параметрах трафика и эксплуатационных характеристиках "шлюзу" на краю сети, где сеть принимает решение об управлении доступом, основанное как на доступности ресурсов, так и на информации политики, связанной со шлюзом.

В DOCSIS пропускная способность сети ограничена, и необходимо осуществлять управление ресурсами "по каждому потоку". В магистральной сети могут иметься несколько альтернатив в диапазоне от "управления доступом по каждому транзитному участку для каждого потока" до крупномасштабного обеспечения ресурсов. Эта Рекомендация имеет дело только с качеством QoS сети доступа и не может служить руководством относительно схем QoS магистральных сетей.

5.6.1 Предотвращение кражи услуги

Сетевые ресурсы, выделенные сеансу, защищены от злоупотребления и включают:

- Авторизацию и защиту: Обеспечение того, что пользователи опознаны и уполномочены перед получением доступа к расширенному качеству QoS, связанному с услугой голосовой связи. Серверу CMC/контроллеру шлюза, участвующему в сигнализации вызова, поручается выполнить эти проверки, и это единственный объект, которому доверяется создание нового шлюза в системе CMTS. С точки зрения управления QoS CMC/GC действует как сервер политики (PDP – policy decision point).
- Управление ресурсом: Обеспечение того, что использование ресурсов учитывается должным образом в соответствии с соглашениями поставщиков, которые являются частью сети КТСОП, в которой начисление оплаты происходит только после того, как вызываемый участник

снимает трубку. Это включает в себя предотвращение использования зарезервированных ресурсов для целей, отличающихся от сеанса, которому они предназначены. Это достигается путем использования шлюзов и координации между шлюзами, которые связывают вместе механизмы фильтрации адресов с резервированием ресурсов.

Так как на эту услугу может начисляться плата на основе по каждому использованию, то имеется существенный риск обмана и кражи услуги. Архитектура дает возможность поставщику осуществлять начисление оплаты за качество обслуживания. Таким образом, это предотвращает сценарии краж услуг, часть которых описана в Приложении IX.

Сценарии краж услуг указываются в этой Рекомендации и в других Рекомендациях. Они мотивируют некоторые компоненты QoS, а также архитектур и протоколов сигнализации вызова.

5.6.2 Двухфазная фиксация ресурсов

Двухфазный протокол для фиксации ресурса является существенным для коммерческой услуги голосовой связи по двум причинам, которые уникальны по отношению к требованиям, связанным с такой услугой. Первое, он гарантирует, что ресурсы доступны перед тем, как участнику на дальнем конце сообщают о том, что осуществляется входящая связь. Второе, он гарантирует, что запись об использовании и выставление счета не начинаются до тех пор, пока на дальнем конце не снимут трубку, что является также точкой, в которой может быть осуществлена просечка голоса. Эти свойства предоставляются протоколами сигнализации обычной телефонии; с подражанием той же самой семантике. Кроме того, если полоса пропускания распределяется прежде, чем на дальнем конце снимают трубку, то становится возможной кража услуги. Требуя от конечных точек недвусмысленно посылать сообщение фиксации, можно получить гарантию того, что запись об использовании основана на знании конечной точки и ее точного действия.

Эта структура также поддерживает такие объекты, как серверы объявлений и шлюзы сетей КТСОП, которые нуждаются в просечке голоса после первой фазы протокола управления ресурсами.

5.6.3 Присвоение сегментированного ресурса

Динамическая архитектура QoS разделяет управление ресурсами на четкие сегменты сети доступа и магистральной сети. Назначение сегментированных ресурсов является выгодным по двум причинам:

- Оно позволяет иметь разные механизмы обеспечения полос пропускания и сигнализации для исходящей сети, сети дальнего конца и магистральной сети.
- Для сегментов, бедных ресурсами, оно позволяет сохранять резервирование по каждому потоку и осторожно управлять использованием ресурсов. В то же самое время, когда сегменты магистральной сети обладают достаточными ресурсами для более крупного управления, оно позволяет магистральной сети избегать сохранения состояния по каждому потоку и тем самым улучшить масштабируемость.

Когда базовая сеть не требует явной сигнализации по каждому потоку (так, как магистральная услуга Diffserv), это уменьшает время, взятое для установления сеанса (сводит к минимуму задержку после набора номера), и позволяет избежать воздействия на время просечки голоса (свести к минимуму задержку после поднятия трубки).

Это потенциально уменьшает состояние объема резервирования, которое должно быть сохранено, если отдаленным клиентом является шлюз сети КТСОП.

После первой фазы сигнализации вызова оба клиента закончили согласование возможностей и знают, какие необходимы сквозные ресурсы. Клиенты посылают сообщения управления ресурсами, используя интерфейс управляющих служб MAC. CMTS преобразует сообщения управления ресурсами в протокол управления ресурсами, используемый на магистральной сети (например, DiffServ IETF). Он также преобразует сообщение управления ресурсами в протокол управления ресурсами, используемый на звене доступа (т. е. DOCSIS).

5.6.4 Изменения ресурсов во время сеанса

Имеется возможность изменять ресурсы, распределенные для сеанса, в течение существования сеанса. Это облегчает такие изменения в середине сеанса, как переключение из низкоскоростного голосового кодека на кодек G.711, когда обнаруживаются тональные частоты модемов, а также добавление данных видео к сеансу, который начинается только как сеанс для голоса.

5.6.5 Динамическое связывание ресурсов

Динамическое связывание ресурсов (повторное резервирование) является требованием для обеспечения эффективного использования ресурсов, когда вызываются такие услуги, как ожидание вызова. Абстрактно, повторное резервирование берет полосу пропускания, распределенную для сеанса между главным компьютером VoIP и клиентом, и перераспределяет ту же самую полосу пропускания сеансу с другим клиентом.

Важно понять потенциальную опасность в перераспределении полосы пропускания сеанса, создавая затем новый запрос для распределения новой полосы пропускания. Есть риск другого клиента, использующего последнюю остающуюся полосу пропускания между двумя шагами, оставляя исходный сеанс без тракта гарантированного качества. Механизм повторного резервирования с одним шагом избегает этого, поскольку полоса пропускания не становится доступной другим клиентам.

5.6.6 Динамические показатели QoS

Обмен сообщениями QoS имеет место в режиме реального времени, в то время как вызывающие абоненты ожидают услуги, которые должны быть активированы или изменены. Таким образом, протокол должен быть быстрым. Количество сообщений сводится к минимуму, особенно количество сообщений, которые транзитом проходят по магистральной сети, а также количество сообщений восходящего потока DOCSIS.

Сообщения управления DOCSIS и сообщения сигнализации вызовов (все вместе указываемые как сообщения сигнализации) транспортируются по сети DOCSIS на основе наилучшего усилия. Если модем CM также поддерживает услуги передачи данных, то услуга наилучшего усилия может быть не способна обеспечить низкое время ожидания, необходимое для сообщений сигнализации. В этой ситуации модем CM МОЖЕТ быть обеспечен отдельным обслуживающим потоком с улучшенным качеством QoS для переноса трафика сигнализации. Например, обслуживающий поток сигнализации способен использовать службу поллинга в том числе и в реальном времени. Этот отдельный обслуживающий поток обеспечивается в той же самой манере, как другие потоки носителей информации DOCSIS, и МОЖЕТ включать классификаторы так, что их присутствие является прозрачным для адаптера MTA.

5.6.7 Класс сеанса

Ресурсы могут быть зарезервированы для различных типов услуг, и каждая услуга может, в свою очередь, определять для своих сеансов различные классы услуг. Резервирование QoS для сеансов, назначенных поставщиком услуги, что должны иметь более высокий приоритет (например, срочные телефонные вызовы), претерпевает более низкую вероятность блокирования, чем нормальные сеансы. Определение, какой класс сеанса назначать сеансу, выполняется поставщиком услуги и является политикой, которая осуществляется первоначальным комплексом агент вызова/контроллер шлюза во время начального запроса сеанса.

5.6.8 Поддержка промежуточной сети

Архитектуре не следует запрещать промежуточные сети между адаптером MTA или мультимедийным ведущим компьютером и модемом CM (например, сеть клиента). Хотя промежуточная сеть не может подпадать под область или ответственность оператора кабельной сети, распределение полосы пропускания в сети оператора кабельной сети DOCSIS возможно, когда промежуточная сеть существует. Желательно также предоставлять решение, которое прозрачно позволяет резервирование ресурсов на промежуточной сети.

5.6.9 Поддержка качества QoS магистралей

Возможно, что будет необходим некоторый механизм для детально управляемых ресурсов магистралей. Сферой применения этой Рекомендации является качество QoS по сети DOCSIS, но архитектура обеспечивает открытые, достаточно общие интерфейсы, которые совместимы со многими из известных механизмов качества QoS магистралей.

5.6.10 Обработка множественных кодеков

Сигнализация NCS, используемая в проекте IPCablecom, допускает установление соединений с помощью множественных кодеков. В случае, когда соединение успешно согласовано со списком множественных кодеков, важно, чтобы необходимые ресурсы были распределены, чтобы делать

последующие замены кодеков в пределах согласованной работы списка как ожидается. Однако только сервер CMC определяет момент авторизации полосы во время фазы установления вызова; также под управлением CMC оказывается эффективность авторизованного диапазона режимов. В случае выбора авторизации ширины полосы перед начальной командой "Создать соединение" (CRCX) NCS, авторизованный диапазон режимов должен будет основываться на предлагаемых параметрах LCO (поскольку неизвестен поднабор, с которым может быть согласован MTA). Если CMC дождется более позднего момента фазы установления вызова, когда кодеки в дальнейшем будут согласованы, он может затем авторизовать поднабор LCO, основанный на текущем согласованном списке без каких либо отрицательных воздействий (в этот момент авторизация DSA/DSC еще не будет окончена). Ниже перечислены компоненты ресурсов, нуждающиеся в распределении:

– Авторизованная ширина полосы: Когда CMC запрашивает MTA о резервировании или фиксировании ресурсов, включая GateID в команде NCS "Создать соединение" или "Модифицировать соединение" (CRCX или MDCX), CMC ДОЛЖЕН гарантировать, что авторизованная ширина полосы в шлюзе обработает любой допустимый запрос ресурса (DSA/DSC) от MTA к CMTS, который является результатом процедуры согласования с кодеками. Иначе говоря, ширина полосы, авторизованная CMC/GC, ДОЛЖНА превышать наименьшую верхнюю границу (LUB) согласованного списка кодеков или быть равной ей.

– Зарезервированная ширина полосы: MTA ДОЛЖЕН зарезервировать наименьшую верхнюю границу (LUB) для полосы кодека, который может использоваться во время вызова (возможные кодеки определяются из процедуры согласования кодеков, описанной в 6.7/J.162).

  ПРИМЕЧАНИЕ. – Если зарезервированная полоса больше зафиксированной, то зарезервированная полоса должна быть обновлена с использованием сообщений DSC к CMTS.

– Фиксированная ширина полосы: MTA ДОЛЖЕН просто зафиксировать текущий используемый кодек в восходящем направлении. Это позволяет использовать избыточную неиспользуемую ширину полосы (разницу между зарезервированной и зафиксированной) для максимальных объемов трафика. В нисходящем направлении, MTA ДОЛЖЕН зафиксировать наименьшую верхнюю границу (LUB) полосы кодека, который может быть использован во время вызова (возможные кодеки определяются из процедуры согласования кодеков, описанной в 6.7/J.162).

Эта процедура гарантирует, что запрос CMC для коммутации любого из кодеков, входящих в согласованный список, будет успешным. Это особенно важно при поддержке таких возможностей, как факс/модем, когда для успешной передачи требуется подключение к G.711.

Если системному поставщику услуг кажется, что описанное выше распределение ресурсов накладывает слишком большие ограничения на количество поддерживаемых голосовых каналов (т. к. во многих случаях ресурсы резервируются с запасом), тогда в LocalConnectionOptions для запроса соединения серверу CMC необходимо установить единственный кодек. Это обеспечит равенство зарезервированных и фиксированных ресурсов (используя тот же механизм, что и в случае множественных кодеков). Тогда, если CMC захочет переключить кодеки, серверу потребуется поместить новый кодек в LocalConnectionOptions для модифицируемого впоследствии соединения. Однако, при таком подходе существуют определенные опасности. Например, когда определен вызов модема и сообщение о нем передано серверу CMC, существует возможность неудачи установления результативной модифицирующей связи, использующей G.711 из-за недостатка ресурсов системы завершения CMTS. Этого не случится, если множественные кодеки уже определены благодаря тому, что LUB уже зарезервирована и гарантированно доступна для последующей фиксации.

5.6.11 Вызовы MTA от порта к порту

Когда устанавливаются голосовые вызовы между различными портами (конечными пунктами) в пределах MTA, правила перенаправления DOCSIS, определяют, что модем CM не должен перенаправлять пакеты по сети DOCSIS. В результате, действия CMC и MTA в этих особых обстоятельствах отличаются от типичного потока вызова между двумя MTA. Вызов от порта к порту определяется обоими конечными пунктами, использующими один и тот же адрес IP.

Если MTA получает запрос соединения без ID шлюза, он НЕ ДОЛЖЕН инициировать никаких сообщений DSx на терминалы CMTS. Если MTA получил инструкции по вызову запроса от порта к порту, MTA НЕ ДОЛЖЕН инициировать никаких DSx-сообщений для установления

обслуживающего потока для этого соединения и НЕ ДОЛЖЕН посылать по сети ни одного пакета голосовой связи. Вдобавок, если MTA уже создал обслуживающий поток для вызова, где SDP дальнего конца был недоступен (но ID шлюза был точно определен в командах CRCX или MDCX), то MTA ДОЛЖЕН разорвать обслуживающий поток после того, как получен протокол SDP и опознан вызов от порта к порту.

Сервер CMC ДОЛЖЕН распознавать вызовы от порта к порту и ДОЛЖЕН оставить управление шлюзом CMTS и ДОЛЖЕН игнорировать ID шлюза в команде соединения с MTA. Аналогично MTA, если CMC уже установлен шлюз для вызова с недоступным удаленным SDP, он ДОЛЖЕН ожидать сообщения "Шлюз Закрыт" от CMTS, как только MTA, разорвет обслуживающий поток после опознания вызова от порта к порту. CMC НЕ ДОЛЖЕН разрывать вызов между конечными пунктами с одним и тем же адресом IP после получения сообщения "Шлюз Закрыт".

5.6.12 Множество разрешений за интервал

Для эффективного использования ресурсов сети DOCSIS, MTA МОЖЕТ выбрать размещение множественных подпотоков с одинаковыми наборами параметров QoS на одном и том же обслуживающем потоке. Поскольку тип "Планирование обслуживающего потока" является частью набора параметров QoS, он ДОЛЖЕН быть общим для всех подпотоков, использующих один и тот же обслуживающий канал в сети DOCSIS. Например, если поток, поддерживающий подавление пауз, использует UGS/AD, а существующий поток сконфигурирован только под UGS, новый поток ДОЛЖЕН быть создан на отдельном обслуживающем канале. Для облегчения исполнения при использовании множественных разрешений за интервал существующий тип планирования обслуживающего потока не может быть изменен.

Для MTA поддержка данной особенности является необязательной. Система терминалов CMTS ДОЛЖНА поддерживать более чем 1 разрешение за интервал. Если MTA запрашивает множественные разрешения за интервал, а сообщение DSx отвергнуто CMTS (т. е. планировщик CMTS не может спланировать этот запрос должным образом для отдельного обслуживающего потока), MTA МОЖЕТ повторить попытку, используя отдельный обслуживающий поток для запроса (если позволяют ресурсы).

Поле активных разрешений за интервал в расширенном заголовке MAC используется для сохранения дорожки активных разрешений на отдельном обслуживающем канале, содержащем множество подканалов. Например, если у вас есть два активных вызова и один из них подвергается подавлению пауз, то количество активных разрешений в расширенном заголовке MAC уменьшается с 2 до 1. При таком развитии событий не требуется обновления DSC для потока, поскольку регистрация активности основывается на потоке а не на разрешении. Количество разрешений за интервал для DSC остается равным 2 для "принятых" и "активных", и обновление потока потребуется только при равенстве 0 числа активных разрешений для всех подпотоков подвергающихся подавлению пауз. Количество активных разрешений за интервал должно быть не больше числа подпотоков. Правила подавления заголовка полезной нагрузки (PHS) для всех подпотоков обслуживающего потока ДОЛЖНЫ быть одинаковыми.

5.7 Теория функционирования

5.7.1 Установка основного соединения

Резервирование ресурсов разделяется на отдельные фазы Reserve [резервировать] и Commit [фиксировать]. В конце первой фазы ресурсы резервируются, но еще не доступны адаптеру MTA. (В соединениях сети DOCSIS допускаются обслуживающие потоки в каждом направлении). В конце второй фазы ресурсы делаются доступными адаптеру MTA, и регистрация использования начинается так, чтобы пользователю можно было начислить плату за использование. (В соединениях сети DOCSIS обслуживающие потоки являются активными).

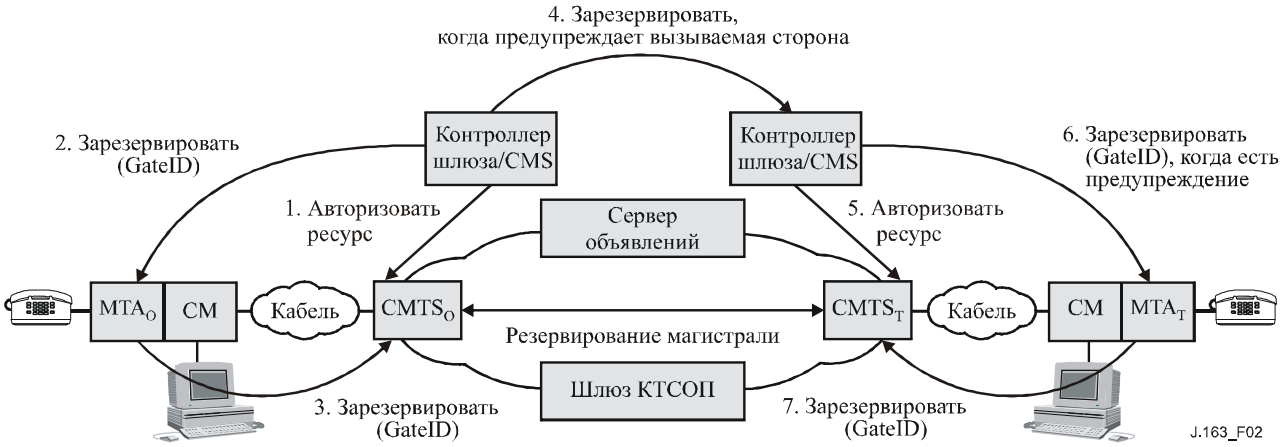


Рисунок 2/J.163 – Фаза 1 управления ресурсами

На рисунке 2 показана первая фаза протокола управления ресурсами для вызова. В этом описании нижние индексы "O" и "T" определяют исходящие и завершающие точки вызова. Как показано на рисунке 2, адаптеры MTA_O и MTA_T запрашивают соответственно у $CMTS_O$ и $CMTS_T$ резервирование ресурсов динамических служб сигнализации сети DOCSIS для встроенных клиентов. $CMTS_O$ и $CMTS_T$ выполняют проверку управления доступом на готовность ресурсов (если необходимо, положив начало сигнализации для резервирования ресурсов в магистральной сети) и посылают ответ на соответствующие адаптеры MTA, которые в свою очередь отвечают серверу CMC.

На рисунке 3 показана вторая фаза. После определения, что ресурсы являются доступными, сервер CMC посылает сообщение к адаптеру MTA_T, давая ему инструкцию дать начало звонку телефона. Когда вызываемый участник снимает телефонную трубку, адаптер MTA_T посылает сообщение на CMC, а CMC дает инструкции MTA_O и MTA_T послать запрос о фиксировании ресурсов. Прибытие сообщений COMMIT на $CMTS_O$ и $CMTS_T$ заставляет их открывать свои шлюзы, а также вести учет использования ресурсов. Чтобы предотвратить некоторые сценарии кражи услуг, каждое система CMTS информирует соответствующий CMC об изменении состояния, посылая сообщение "Шлюз открыт".

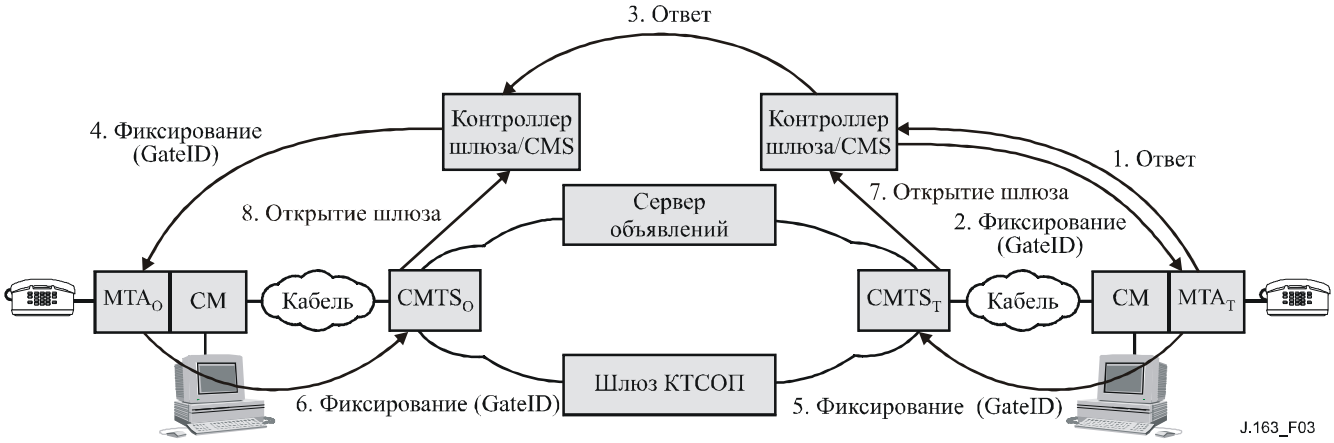


Рисунок 3/J.163 – Фаза 2 управления ресурсами

5.7.2 Координация шлюзов

Сигнализация QoS приводит к созданию шлюза в каждом терминале CMTS, связанном с клиентом, который участвует в сеансе. Каждый шлюз поддерживает данные использования для сеанса и контролирует, получают ли пакеты, произведенные связанным клиентом, доступ к расширенному качеству QoS. Координация шлюзов необходима, чтобы предотвратить мошенничество и кражу услуги в ситуациях, где неисправно работающий или модифицированный клиент не выпускает ожидаемые сообщения сигнализации. Существенно, что механизмы протокола являются устойчивыми против злоупотребления[2]. Протокол координации шлюза гарантирует, что:

- Устраняется возможность для одностороннего установления сеанса без выписывания счетов. Поскольку клиенты могут иметь соответствующие сведения и им не доверяют, можно предвидеть клиентов, устанавливающих два односторонних сеанса, чтобы обеспечить пользователей соответствующим диалоговым каналом голосовой связи. Координация шлюзов предотвращает такие сеансы, устанавливаемые без возможности тарифицировать их поставщиком.
- Открытие и закрытие каждого шлюза тесно синхронизированы с соответствующими изменениями состояния дляCMC.

5.7.3 Изменение пакетных классификаторов, связанных со шлюзом

Как только пара шлюзов установлена, клиенты могут осуществлять связь по сети с улучшенным качеством QoS. Несколько особенностей, необходимых для коммерческой услуги голосовой связи, включают в себя изменение клиентов, вовлеченных в сеанс, например, когда сеанс переносится или переадресовывается либо во время вызова с тремя участниками. Это требует, чтобы пакетные классификаторы, связанные со шлюзом, были изменены, чтобы отразить адрес нового клиента. Кроме того, изменение конечных точек, вовлеченных в сеанс, может затронуть аспект начисления оплаты за сеанс. В результате этого шлюз включает информацию адресации для исходящей и завершающей точек.

5.7.4 Ресурсы сеанса

Взаимоотношения между различными категориями ресурсов, авторизованных, зарезервированных и зафиксированных, показаны на рисунке 4. Набор ресурсов представлен *n*-размерным пространством (показанным здесь как двухмерное), где *n* – число параметров (например, полоса пропускания, размер пакета, фазовые дрожания, классификаторы), необходимых для описания ресурсов. Точные процедуры для сравнения *n*-размерных векторов ресурсов даются в Рекомендации МСЭ-Т J.112.

Когда сеанс устанавливается впервые, протоколы DQoS авторизуют использование некоторого максимального количества ресурсов, обозначенных внешним овалом, определяя разрешенные ресурсы. Когда клиент осуществляет резервирование для сеанса, то он резервирует некоторое количество ресурсов, которое не больше, чем то, что было авторизовано. Когда сеанс готов для продолжения, клиент фиксирует некоторое количество ресурсов, которое не больше зарезервированных ресурсов. Во многих общих случаях зафиксированные и зарезервированные ресурсы будут равными. Зафиксированные ресурсы представляют ресурсы, которые используются активным сеансом в настоящее время, тогда как зарезервированные ресурсы представляют те ресурсы, которые связаны с клиентом, и были удалены из объединения ресурсов для целей управления доступом, но которые необязательно используются клиентом.

---

[2] Несколько сценариев кражи услуг описываются в Дополнении IX.

Рисунок 4/J.163 – Авторизованные, зарезервированные и зафиксированные ресурсы

Авторизация затрагивает только будущие запросы на резервирование ресурсов. Ресурсы, которые были зарезервированы до изменения авторизации, не затрагиваются.

Ресурсы, которые были зарезервированы, но не зафиксированы, доступны системе только для таких краткосрочных применений, как обработка данных наилучшего усилия. Эти ресурсы не доступны для другого резервирования (т. е. избыточное бронирование ресурсов не разрешается). Максимальная часть доступных ресурсов, которые могут быть зарезервированы сразу, является решением политики CMTS и выходит за рамки DQoS.

Дополнительные ресурсы, зарезервированные выше тех, что были зафиксированы, освобождаются, если клиент явно не запрашивает, чтобы путем операций обновления резервирования они были сохранены. Поддержанию такого состояния в течение долгих периодов времени препятствуют, поскольку это уменьшает полную пропускную способность системы. Однако есть ситуации (например, услуга ожидания вызова, где вызов на удержании требует ресурсы за пределами тех, что нужны для активного вызова), где дополнительные резервирования необходимы.

5.7.5 Управление доступом и классы сеансов

Предусматривается, что шлюз в системе завершения CMTS может использовать один или более классов сеансов для ресурсов, зарезервированных от адаптера MTA. Классы сеанса определяют политику обеспеченного управления доступом, или их параметры. Ожидается, что поставщик предоставил бы необходимые параметры и/или альтернативные политики по управлению доступом в CMTS и в контроллере шлюза. Например, мог быть определен класс сеанса для осуществления нормальной голосовой связи и класс перекрывающегося сеанса для срочных телефонных вызовов, чтобы позволить, соответственно, распределение до 50% и 70% совокупных ресурсов этим классам вызовов, и оставляя остаток 30–50% общей полосы пропускания, доступной другим услугам, возможно, с низким приоритетом. Более того, классы сеансов могут позволить выгрузку уже зарезервированных ресурсов, когда политика для такой выгрузки была бы предоставлена поставщиком услуги. Когда авторизованный диапазон режимов передается шлюзу CMTS с помощью контроллера шлюза в сообщении Gate-Set, контроллер шлюза включает соответствующую информацию, чтобы указать, какой класс сеанса следует применять, когда обрабатывается соответствующий запрос DSA/DSC.

5.7.6 Повторное согласование ресурсов

Несколько особенностей поддерживаемых сеансов требуют пересмотра параметров QoS, связанных с сеансом, в течение всей продолжительности сеанса. Например, клиенты могли бы начать осуществлять связь с использованием низкоскоростного кодека аудио. Они могут впоследствии переключиться на более высокоскоростной кодек или добавить поток видео, пока требуемое качество QoS находится в пределах авторизованной ширины полосы, а в сети есть доступная полоса пропускания. Использование диапазона режимов авторизованного QoS, который был предварительно авторизован контроллером шлюза, действующим в качестве точки решения политики, дает клиентам гибкость в повторном согласовании качества QoS с сетью, не требуя последующего привлечения контроллера шлюза. Это по существу означает, что использование ресурсов вплоть до пределов диапазона режимов является предварительно авторизованным, но НЕ предварительно зарезервированным. Успешное распределение ресурсов в пределах авторизованного диапазона режимов требует решения по управлению допуском и не гарантируется. Последующим за управлением допуском резервируются ресурсы для потока, хотя фактическое использование ресурсов разрешается только после того, как завершается фаза Commit [зафиксировать] протокола

резервирования ресурсов. Однако во время фиксации ресурсов никакое решение по управлению допуском не требуется. Каждое изменение в фиксации ресурсов внутри пределов решения об управлении допуск не требует дальнейшего резервирования. Все запросы на резервирование, которые проходят управление допуском, ДОЛЖНЫ помещаться внутри диапазона режимов авторизации.

5.7.7 Динамическое связывание ресурсов (повторное резервирование)

Архитектура динамического качества QoS признает, что может быть потребность совместно использовать ресурсы через многократные сеансы, особенно тогда, когда ресурсы ограничены. В частности, при использовании функции "ожидание вызова" в приложениях, подобных телефонии, клиент может быть вовлечен в два одновременных сеанса, но в данный момент времени будет активен только в одном разговоре. В этом случае является реальным совместно использовать ресурсы сетевого уровня (в частности, на звене доступа) между этими двумя разговорами. Поэтому эта архитектура позволяет точно определять набор ресурсов сетевого уровня (типа резервирования полосы пропускания) и позволяет одному шлюзу или более связываться с такими ресурсами. Примитивы сигнализации позволяют совместно использовать ресурсы, связанные со шлюзами, с другими шлюзами в том же самом CMTS. Это улучшает эффективность, с которой в сети DOCSIS используются ресурсы.

При переключении назад и вперед между двумя сеансами в сценарии ожидания вызова клиент должен держать достаточное количество зарезервированных ресурсов, чтобы приспособиться к любому из сеансов, которые в общем случае могут не нуждаться в том же самом количестве ресурсов. Таким образом, операция повторной фиксации может изменить зафиксированные ресурсы. Однако зарезервированные ресурсы в этом случае не изменяются, поскольку клиенту не придется проходить через управление доступом при обратном переключении на другой сеанс.

Принимая во внимание, что зафиксированные ресурсы всегда связываются с текущим активным сеансом (и с его соответствующим потоком IP), резервируемые ресурсы могут быть в разное время связаны с различными потоками и с различными шлюзами. Чтобы определять набор зарезервированных ресурсов привязки потока к таким ресурсам, используется дескриптор, называемый ресурсом ID.

5.7.8 Поддержка выписки счетов

Сигнализация QoS может использоваться для поддержки широкого диапазона моделей выписки счетов, основанных только на потоке записей событий от системы CMTS. Так как шлюз находится в тракте передачи данных и поскольку он участвует во взаимодействиях управления ресурсами с клиентом, ведение учета использования ресурсов осуществляется шлюзом. Шлюз в CMTS является соответствующим местом для осуществления ведения учета ресурсов, поскольку система завершения CMTS непосредственно вовлечена в управление ресурсами, предоставляемыми клиенту. Также важно осуществлять учет использования в CMTS, чтобы справляться с ошибками клиента. Если клиент, который вовлечен в активный сеанс, терпит неудачу, то терминал CMTS ДОЛЖЕН обнаружить это и остановить для сеанса учет использования. Это может быть достигнуто, контролируя поток пакетов по тракту передачи данных для приложений с непрерывными носителями информации, или другими механизмами (типа технического обслуживания станции), выполняемого с помощью терминала CMTS. Кроме того, поскольку шлюз сохраняет состояние для потоков, которые были авторизованы контроллером, характерным для услуги, это используется, чтобы удерживать такую информацию, характерную для услуги, относящуюся к тарификации, как расчетный счет абонента, который будет оплачивать сеанс. Функция политики в контроллере шлюза тем самым становится не имеющей состояния.

Поддержка, требуемая в CMTS, состоит в порождении и передаче сообщения о событии к серверу хранения записей на каждое изменение для QoS, как авторизовано и определено шлюзом. Непрозрачные данные, предусматриваемые контроллером шлюза, которые могут быть уместны для сервера хранения записей, также могут быть включены в сообщение. Требования для обработки записей о событиях содержатся в других спецификациях Поддержки операций.

5.7.9 Управление магистральным ресурсом

Когда терминал CMTS получает сообщение резервирования ресурсов от адаптера MTA, он сначала проверяет, что соответствующая полоса пропускания восходящего и нисходящего потоков доступна по каналу доступа, используя информацию планирования, доступную локальным образом. Если эта проверка является успешной, то система CMTS может либо породить новое сообщение резервирования магистральных ресурсов, либо отправить к магистральной сети измененную версию

сообщения о резервировании ресурсов, полученного от адаптера MTA. CMTS выполняет любое характерное для технологии магистральной сети преобразование для резервирования ресурсов, которое необходимо. Это позволяет архитектуре приспосабливать различные технологии магистральной сети при выборе поставщика услуги. Конкретные механизмы для резервирования магистрального качества QoS выходят за рамки этой Рекомендации.

В сети DOCSIS, где маршрутизация является симметричной, для резервирования ресурсов используется двунаправленная модель. Однонаправленная модель используется для резервирования ресурсов в магистральной сети, которая позволяет асимметрию маршрутизации. Таким образом, когда адаптер MTA_O осуществляет резервирование с помощью CMTS, то он знает две вещи: что он имеет соответствующую полосу пропускания в обоих потоках по сети DOCSIS, и что он имеет соответствующую полосу пропускания по магистральным сетям для потока от адаптера MTA_O к адаптеру MTA_T. Таким образом, адаптер MTA_O знает, что доступны сквозные ресурсы в обоих потоках, когда он получает ответ от адаптера MTA_T.

5.7.10 Установка кодовой точки DiffServ

Эта архитектура также учитывает использование магистральной сети дифференцированных услуг, где имеется соответствующая полоса пропускания, чтобы осуществлять перенос голосовых диалогов, но доступ к этой полосе пропускания находится на управляемой основе. Доступ к полосе пропускания и дифференцированной обработке обеспечивается для пакетов с соответствующими кодированными битами в поле заголовка IP, указанного для дифференцированных услуг. Это называют кодовой точкой DiffServ (DSCP, DiffServ code point). Поле DS поддерживает обратную совместимость с существующими случаями использования битов Precedence [приоритет] IP в байте IPv4 TOS (RFC 2474 IETF). Желательно обладать способностью устанавливать кодовую точку пакетов DiffServ, которые собираются входить в магистральную сеть поставщика от системы завершения CMTS. Так как ресурсы, использованные этими пакетами в магистральной сети, могут в сильной степени зависеть от этой маркировки, то эта архитектура обеспечивает управление маркировкой к сетевым объектам. Это позволяет сети и поставщику услуги осуществлять управление использованием улучшенного качества QoS вместо того, чтобы доверять это адаптеру MTA. Поставщик услуги может формировать политики в CMTS, которые решают, как установить точку DSCP для потоков, которые проходят через CMTS. Такие политики посылаются к терминалу CMTS в протоколе установки шлюза от модема CM/контроллера GC.

Для эффективности выполнения пересылают информацию к адаптеру MTA о соответствующей для этого точке DSCP, чтобы использовать ее в данном сеансе. Система CMTS все еще нуждается в наблюдении за полученными пакетами, чтобы гарантировать, что используется правильная точка DSCP и что объем пакетов в данном классе находится в пределах авторизованных границ.

5.8 Типовое отображение описаний SDP в flowspecs RSVP

Сообщения протокола дескриптора сеанса используются для описания мультимедийных сеансов в целях объявления сеанса, приглашения к сеансу и других форм мультимедийного инициирования сеанса согласно документу RFC 2327 IETF. Это приложение описывает механизм для преобразования описания SDP в сочетания flowSpecs RSVP.

Типичное описание SDP содержит много полей, которые имеют в своем составе информацию относительно описания сеанса (версия протокола, название сеанса, линии атрибута сеанса и т. д.), описание времени (время, когда сеанс является активным и т. д.), а также описание носителей информации (название и транспорт носителей информации, название носителей информации, информация о соединении, линии атрибута носителя информации и т. д.). Двумя критическими компонентами для преобразования описания SDP в сообщение FlowSpec RSVP являются название носителей информации и транспортный адрес (m), а также линии атрибута носителей информации (a).

Название носителя информации и транспортный адрес (m) имеют форму:

m = <media> [носитель информации] <port> [порт] <transport> [транспорт] <fmt list> [перечень]

Линия (линии) (a) атрибута носителя информации имеет форму (a):

a = <token>[маркер]:<value>[значение]

Типовая голосовая связь IP имела бы следующую форму:

m = аудио 3456 RTP/AVP 0
a = ptime: 10

На линии транспортного адреса (m) первый член определяет тип носителя информации, которым в случае голосового сеанса IP является аудио. Второй член определяет порт UDP, к которому посылается носитель информации (порт 3456). Третий член указывает, что этот поток представляет собой профиль аудио/видео RTP. Наконец, последний член является типом полезной нагрузки носителя информации, как определено в профиле аудио/видео RTP (ссылка на документ RFC 3551 IETF). В этом случае 0 представляет статический тип полезной нагрузки аудио единственного канала ИКМ, кодированного по μ-закону, который дискретизируется с частотой 8 кГц. На линии атрибута носителя информации (a) первый член определяет время формирования пакета (10 мс).

Другие типы полезной нагрузки, кроме тех, что определены в документе RFC 1890 IETF, динамически ограничены путем использования динамического типа полезной нагрузки из диапазона 96-127, как определено в документе RFC 2327 IETF, и линии атрибута носителя информации. Например, типичное сообщение SDP для G.726 было бы составлено следующим образом:

m = аудио 3456 RTP/AVP 96

a = rtpmap:96 G726-32/8000

Тип полезной нагрузки 96 указывает, что локальным образом тип полезной нагрузки определяется для продолжительности этого сеанса, а следующая строка указывает, что тип 96 полезной нагрузки привязан к кодированию "G726-32" с тактовой скоростью 8000 отсчетов в секунду. Для каждого определенного КОДЕКА (представлен ли он в SDP как тип статической или динамической полезной нагрузки) нужно иметь табличное преобразование из любого типа полезной нагрузки или представление строки ASCII в требования полосы пропускания для такого КОДЕКА.

Для редко употребляемых кодеков требования полосы пропускания не могут быть определены с помощью адреса названия носителя информации и транспорта (m) и атрибута носителя информации

a) только линии. В этой ситуации SDP ДОЛЖЕН использовать параметр полосы пропускания;

b) линия для определения требований SDP к полосе пропускания для неизвестного кодека. Параметр линии полосы пропускания (b) имеет форму:

b = <модификатор>:<значение полосы пропускания>

Например:

b = AS:99

Данный параметр полосы пропускания вместе с атрибутом носителя информации ДОЛЖЕН использоваться для преобразования SDP в сочетания Флоспек, которые будут использоваться в решении авторизации политики и последующем выделении шлюза.

ПРИМЕЧАНИЕ. – Решением политики для CMC/ CMTS является принятие SDP запрашиваемой полосы пропускания или отказ от нее.

Параметр полосы пропускания (b) включает необходимый предзаголовок полосы пропускания для заголовков IP/UDP/RTP. Вдобавок, любые PHS используемые в связях DOCSIS никак не указываются в запрашиваемой ширине полосы. В том особом случае, когда многократные кодеки определены в SDP, параметр полосы пропускания должен содержать максимальное количество желаемых полос пропускания кодека.

Преобразование кода RTP/AVP в сочетания Флоспек происходит согласно таблице 2/J/161.

6 Протокол QoS для встроенного адаптера MTA – модема CM (pkt-q1)

Система CMTS ДОЛЖНА поддерживать интерфейс DOCSIS MAC таким образом, как это описано в данном разделе. Встроенный адаптер MTA ДОЛЖЕН использовать механизмы , описанные в данном разделе для динамического резервирования локальных ресурсов QoS.

Используя данный подход, встроенный MTA непосредственно сигнализирует локальной QoS доступа, используя интерфейс управляющей службы MAC, определенный в Рекомендации DOCSIS RFI (Рекомендации МСЭ-Т J.112 и J.122). Встроенный MTA сигнализирует об уровне требований QoS своего сеанса с помощью протоколов сигнализации (DCS и NCS). Как только встроенный MTA определяет, что ресурсы QoS нуждаются в резервировании или фиксации, адаптер MTA ДОЛЖЕН инициировать сигнализацию динамического потока услуг DOCSIS, чтобы вызвать создание, изменение и/или удаление потока (потоков) услуг и перераспределение ресурсов DOCSIS. Независимо от того, вызван ли сеанс связи равноправным объектом или узлом сети, MTA пересылает

требования QoS к MAC DOCSIS через интерфейс услуги управления MAC. Это приводит к созданию или модификации необходимого потока (потоков) услуг на время сеанса, используя сообщения динамического потока услуг DOCSIS. В последующих разделах обсуждается преобразование MTA требований QoS уровня сеанса в DOCSIS, поддержка DOCSIS двухфазного резервирования/фиксации и использование интерфейса услуги управления MAC DOCSIS.

6.1 Сочетание FlowSpecs протокола RSVP

Архитектура интегрированных услуг IETF использует описания общей цели (не зависящие от уровня 2) из характеристик трафика и требований ресурсов потока. Описание трафика известно как Spec, требования ресурса содержатся в RSpec, а их сочетание известно как FlowSpec. Чтобы зарезервировать ресурсы на таком определенном носителе информации уровня 2, как сеть DOCSIS, необходимо определить преобразование из сочетания FlowSpec, не зависящего от уровня 2, в характерные параметры уровня 2. Преобразования для множества других технологий (ATM, 802.3 ЛВС и пр.) уже были определены.

Другие спецификации (например, спецификация Рекомендации МСЭ-Т J.161 CODEC IPCablecom) содержат требования по преобразованию в сочетание FlowSpecs описаний услуг верхних уровней (например, SDP, как используется в приложениях VoIP). В этом разделе определено, как CMTS и адаптер MTA ДОЛЖНЫ преобразовывать сочетания FlowSpecs в параметры уровня 2 DOCSIS.

Интегрированные услуги в настоящее время определяют два типа услуг: с управляемой нагрузкой и с гарантированной нагрузкой, при этом последняя услуга является более подходящей для приложений, чувствительных к задержке. При осуществлении резервирования для гарантированной услуги сочетание FlowSpec содержит:

TSpec

- глубина области памяти (b) – байты
- скорость области памяти (r) – байты/секунда
- пиковая скорость (p) – байты/секунда
- минимальный наблюдаемый элемент (m) – байты
- максимальный размер дейтаграммы (M) – байты

RSpec

- зарезервированная скорость (R) – байты/секунда
- пассивный член (S) – микросекунды

Члены TSpec являются по большей части очевидными. Члены (r, b) определяют маркерную область памяти, которой соответствует трафик, p – пиковая скорость, на которой источник будет передавать, и M – это максимальный размер пакета (включая заголовок IP и заголовки более высоких уровней), который будет произведен источником. Минимальный наблюдаемый элемент m – это обычно наименьший размер пакета, который произведет источник; если источник посылает меньший пакет, то для целей наблюдения он будет считаться как пакет размером m.

Чтобы понимать значение RSpec, полезно понять, как вычисляется задержка в конфигурации интегрированных услуг. Максимальная сквозная задержка, ощущаемая гарантированной услугой получения пакета, равна:

$$\text{Задержка} = b/R + C_{tot}/R + D_{tot},$$

где b и R определены выше, а C_{tot} и D_{tot} являются накопленными "ошибочными членами", обеспечиваемыми сетевыми элементами вдоль по тракту, которые описывают их отклонение от "идеального" поведения.

Скорость R, предоставляемая в RSpec, является суммой полосы пропускания, распределенной потоку. Она ДОЛЖНА быть больше или равна r из описания TSpec для вышеуказанной задержки, которой нужно придерживаться. Таким образом, предел задержки потока полностью определяется выбором R; причиной использовать значение R больше, чем r, было бы желание уменьшить задержку, испытываемую потоком.

Поскольку не разрешается устанавливать R < r, то узел, осуществляющий резервирование, может выполнить вышеуказанные вычисления и определить, что предел задержки является более строгим, чем нужно. В таком случае узел может установить R = r и установить S в ненулевое значение. Значение S следует выбрать так, что:

$$\text{Желаемый предел задержки} = S + b/R + C_{tot}/R + D_{tot}.$$

Гарантированная услуга не стремится ограничить дрожание больше, чем подразумевается пределом задержки. Вообще, минимальная задержка, которую пакет мог бы ощущать, является задержкой скорости света, а максимумом является предел задержки, приведенный выше; максимальное дрожание представляют разность между этими двумя величинами. Таким образом, дрожанием можно управлять путем подходящего выбора R и S.

6.1.1 Сложные описания SDP с помощью множественных кодеков

Есть различные ситуации, в которых резервирование должно охватывать диапазон возможного сочетания FlowSpecs. Например, для некоторых приложений желательно создать резервирование, которое может управлять переключением от одного кодека на другой в середине сеанса, не проходя по времени через управление доступом в каждом переключателе.

Описание TSpec со стороны отправителя ДОЛЖНО содержать наименьшую верхнюю границу (LUB) необходимых параметров потока для составного потока.

Наименьшая верхняя граница потоков с двумя различными планируемыми типами, планируемыми DOCSIS, не допускается.

Наименьшая верхняя граница (LUB) двух потоков A и B, LUB(A, B) является "наименьшим" диапазоном режимов, который мог бы транспортировать оба этих потока A и B не одновременно. LUB (A, B) вычисляется на основе параметр – к параметру следующим образом.

Определим значения TSpec для потока α так же, как в пункте 6. Определим еще период Pα как Mα/rα. Тогда LUB(A, B) дается выражением:

LUB(A, B) ≡ { bLUB(A, B) ≡ MAX(bA, bB),

r LUB(A, B) ≡ (M LUB(A, B)/P LUB(A, B)),

p LUB(A, B) ≡ MAX(pA, pB, r LUB(A, B)),

m LUB(A, B) ≡ MAX(mA, mB),

M LUB(A, B) ≡ MAX(MA, MB)

},

где:

p LUB(A, B) ≡ GCF(PA, PB);

функция MAX(x, y) означаеts " возьмите наибольшее из двух значений (x, y)";

функция MAX(x, y, z) ≡ MAX(MAX(x, y), z);

функция GCF(x, y) означает "Возьмите наибольший общий множитель пары (x, y)".

LUB n потоков (n ≠ 2), LUB(n1, n2, ...), определяется рекурсивно, как:

$$\text{LUB}(n1, n2, ..., N) \equiv \text{LUB}(n1, \text{LUB}(n2, ..., N)).$$

Более того, пассивный член соответствующего выражения RSpec позволяет использовать ресурсы составляющему потоку. Для того, чтобы удовлетворить этому условию, RSpec для потока принимается равным минимальному значению RSpec для составляющих потоков. То есть:

$$\text{SLUB}(A, B) \equiv \text{MIN}(SA, SB),$$

где функция MIN(x, y) означает "возьмите наименьшее значение из пары (x, y)".

Следующий пример показывает, как параметры TSpec определяются, используя определенный выше алгоритм LUB:

1) Как результат согласования кодека, для вызова выбираются следующие кодеки:
G711(20 мс) и G728(10 мс)

2) Глубина области памяти для LUB для выбранных кодеков составляет:
G711(20 мс) = (8000/50) + 40 = 200 байтов
G728(10 мс) = (2000/100) + 40 = 60 байтов
b[LUB] = m[LUB] = M[LUB] = MAX(200, 60) = 200 байтов

3) Скорость области памяти LUB для выбранных кодеков равна:
P [LUB] = GCF(10 мс, 20 мс) = 10 мс = 0,01 секунды
r[LUB] = M × 1/P = 200 × 1/0,01 = 20 000 байтов в секунду
r[G711(20мс)] = 200 × 1/0,02 = 10 000 байтов в секунду
r[G728(10мс)] = 60 × 1/0,01 = 6000 байтов в секунду
p[LUB] = MAX(10000, 6000, 20000) = 20 000 байтов в секунду

6.1.2 Преобразование сообщений Flowspecs RSVP в параметры QoS DOCSIS

Терминал CMTS, получив запрос о резервировании, ДОЛЖЕН использовать следующие алгоритмы при преобразовании сообщений FlowSpecs RSVP в параметры QoS DOCSIS

Адаптер MTA ДОЛЖЕН использовать требования, определенные в следующем пункте для преобразования требований QoS уровня сеанса в параметры QoS DOCSIS.

В качестве дополнения к этим требованиям встроенные адаптеры MTA ДОЛЖНЫ включать собственные адреса отправителя (т. е. источника в восходящем направлении) и получателя (т. е. получателя в нисходящем направлении и портов во всех величинах классификатора TLV, получаемых в сообщениях DSx. Адреса дальнего конца и принимающие порты МОГУТ быть трафаретными символами, если не получен порт SDP и значения по LCO. Если эти значения получены в каком-либо формате, они ДОЛЖНЫ быть включены в значения TLV классификатора. Порты источника дальнего конца ДОЛЖНЫ в любом случае быть трафаретными символами, поскольку этот параметр не передается через SDP.

Необходимо заметить, что примеры, приведенные в данной главке, включают предзаголовок, связанный с расширенным заголовком BPI+ сети DOCSIS, как предписано в Рекомендации по безопасности (Рекомендация МСЭ-Т J.170). Если BPI+ отключен (напр., для тестирования), значения, приведенные в этих примерах, необходимо обновить надлежащим образом, вычтя пять байтов из заголовка уровня связи из расчета Размера разрешения для восходящего потока.

6.1.2.1 Кодирование качества обслуживания восходящего потока

Объекты восходящего потока DOCSIS должны быть установлены, как указано ниже. Все другие кодировки TLV для потока услуг QoS НЕ ДОЛЖНЫ определяться, позволяя, таким образом, использовать значения по умолчанию. Если MTA позволяет получить одно из установленных значений TLV, тогда CMTS ДОЛЖЕН отвергнуть запрос, выдав код ошибки "reject permanent/reject admin".

Значение таймера *Активный таймаут DOCSIS* используется для установления неактивности и инициирования восстановления ресурсов для зафиксированных потоков услуг. Синхронизация MTA/CMTS может координироваться CMTS путем передачи соответствующего значения в сообщении REQ/RSP DSA/DSC. Это поле НЕ ДОЛЖНО быть занято MTA.

Значение таймера *Допустимый таймаут DOCSIS* используется для установления неактивности и инициирования восстановления ресурсов для зарезервированных потоков услуг. Синхронизация MTA/CMTS может координироваться CMTS путем передачи соответствующего значения в сообщении REQ/RSP DSA/DSC. Это поле НЕ ДОЛЖНО быть занято MTA.

Параметр размер пакета в *Минимальных принимаемых DOCSIS* границах НЕ ДОЛЖЕН устанавливаться для восходящего потока.

Если устройство решает запросить многократные разрешения за интервал, тогда параметр Разрешения за интервал DOCSIS ДОЛЖЕН быть установлен в целое значение, не меньшее 1. Если устройство не поддерживает или не запрашивает многократные разрешения за интервал, то параметр Разрешения за интервал DOCSIS ДОЛЖЕН быть установлен в 1.

Параметр *Номинальный интервал разрешений DOCSIS* ДОЛЖЕН быть равным интервалу пакетизации кодека,

DOCSIS Nominal Grant Interval = 10000 или 20000 или 30000

Параметр *Допустимое дрожание разрешений DOCSIS* ДОЛЖЕН быть установлен в определенное CMS значение, базирующееся на информации о цене маршрутизации. Допустимые границы для параметра лежат между 0 и 2 × интервал пакетизации. Если значение не определено CMS, ДОЛЖНО использоваться значение по умолчанию, равное 800 мкс.

Параметр *Номинальный интервал опроса DOCSIS* НЕ ДОЛЖЕН определяться для потоков услуг UGS и ЖЕЛАТЕЛЬНО должен принимать значение, кратное интервалу пакетизации кодека для пакетов услуг UGS/AD.

Параметр *Допустимое дрожание опроса DOCSIS* НЕ ДОЛЖЕН определяться для потоков услуг UGS и ЖЕЛАТЕЛЬНО должен принимать значение, кратное интервалу пакетизации кодека для пакетов услуг UGS/AD.

Параметр *Политика запроса/передачи DOCSIS* является маской битов и для потоков услуг UGS/AD ДОЛЖНЫ быть установлены биты 0–6 и 8.

Параметр Переписать DOCSIS TOS НЕ ДОЛЖЕН использоваться. Даже если этот параметр определен сетью DOCSIS, использование поля запрещается кабелем PacketCable.

Параметр *Размер незапрашиваемого разрешения DOCSIS* ДОЛЖЕН вычисляться начиная с заголовка FC MAC DOCSIS до конца CRC. В это значение включается предзаголовок заголовка Ethernet длиной 18 байтов (6 байтов для адреса источника, 6 байтов для пункта назначения, 2 байта для длины и 4 байта для CRC). Это значение также объединяет заголовок уровня MAC DOCSIS, включая базовый заголовок DOCSIS (6 байтов), расширенный заголовок UGS (3 байта) и расширенный заголовок BPI+ (5 байтов). Если подавление заголовка полезной нагрузки (PHP) активно, тогда число подавляемых байтов НЕ ДОЛЖНО включаться. Заметим, что расширенный заголовок PHS (2 байта) НЕ ДОЛЖЕН включаться для потоков услуг UGS/AD, поскольку соответствующая информация помещена в расширенный заголовок UGS.

DOCSIS Unsolicited Grant Size^8, 9 = M + 32 – PHS[3, 4]

Параметр *Планируемый тип восходящего потока DOCSIS* ДОЛЖЕН быть установлен в UGS или UGS/AD, в зависимости от того, поддерживается ли подавление пауз во время вызова

Если адаптером MTA осуществляется резервирование или фиксация для кодека, не поддерживающего установление голосовой активности, то MTA ДОЛЖЕН использовать в качестве запланированного типа UGS; в противном случае ДОЛЖЕН использоваться UGS/AD.

Если MTA осуществляет резервирование для потока услуг и многократных кодеков, из которых хотя бы один осуществляет установление голосовой активности, то MTA ДОЛЖЕН запросить UGS/AD о резервировании и фиксации свойств только активных кодеков, как описано в этом параграфе выше.

6.1.2.2 Кодирование классификации пакетов восходящего потока

Запросы пакетной классификации восходящего потока DOCSIS

Объекты восходящего потока сети DOCSIS должны быть установлены, как описано ниже. Кодирование всех других сообщений TLV классификации НЕ ДОЛЖНО определяться, что позволяет, таким образом, использовать значения по умолчанию. Если MTA передает значение TLV,

---

[3] В данном примере предполагается, что BPI+ используется как подмандатный Спецификации безопасности PacketCable.

[4] PHS, использованный в данном примере, описан в спецификации RFI DOCSIS, п. B.C.2.2.10.4/J.112.

которое должно быть опущено, то терминал CMTS ДОЛЖЕН отвергнуть запрос, выдав сообщение об ошибке "reject permanent/reject admin".

В случае, если он определен CMTS, параметр *Идентификатор классификатора DOCSIS* ДОЛЖЕН использоваться. В противном случае параметр *Ссылка классификатора DOCSIS* ДОЛЖЕН принимать для каждого Сообщения динамической услуги уникальное значение.

Параметру *Ссылка на поток услуг DOCSIS* ДОЛЖНО быть присвоено уникальное значение E-MTA для сообщений REQ_DSA в имеющихся вызовах, а для всех других сообщений он ДОЛЖЕН быть опущен. Вместо этого должен быть использован параметр *Идентификатора потока услуг DOCSIS*, выдаваемый CMTS.

Параметр *Приоритет управления DOCSIS* ДОЛЖЕН быть установлен в 128.

Параметр *Состояние активации классификации DOCSIS* ДОЛЖЕН быть установлен в активное состояние (1), когда вызов, использующий поток услуг, зафиксирован, а во всех других случаях он ДОЛЖЕН устанавливаться в неактивное состояние (0).

Действие изменение динамической услуги DOCSIS МОЖЕТ использовать Классификатор дополнения DSC (0), Классификатор замены DSC (1), Классификатор удаления DSC (2) в каждой спецификации RFI DOCSIS.

TOS IP DOCSIS и поля маски МОГУТ быть опущены, поскольку PacketCable не включает параметры TOS как часть своего классификатора. Однако, если этот параметр имеется, он должен соответствовать значению TOS, определенному CMS, или обусловленному значению для потоков голосовых услуг.

Параметр *протокол IP DOCSIS* ДОЛЖЕН быть установлен в UDP (17).

Параметр *Адрес источника IP DOCSIS* ДОЛЖЕН принимать то же значение адреса, что и указанный в шаблоне отправителя, если только он не принимает нулевого значения. Если адрес, определенный в шаблоне отправителя равен нулю, этот параметр ДОЛЖЕН быть опущен.

Параметр *Маска источника IP DOCSIS* ДОЛЖЕН быть опущен.

Параметры *Порт источника IP DOCSIS – старт* и *Порт источника IP DOCSIS – завершение* ДОЛЖНЫ быть равны значению порта транспорта, указанному в шаблоне обратного отправителя.

Параметр *Адрес назначения IP DOCSIS* ДОЛЖЕН получить то же значение, адреса, что и указанное в объекте сеанса, пока этот последний не равен нулю, в противном случае данный параметр должен быть опущен.

Параметр *Маска получателя IP DOCSIS* ДОЛЖЕН быть опущен.

Параметры *Порт получателя IP DOCSIS – старт* и *Порт получателя IP DOCSIS – завершение* ДОЛЖНЫ быть переданы порту, указанному в объекте сеанса, пока значение этого последнего не равно нулю. Если порт назначения определен в объекте сеанса равным нулю, TLV обоих параметров должны быть опущены.

Параметры *Кодирования пакетной классификации LLC Ethernet DOCSIS* ДОЛЖНЫ быть опущены.

Параметры *Кодирования пакетной классификации 802.1P/Q DOCSIS* ДОЛЖНЫ быть опущены.

Поведение CMTS при запросах пакетной классификации восходящего потока DOCSIS

При получении запроса дополнения классификатора (например путем получения сообщений DSx), CMTS ДОЛЖЕН сравнить установки шлюза, на которые указывает ID шлюза со значениями TLV в запросе. Если значения TLV не подходят, CMTS ДОЛЖЕН вернуть код ошибки классификатора DOCSIS со следующей информацией:

- Параметр *Код ошибки* ДОЛЖЕН содержать значение "reject-authorization-failure".

  Параметр *Ошибочный параметр* ДОЛЖЕН указывать значение первой TLV, не прошедшей авторизацию. Поскольку при различных реализациях TLV могут быть подтверждены в различном порядке, возвращенные в этом поле значения TLV при одинаковых исходных условиях могут не совпадать.
- Параметр *Сообщение об ошибке* МОЖЕТ быть заполнен.

6.1.2.3 Кодирование подавления заголовка полезной нагрузки

Запросы подавления заголовка полезной нагрузки в сети DOCSIS

Подавление заголовка полезной нагрузки является необязательным, однако в случае его применения необходимо следовать следующим требованиям, которые относятся к PHS как в восходящем так и в нисходящем потоках.

Параметр *Поле подавления заголовка полезной нагрузки DOCSIS* ссылается на те байты в заголовке, которые ДОЛЖНЫ быть подавлены посылающим объектом и должны быть восстановлены принимающим объектом.

Параметр *Размер подавления заголовка полезной нагрузки DOCSIS* ДОЛЖЕН быть равен общему числу байтов в поле подавления заголовка нагрузки (PHSF).

Параметр *Маска подавления заголовка полезной нагрузки DOCSIS* ДОЛЖЕН указывать байты, подвергающиеся подавлению.

Параметр *Подтверждение подавления заголовка полезной нагрузки DOCSIS* ЖЕЛАТЕЛЬНО установить в 0 (подтвердить).

Параметр *Идентификатор классификатора DOCSIS* ДОЛЖЕН быть использован в случае определения системой CMTS. В противном случае ДОЛЖЕН быть использован параметр *Ссылка на классификатор DOCSIS*, используемый в определении классификатора.

Параметр Ссылка на классификатор DOCSIS ДОЛЖЕН использоваться, если идентификатор классификатора DOCSIS не определен CMTS. В противном случае используется параметр Идентификатор классификатора DOCSIS, используемый в определении классификатора.

Параметр *Идентификатор потока услуг DOCSIS* ДОЛЖЕН использоваться в том случае, если он определен системой CMTS. В противном случае ДОЛЖЕН использоваться параметр *Ссылка на поток услуг*, который используется в определении классификатора.

Действие *Изменение динамической услуги DOCSIS* МОЖЕТ использовать правило дополнения PHS (0), правило установки PHS (1), правило удаления PHS (2) и операции правил удаления всех PHS для каждой спецификации RFI DOCSIS.

Поведение CMTS для запросов подавления заголовка полезной нагрузки DOCSIS

Описываемая здесь обработка ошибок PHS, дает довольно сложный механизм обратной связи между CMTS, отвергающей исходный запрос PHS и запрашивающим MTA с тем, чтобы выдаваемая в ответ на ошибку информация могла быть использована для упрощения альтернативного успешного подхода (т. е. успешного доступа к потоку UGS без подавления или с упрощенным правилом PHS).

При получении запроса DSx с Подавлением заголовка полезной нагрузки DOCSIS, если CMTS решает, что не может поддерживать запрашиваемое подавление (возможно, из-за недостатка ресурсов памяти или вычислительных), но может поддерживать услугу незапрашиваемых разрешений без подавления, то система ДОЛЖНА вернуть код подтверждения "reject-header-suppression" в кодировках ошибок подавления заголовка полезной нагрузки и в параметре ошибок DOCSIS, как описано ниже. МОЖЕТ использоваться Сообщение об ошибке DOCSIS.

Если система CMTS не может поддерживать запрашиваемое комплексное подавление заголовка полезной нагрузки DOCSIS, но может поддерживать более простую форму подавления, CMTS ДОЛЖНА поместить маску подавления заголовка полезной нагрузки DOCSIS в поле ошибочного параметра DOCSIS.

Ошибочный параметр DOCSIS = Маска подавления заголовка полезной нагрузки DOCSIS

Если CMTS не может поддерживать запрашиваемый размер для Подавления заголовка полезной нагрузки DOCSIS, но может поддерживать меньший размер такого подавления, то CMTS ДОЛЖЕН поместить Размер подавления заголовка полезной нагрузки DOCSIS в поле Ошибочного параметра DOCSIS.

Ошибочный параметр DOCSIS = размер подавления заголовка полезной нагрузки DOCSIS

Поведение E-MTA при запросах подавления заголовков полезной нагрузки DOCSIS

При получении кода подтверждения "reject-header-suppression" в котором Ошибочный параметр DOCSIS содержит Маску подавления заголовка полезной нагрузки, E-MTA МОЖЕТ повторно запросить ширину полосы без Подавления заголовка полезной нагрузки DOCSIS или может переопределить Маску подавления заголовка полезной нагрузки DOCSIS таким образом, что маска содержала бы более простое правило подавления (например, указывающее смежный блок подавляемых байтов).

При получении кода подтверждения "reject-header-suppression" в котором Ошибочный параметр DOCSIS содержит Размер подавления заголовка полезной нагрузки DOCSIS, E-MTA МОЖЕТ повторно запросить ширину полосы без Подавления заголовка полезной нагрузки DOCSIS.

Использование E-MTA расширенного заголовка UGS DOCSIS

Параметр *Индекс подавления заголовка полезной нагрузки* DOCSIS ДОЛЖЕН содержать заранее установленное значение индекса PHS или ноль, если для потока услуг не определено Подавление заголовка полезной нагрузки.

Параметр индикатора очереди DOCSIS ДОЛЖЕН быть установлен E-MTA всегда, когда в очереди на передачу находится более одного пакета. В противном случае это значение ЖЕЛАТЕЛЬНО очистить, приравняв нулю.

Поле Активных разрешений расширенного заголовка MAC DOCSIS ДОЛЖНО отражать только те субпотоки (вспомним, что в вырожденном случае существует только один субпоток), которые не находятся в режиме подавления пауз и ДОЛЖНЫ быть установлены в ноль всегда, когда E-MTA реализует Подавление пауз, для кодека, используемого для потока данных, связанного с этим потоком услуг.

6.1.2.4. Кодирование QoS в нисходящем направлении

Кодировки значений TLV качества обслуживания для потока услуг в нисходящем направлении сети DOCSIS ДОЛЖНЫ быть установлены, как указано ниже. Все остальные значения TLV НЕ ДОЛЖНЫ определяться, таким образом позволяя использовать значения по умолчанию. Если MTA использует одно из подобных TLV, то система CMTS ДОЛЖНА отвергнуть запрос выдав код ошибки "reject permanent/reject admin".

Параметры нисходящего потока DOCSIS вычисляются начиная с байта заголовка MAC DOCSIS, затем следуя от HCS до конца CRC. Заголовок уровня MAC (т. е. Ethernet) равен 18 байтам (6 байтов для адреса источника, 6 байтов для адреса получателя, 2 байта для длины и 4 байта для CRC).

На основании данного заголовка параметр *Размер пакета минимальной допустимой зарезервированной скорости DOCSIS* ДОЛЖЕН вычисляться так:

$$\text{DOCSIS Assumed Minimum Reserved Rate Packet Size} = m + 18 - \text{PHS}.$$

Параметр *Максимальная скорость поддерживаемого трафика DOCSIS*[5] выражается в бит/с, включая предзаголовок уровня MAC Ethernet (не сети DOCSIS). Преобразование из специфических параметров IP включает, во-первых, определение скорости пакетирования путем деления максимальной скорости на размер минимального наблюдаемого элемента. Это значение затем умножается на размер пакета, с поправкой на включение предзаголовка уровня MAC, и итоговый результат масштабируется из байтов в биты. Максимальная скорость поддерживаемого трафика DOCSIS ДОЛЖНА вычисляться как:

$$\text{DOCSIS Maximum Sustained Traffic Rate} = (p/m) \times (m + 18 - \text{PHS}) \times 8 \times z,$$

где z = число подпотоков в потоке услуги.

Параметр *Минимальная скорость зарезервированного трафика DOCSIS*[5] вычисляется способом, аналогичным Максимальной скорости поддерживаемого трафика, с той разницей, что вместо параметра пиковой скорости (p) используется зарезервированная скорость (R):

---

[5] Следует отметить, что если значение имеет дробную величину, то оно должно быть округлено.

DOCSIS Minimum Reserved Traffic Rate = (R/m) × (m + 18 – PHS) × 8 × z,

где z = количество разрешений за интервал, используемое в потоке восходящего потока.

Параметр *Максимальный пакет трафика DOCSIS* ДОЛЖЕН принимать наибольшее из нижеуказанных значений:

1) целый множитель Допустимого значения минимальной зарезервированной скорости; или

2) минимальное значение, определенное для сети DOCSIS и равное 1552.

DOCSIS Maximum Traffic Burst = max((M + 18 – PHS) × 3 × z, 1522)

где z = количество разрешений за интервал, используемое в потоке восходящего потока.

Параметр *Приоритет трафика DOCSIS* ДОЛЖЕН быть установлен в 5.

Параметр *Скрытность нисходящего потока DOCSIS* НЕ ДОЛЖЕН использоваться.

Значение для таймера *Активный таймаут DOCSIS* используется для обнаружения неактивности и инициирования восстановления ресурса для зафиксированных потоков услуг. Поскольку потоки услуг в восходящем и нисходящем потоках, а также шлюзы управляются с использованием одного и того же ID шлюза и вычеркиваются парами, то в модели PacketCable не нужно вести наблюдение одновременно за активностью восходящего и нисходящего потоков. По этой причине с использованием значения Активного таймаута DOCSIS ведется наблюдение только за потоками услуг восходящего потока. Это поле MTA и CMTS НЕ ДОЛЖНЫ заполнять для потоков услуг нисходящего потока.

Значение таймера Допустимый таймаут DOCSIS используется для обнаружения неактивности и инициирования восстановления ресурса для зарезервированных потоков услуг. Однако, по соображениям, аналогичным указанным выше, для параметра Активный таймаут, при использовании параметра Допустимый таймаут в модели IPCablecom не определен мониторинг для потоков услуг нисходящего потока. Это поле MTA и CMTS НЕ ДОЛЖНЫ заполнять для потоков услуг нисходящего потока.

6.1.2.5 Кодирование классификации пакетов нисходящего потока

Запросы пакетной классификации нисходящего потока DOCSIS

Объекты нисходящего потока сети DOCSIS должны быть установлены, как описано ниже. Кодирование всех других сообщений TLV классификации НЕ ДОЛЖНО определяться, что позволяет, таким образом, использовать значения по умолчанию. Если MTA содержит значение TLV, которое должно быть опущено, то терминал CMTS ДОЛЖЕН отвергнуть запрос, выдав сообщение об ошибке "reject permanent/reject admin".

В случае, если он определен CMTS, параметр *Идентификатор классификатора DOCSIS* ДОЛЖЕН использоваться. В противном случае параметр *Ссылка классификатора DOCSIS* ДОЛЖЕН принимать для каждого сообщения динамической услуги уникальное значение.

Параметру *Ссылка на поток услуг DOCSIS* ДОЛЖНО быть присвоено уникальное значение E-MTA для REQ – сообщений DSA в актуальных вызовах, а для всех других сообщений он ДОЛЖЕН быть опущен. Вместо этого должен быть использован параметр *Идентификатора потока услуг DOCSIS*, выдаваемый CMTS.

Параметр *Приоритет управления DOCSIS* ДОЛЖЕН быть установлен в 128.

Параметр *Состояния активации классификации DOCSIS* ДОЛЖЕН быть установлен в активное состояние (1), когда вызов, использующий поток услуг, зафиксирован, а во всех других случаях он ДОЛЖЕН устанавливаться в неактивное состояние (0).

Действие *Изменение динамической услуги DOCSIS* МОЖЕТ использовать Классификатор дополнения DSC (0), Классификатор замены DSC (1), Классификатор удаления DSC (2) в каждой спецификации RFI DOCSIS.

Поля *TOS IP DOCSIS* и поля масок *в* НЕ ДОЛЖНЫ использоваться.

Параметр *IP – протокола DOCSIS* ДОЛЖЕН быть установлен в UDP (17).

Параметр *Адрес источника IP DOCSIS* ДОЛЖЕН принимать то же значение адреса, что и указанный в шаблоне обратного отправителя, если только он не принимает нулевого значения. Если адрес, определенный в шаблоне обратного отправителя равен нулю, этот параметр ДОЛЖЕН быть опущен.

Параметр *Маска источника IP DOCSIS* ДОЛЖЕН быть опущен.

Параметры *Порт источника IP DOCSIS – старт* и *Порт Источника IP DOCSIS – завершение* ДОЛЖНЫ быть равны значению порта транспорта, указанному в шаблоне обратного отправителя, если оно не равно нулю. Если IP порт источника определен в шаблоне обратного отправителя, как нулевое значение, то сообщения TLV для параметров Старт и Завершение порта источника IP сети DOCSIS ДОЛЖНЫ быть опущены.

Параметр *Адрес получателя IP DOCSIS* ДОЛЖЕН получить то же значение, адреса, что и указанное в объекте обратного сеанса.

Параметр *Маска получателя IP DOCSIS* ДОЛЖЕН быть опущен.

Параметры *Порт получателя IP DOCSIS – старт* и *Порт получателя IP DOCSIS – завершение* ДОЛЖНЫ быть переданы порту, указанному в объекте обратного сеанса.

Кодирование пакетной классификации LLC Ethernet DOCSIS ДОЛЖНЫ быть опущены.

Кодирование пакетной классификации 802.1P/Q DOCSIS ДОЛЖНЫ быть опущены.

Поведение CMTS при запросах пакетной классификации нисходящего потока DOCSIS

При получении запроса дополнения классификатора (например, путем получения сообщений DSx), система терминалов CMTS ДОЛЖНА сравнить установки шлюза, на которые указывает ID шлюза со значениями TLV в запросе. Если значения TLV не подходят, CMTS ДОЛЖЕН вернуть код ошибки классификатора DOCSIS со следующей информацией:

- Параметр *Код ошибки* ДОЛЖЕН содержать "reject-authorization-failure".
- Параметр *Ошибочный Параметр* ДОЛЖЕН указывать значение первой TLV, не прошедшей авторизацию. Поскольку при различных реализациях TLV могут быть аутентифицированы в различном порядке, возвращенные в этом поле значения TLV при одинаковых исходных условиях могут не совпадать.
- Параметр Сообщение об ошибке МОЖЕТ быть заполнен.

6.1.2.6 Пример преобразования

Рассмотрим следующий пример. Речевой кодек создает выходной поток данных CBR со скоростью 64 кбит/с, который пакетизирован с интервалом 10 мс, т. е. с полезной нагрузкой в 80 байтов каждые 10 мс. Полезная нагрузка инкапсулируется с помощью RTP/UD/IP, причем дополнительные 40 байтов приводят к увеличению пакета до 120 байтов в каждые 10 мс. В этом случае сообщение TSpec имеет вид:

глубина области памяти (b) = 120 байтов

скорость области памяти (p) = 12 000 байтов/с

минимальный наблюдаемый элемент (m) = 120 байтов

максимальный размер дейтаграммы (M) = 120 байтов

Предположим, что клиент запрашивает резервирование, используя указанные сообщения TSpec и RSpec при R = r. Система завершения CMTS при получении этого сообщения установит поток услуг, использующий услугу незапрашиваемого разрешения, поскольку p = r и M = b , что указывает на поток CBR. Он может использовать разрешение с размером M и интервалом M/R, равным 10 мс.

При вычислении дрожания адаптер MTA не знает, насколько CMTS отклоняется от идеала при запланированном поведении. Клиент должен считать, что CMTS является идеальной, что означает, что задержка при данном TSpec и резервированной скорости R = r будет просто:

b/r + задержки на распространение сигнала.

Не учитывая задержки на распространение сигнала, это приведет к задержке в 10 мс. Предположим, что клиенту на этот сеанс нужна допустимая задержка в 15 мс (только для тракта клиентской CMTS)

тогда пассивный член (S) примет значение, равное 15 – 10 = 5 мс. При получении резервирования, система CMTS воспримет это как показатель того, что для клиента допустимо дрожание в 5 мс.

Допустим, клиент считает допустимой задержку в 25 мс и устанавливает пассивный член равным 25 – 10 = 15 мс. CMTS может использовать данную информацию для определения в качестве допустимого большего интервала разрешения, например, равного 20 мс, поскольку это приводит к возможному росту задержки до 20 мс для пакета, который поступает на CM непосредственно после разрешения. Остаются еще пассивные 5 мс, которые CMTS может использовать для установки разрешенного дрожания.

Заметим, что такой подход оставляет значительную гибкость для того, чтобы CMTS могла удовлетворить требованиям клиента относительно задержки способом, в наибольшей степени учитывающим возможности данной CMTS.

6.1.3 Авторизация и поведение CMTS

CMTS, по получении запросов о резервировании или фиксировании ширины полосы, содержащих ID шлюза, должен осуществить контроль доступа к запросу, использующему объекты, связанные с ID шлюза.

Каждый запрос DSA или DSC исходящий от E-MTA в поддержку конкретного сеанса вызова ДОЛЖЕН содержать в Блоке авторизации ID шлюза, в противном случае система завершения CMTS ДОЛЖНА отвергнуть запрос, выдав код подтверждения 24 (Ошибка авторизации). Если получено сообщение запроса DSC, содержащее ID шлюза, отличное от содержащегося в запросе DSA, использованного при создании потока услуг, то CMTS ДОЛЖНА осуществить обычную операцию авторизации и допуска с использованием шлюза, связанного с новым ID шлюза.

Если MTA не использует Многократные разрешения на интервал в модифицируемом потоке услуг, а контроль авторизации и допуска пройден успешно, CMTS ДОЛЖНА связать новый ID шлюза с модифицированным потоком услуг, заменить параметры сети DOCSIS Допустимый таймаут потока и Активный таймаут потока для связанного потока услуг на таймеры T7 и T8 нового шлюза восходящего потока и включить эти значения таймеров в ответное сообщение DSC адаптеру MTA. В этом случае система CMTS ДОЛЖНА немедленно удалить исходный шлюз и уведомить сервер CMS сообщением Закрыть шлюз с Подкодом причины, равным 0 (норма).

Если MTA использует многократные разрешения на интервал, а контроль авторизации и доступа успешно пройден, CMTS ДОЛЖНА связать новый ID шлюза с новым подпотоком, не внося никаких изменений в уже существующие подпотоки и связанные с ними шлюзы. Значения параметров сети DOCSIS Допустимый таймаут потока и Активный таймаут потока, связанные с потоком услуг таймерами T7 и T8 нового шлюза восходящего потока и включить значения этих таймеров в ответное сообщение DSC адаптеру MTA.

Элементы CMTS и CMS НЕ ДОЛЖНЫ снова использовать шлюз, ранее связанный с потоком услуг, при авторизации отдельного потока услуг. CMTS ДОЛЖЕН отвергнуть запрос о резервировании или фиксации для нового потока услуг относительно шлюза, авторизующего отдельный поток услуг с помощью кода подтверждения, равного 24 (ошибка авторизации).

Заметим, что указанное требование применимо к запросам полосы, обрабатываемым модулем авторизации IPCablecom. Это не предотвращает использование модуля авторизации сети DOCSIS для обработки других запросов без использования блока авторизации. Модули авторизации проекта IPCablecom и сети DOCSIS являются логическими функциями системы CMTS, которые одобряют или отвергают параметры и классификаторы QoS. Концептуально, когда запрос QoS поступает на CMTS, модуль авторизации DOCSIS определяет, будет ли обрабатываться запрос внутри модуля авторизации DOCSIS или будет передан модулю авторизации IPCablecom.

Если CMTS не может отыскать шлюз, соответствующий данному ID шлюза, она ДОЛЖНА вернуть код подтверждения, равный 24 (ошибка авторизации), показывающий, что этот запрос не прошел авторизацию и будет отвергнут.

Если CMTS находит шлюз, соответствующий ID шлюза, то CMTS должен следовать процедуре авторизации, описанной ниже. Для осуществления управления доступом для сообщений DSx сети DOCSIS и сравнения этих сообщений на основе учета параметров с сообщениями, авторизованными через объект GateSpec, CMTS должен нормализовать параметры QoS как для второго, так и для

третьего уровня, прибавляя или вычитая предзаголовок связывания слоев. В примерах, приведенных в данной Рекомендации, подразумевается, что нормализация выражается в параметрах уровня три путем преобразования параметров сети DOCSIS в их RSVP-эквиваленты, используя методы, описанные в данном разделе.

– Глубина области памяти GateSpec (b) ДОЛЖНА быть не меньше запрашиваемого MTA значения
– Скорость области памяти GateSpec (r) ДОЛЖНА быть не меньше запрашиваемого MTA значения
– Максимальный размер дейтаграммы GateSpec (M) ДОЛЖЕН быть не меньше запрашиваемого MTA значения
– Минимальный размер дейтаграммы GateSpec (m) ДОЛЖЕН быть не меньше запрашиваемого MTA значения.
– Пиковая скорость GateSpec (p), ДОЛЖНА быть не меньше запрашиваемого MTA значения.
– Зарезервированная скорость GateSpec (R), ДОЛЖНА быть не меньше запрашиваемого MTA значения.
– Пассивный член GateSpec (s) ДОЛЖЕН быть не больше запрашиваемого MTA значения.
– Протокол GateSpec ДОЛЖЕН быть эквивалентен протоколу, запрашиваемому MTA.
– Адрес получателя GateSpec ДОЛЖЕН быть тем же, что и адрес, запрашиваемый MTA, если GateSpec содержит ненулевое значение. Если GateSpec содержит нулевое значение, то данное сравнение ДОЛЖНО быть опущено.
– Порт получателя GateSpec ДОЛЖЕН быть тем же, что и порт, запрашиваемый MTA, если GateSpec содержит ненулевое значение. Если GateSpec содержит нулевое значение, то данное сравнение ДОЛЖНО быть опущено.
– Адрес отправителя GateSpec ДОЛЖЕН быть тем же, что и адрес, запрашиваемый MTA, если GateSpec содержит ненулевое значение. Если GateSpec содержит нулевое значение, то данное сравнение ДОЛЖНО быть опущено.
– Порт отправителя GateSpec ДОЛЖЕН быть тем же, что и порт, запрашиваемый MTA, если GateSpec содержит ненулевое значение. Если GateSpec содержит нулевое значение, то данное сравнение ДОЛЖНО быть опущено.

Если одно из вышеуказанных сравнений авторизации оказывается неудачным для сообщения, запрашивающего новый поток услуг или изменяющего параметры резервирования уже существующего потока, то CMTS НЕ ДОЛЖНА отвечать на запрос созданием нового потока услуг или изменением параметров уже существующего. Если MTA запрашивает операцию фиксации для зарезервированного потока, то авторизация ДОЛЖНА быть проведена с использованием параметров сети DOCSIS и с использованием определенного в DOCSIS метода.

6.2 Поддержка в DOCSIS резервирования ресурса

В Рекомендации МСЭ-Т J.112 не описан путь прохождения авторизации информации, передаваемой от CM к модулю авторизации CMTS. Модуль авторизации является логической функцией CMTS, определенной в Рекомендации МСЭ-Т J.112. Эта Рекомендация использует новое значение TLV DOCSIS, которое проходит блок авторизации, состоящий из произвольной строки длиной *n* в направлении CMTS, чтобы затем быть интерпретированным и обработанным только модулем авторизации.

Модель DQoS это модель, в которой проходит авторизацию каждый сеанс. Авторизация каждого сеанса использует дескриптор, который применяется одновременно для CMTS и MTA и которая используется для согласования запросов и авторизации. Этим дескриптором является ID шлюза. После получения информации, сигнализирующей о вызове, MTA передает ID шлюза в систему терминалов CMTS, используя сообщение TLV, прошедшее блок авторизации и содержащееся в сообщении DSA/DSC.

CMTS IPCablecom ДОЛЖНА иметь возможности подключения/отключения различных методов для авторизации DSx-запроса модема CM для открытия (start) и/или модифицирования потоков услуг. CMTS IPCablecom ДОЛЖНА осуществлять метод "GateID authorization", в котором CMTS будет

авторизировать только запросы, содержащие ID шлюза в блоке авторизации IPCablecom. Для CMTS ЖЕЛАТЕЛЬНО осуществлять авторизацию Имени класса услуг (SCN); при этом CMTS будет авторизовать запросы DSx только для конфигурированного набора имен класса услуг, определенного в CMTS.

6.2.1 Резервирование/Фиксирование с двухступенчатым качеством QoS

Поток услуг в сети DOCSIS имеет три связанных набора параметров качества обслуживания, называемых Обеспечиваемый, Допустимый, или Активный набор параметров QoS. Связь между ними аналогична описанной в разделе 5.7.4 между Авторизованным, Зарезервированным и Фиксированным ресурсами.

Операции Зарезервировать и Зафиксировать обе осуществляются с использованием сообщений динамической услуги сети DOCSIS путем изменения значений AdmittedQoSParameterSet (набор параметров допустимого QoS) и ActiveQoSParameterSet (набор параметров активного QoS) для потока услуг. В сообщениях добавления динамической службы (DSA) и изменения динамической службы (DSC), операция Зарезервировать совершается путем включения в кодировки потоков как восходящего, так и нисходящего потоков сообщения TLV типа набора параметров QoS (QoSParameterSetType), со значением, установленным в Допустимое (значение 2). Аналогично, операция Зафиксировать выполняется при значении TLV, для типа набора параметров QoS (QoSParameterSetType), установленном в Активное (значение 4) или Допустимое + Активное (значение 6)

Обмен сообщениями DSA и DSC между модемом CM и системой завершения CMTS представляет из себя трехэтапное установление соединения: сообщения запроса, сопровождаемого ответом и завершаемого подтверждением. Это проиллюстрировано рисунком 5.

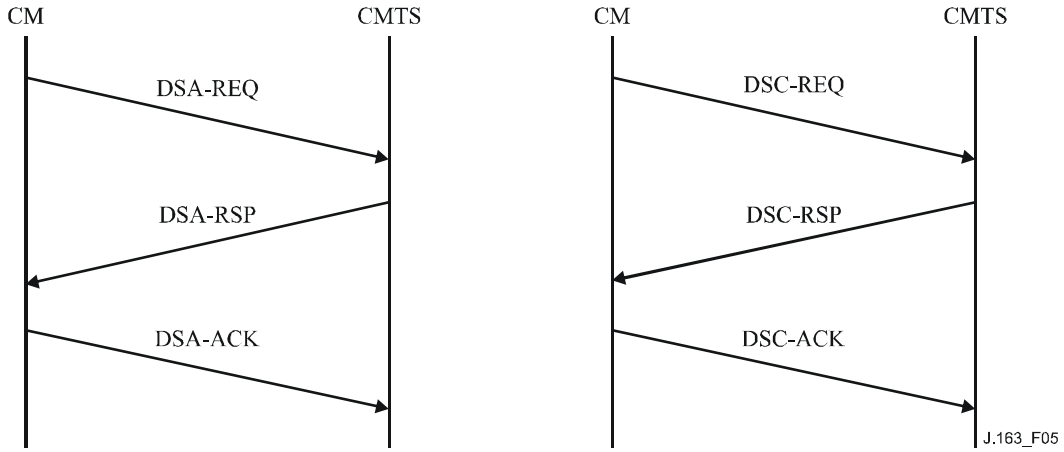


Рисунок 5/J.163 – Обмен сообщениями DSA и DSC между модемом CM и системой CMTS

Например, нижеследующее сообщение DSA-REQ приводит к установлению потоков услуг восходящего и нисходящего потока, что означает резервирование ресурсов QoS, используемых в сети DOCSIS.

DSA-REQ

TransactionID		1
UpstreamServiceFlow	ServiceFlowReference	1
	QoSParameterSetType	Допустимый (2)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 мс
	ToleratedGrantJitter	2 мс
	GrantsPerInterval	1
	UnsolicitedGrantSize	222
DownstreamServiceFlow	ServiceFlowReference	2
	QoSParameterSetType	Допустимый (2)
	TrafficPriority	3
	MaximumSustainedRate	12000

В качестве примера, следующий обмен сообщениями DSC-REQ вызывает активацию потока услуг, что означает, что ресурсы QoS, используемые DOCSIS, зафиксированы.

DSC-REQ

TransactionID		1
UpstreamServiceFlow	ServiceFlowID	10288
	QoSParameterSetType	Admitted + Active (6)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	222
DownstreamServiceFlow	ServiceFlowID	10289
	QoSParameterSetType	Admitted + Active (6)
	TrafficPriority	3
	MaximumSustainedRate	12000

Спецификация набора параметров Допустимого и Активированного QoS от MTA передается путем запроса MAC "СОЗДАТЬ ПОТОК УСЛУГ" и запроса MAC "ИЗМЕНИТЬ ПОТОК УСЛУГ". Ко времени установления потока услуг он обычно имеет связанный классификатор(ы).

6.2.2 Поддержка резервирования

Параметры QoS потока услуг сети DOCSIS "Таймаут для активных параметров QoS" и "Таймаут для допустимых параметров QoS" допускают прерывание сеанса и высвобождение ресурсов из-за неактивности.

Таймаут для активных параметров QoS (TimeoutForActiveQoSParameters) предназначен для восстановления ресурсов, назначенных модемам CM, которые приходят в негодность и тем или иным способом теряют способность устанавливать соединение с кабельной сетью. Для того, чтобы такое восстановление не понадобилось, достаточно осуществлять передачу пакетов данных в нормальном режиме.

Если Активный таймаут (время ожидания) DOCSIS в системе CMTS заканчивается для потока услуг, который авторизован через шлюз (например, поток услуг PacketCable), то сеть CMTS удалит все потоки услуг, связанные со шлюзом, использующим запрос DSD сети DOCSIS. Сеть завершения CMTS, информируя GC о закрытии шлюза, выдаст определение: "Истечение времени таймера T8; неактивность потока услуг в восходящем направлении".

Если MTA осуществляет действие Установление голосовой активности с типом планирования потока услуг, равным UGS/AD а CMTS активно выполняет мониторинг активности восходящего потока, то во время периодов продолжительного молчания MTA ДОЛЖЕН или посылать периодические пакеты данных в поток услуг или возобновлять действие активного таймера с помощью сообщений DSC. таймаут параметров допустимого QoS (TimeoutForAdmittedQoSParameters) предназначен для восстановления ресурсов, зарезервированных для CM, но не зафиксированных. Как правило, зафиксированные параметры совпадают с зарезервированными, и особых проблем не возникает. Когда фиксирование осуществляется для меньшего набора параметров, чем резервирование, необходимо периодически возобновлять включение таймера CMTS. Это происходит при выполнении операции DSC-REQ, которая резервирует те же ресурсы, что и ранее.

6.2.3 Поддержка динамического связывания ресурсов

Модель динамического QoS требует способности динамически модифицировать связывание ресурсов с потоками. Например, для обеспечения ожидания вызова, может быть желательным иметь ресурсы, достаточные для осуществления только одного вызова для произвольного абонента сети DOCSIS и, по мере надобности, переназначать эти ресурсы от одного абонента к другому.

Чтобы обеспечить такую функциональность, добавляется объект "ID ресурса". Объект ID ресурса является непрозрачным идентификатором, генерируемым узлом, управляющим ресурсами, т. е. в данном случае системой CMTS.

Когда клиент посылает запрос резервирования для нового потока, это указывает CMTS, что этому сеансу желательно поделить ресурсы этого нового шлюза (Шлюз 1) с созданным ранее шлюзом (Шлюз 2), включив в запрос ID ресурса. Пока назначением ширины пропускания, не большей существующего шлюза, могут удовлетворяться требования QoS, запрашиваемого для нового шлюза, в сети DOCSIS не происходит резервирования новой полосы пропускания. Однако может понадобиться резервирование полосы пропускания в зависимости от сквозного тракта, занятого в магистральной сети новым сеансом. Доступ к разделенным (shared) зарезервированным ресурсам осуществляется взаимоисключающим способом.

Динамическое связывание ресурсов, требуемое в разделе 5.7.7, осуществляется согласно Рекомендации МСЭ-T J.112 с использованием сообщения TLV блока авторизации.

Система терминалов CMTS ДОЛЖНА включать в TLV блока авторизации идентификатор ID ресурса для сообщения DSA-RSP, которое она посылает клиенту. Абонент в дальнейшем МОЖЕТ включать ID ресурса в сообщения DOCSIS, соответствующие рассматриваемым ресурсам. Очень важно иметь в виду, что если абонент хочет установить новый сеанс и вновь использовать ресурсы существующего сеанса, он ДОЛЖЕН сначала деактивировать потоки услуг прежнего сеанса с помощью DSC-REQ и включить ID ресурса, связанный с прежним сеансом в сообщение DSA-REQ, посылаемое CMTS.

6.2.4 Преобразование параметров QoS для авторизации

Шлюз, идентифицированный ID шлюза параметризуется с использованием сочетания FlowSpec RSVP (образованного из объектов RSpec и TSpec) в каждом направлении. Модуль авторизации в CMTS должен преобразовать параметры QoS сети DOCSIS в соответствующие параметры RSVP, используя определенные ниже правила.

Параметры *Размер области памяти маркера* (b), *Максимальный размер пакета* (M), *Минимальный наблюдаемый элемент* (m) ДОЛЖНЫ быть установлены в *Размер незапрашиваемого разрешения* минус заголовок восходящего UGS[6] DOCSIS для восходящего потока и в *Размер допустимой минимальной зарезервированной скорости пакета DOCSIS* минус нисходящий заголовок[7] в нисходящем направлении.

Для нисходящего потока параметры *Скорость области памяти маркера* (r) и *Пиковая скорость данных)* (p) должны быть получены преобразованием *Максимальной поддерживаемой скорости DOCSIS* в термины уровня 3 путем деления ее на *Размер пакета минимальной допустимой поддерживаемой скорости сети DOCSIS* и затем умножения результата на вычисленный ранее максимальный размер пакета. Для потока восходящего потока параметры *Скорость области памяти маркера* (r) и *Пиковая скорость данных* (p) ДОЛЖНЫ быть равны *Номинальному параметру разрешения DOCSIS*, умноженному на *Размер незапрашиваемого разрешения*.

Для нисходящего потока параметр Скорость (R) ДОЛЖЕН быть вычислен, используя преобразование *максимальную скорость зарезервированного трафика DOCSIS* в термины уровня 3 делением ее на *Размер пакета минимальной допустимой зарезервированной скорости DOCSIS* и затем умножением полученного результата на предварительно вычисленный *Минимальный наблюдаемый элемент*. Для восходящего потока параметр *Скорость* (R) ДОЛЖНА быть установлена равной *Номинальному интервалу разрешения DOCSIS*, умноженному на *Размер незапрашиваемого разрешения.*

Пассивный член ДОЛЖЕН быть для восходящего потока установлен в *Допустимое Дрожание Разрешения DOCSIS* .Для нисходящего потока Пассивный член ДОЛЖЕН быть установлен равным нулю, указывая, что этот параметр не будет определяться адаптером MTA.

ID протокола ДОЛЖЕН быть установлен в *ID протокола DOCSIS*.

Адрес Получателя должен быть установлен в *Адрес Получателя DOCSIS*. Если этот параметр опускается, значение ДОЛЖНО быть установлено в ноль.

Адрес Получателя ДОЛЖЕН быть установлен в *Адрес Получателя IP DOCSIS*. Если этот параметр опущен, значение ДОЛЖНО быть установлено в ноль.

Порт Назначения ДОЛЖЕН быть установлен в *Старт Порта Назначения IP DOCSIS*. Если этот параметр опущен, это значение ДОЛЖНО быть установлено в ноль.

Адрес Источника ДОЛЖЕН быть установлен в *Адрес Источника IP DOCSIS*.

Порт Источника ДОЛЖЕН быть установлен в *Старт Порта Источника IP DOCSIS*.

Для итоговых объектов RSVP должно быть подтверждено их соответствие шлюзам согласно следующим правилам:

Все запрашиваемые параметры сочетания *FlowSpec RSVP* и *Пассивного члена* ДОЛЖНЫ быть не больше значений, определенных шлюзом.

Все запрашиваемые параметры *TSpec RSVP* ДОЛЖНЫ быть равны значениям, определенным шлюзом, кроме случая, когда значение шлюза равно нулю, в котором соответствующий параметр запроса НЕ ДОЛЖЕН подтверждаться.

Если подтверждение прошло успешно, то CMTS ДОЛЖНА продолжить обработку запроса. В противном случае CMTS ДОЛЖНА постоянно отвергать запрос из-за ошибки авторизации.

---

[6] Предзаголовок должен включать предзаголовок заголовка Ethernet размером 18 байтов (6 байтов на адрес источника, 6 байтов на адрес получателя, 2 байта на длину, 4 байта для CRC). Эта величина также включает предзаголовок уровня MAC, включая базовый заголовок DOCSIS (6 байтов), расширенный заголовок UGS, (3 байта) и расширенный заголовок BPI+ (5 байтов). Если подавление заголовка полезной нагрузки активно, то количество подавляемых байтов должно прибавляться к Размеру незапрашиваемого разрешения DOCSIS.

[7] Предзаголовок уровня MAC сети DOCSIS должен включать 18 байтов (6 байтов адреса отправителя, 6 байтов адреса получателя, 2 байта на длину и 4 байта CRC). Если используется подавление заголовка полезной нагрузки, количество подавляемых байтов должно вычитаться из Размера пакета минимальной допустимой зарезервированной скорости.

Например, при значениях кодека, G.711, установке кадра в 20 мс, 2-байтном RTP-S MAC и активном BPI+:

G.711 @ 20 ms

номинальная битовая скорость 64 кбит/с

номинальная байтовая скорость 8 кбайт/с

скорость установки кадра = 20 мс = 50 пакетов/с

полезная нагрузка = 8 кбайт/с / 50 = 160 байтов на пакет

42 байта заголовка IP/UDP/RTP

всего 160 + 42 = 202 байта на пакет

актуальная байтовая скорость 202 × 50 = 10,1 кбайт/с

актуальная битовая скорость 10,1 × 8 = 80,8 кбит/с

Итоговые параметры GateSpec после их установки сервером CMS:

Глубина области памяти (b) = размеру дейтаграммы, включая предзаголовок заголовка IP/UDP/RTR = 202 байтам.

Минимальный наблюдаемый элемент (m) = глубине области памяти (b) = 202 байтам

Максимальный размер дейтаграммы (M) = глубине области памяти (b) = 202 байтам

Скорость области памяти (r) = актуальной (наличной) скорости данных, включая предзаголовок заголовка IP/UDP/RTP = 10 100 байтам в секунду

Пиковая скорость (p) = скорость области памяти (r) = 10 100 байтам в секунду

Зарезервированная скорость (R) = скорость области памяти (r) = 10 100 байтам в секунду

Параметры DOCSIS в восходящем направлении включают заголовок от байта FC через CRC.

Базовый заголовок DOCSIS (от FC к HCS, без расширенных заголовков); 6 байтов

Расширенный заголовок UGS, 3 байта

Расширенный заголовок BPI+, 5 байтов

Заголовок Ethernet, 14 байтов

CRC, 4 байтов

Полный заголовок восходящего потока, 32 байта на пакет

Параметры восходящего потока услуг DOCSIS:

Тип планирования восходящего потока: UGS

Запрос/Алгоритм передачи (Бит – маска); набор битов 0-6; 8 (двоичный 101111111)

Размер разрешения: 234 байта

Разрешения на интервал (целое): 1

Интервал разрешения: 20000 микросекунд

Допустимое дрожание разрешений: 800 микросекунд

Процедура управления авторизацией в CMTS проводится следующим образом:

Для сравнения с параметрами спецификации GateSpec, заголовок уровня MAC должен быть вычтен из параметров DOCSIS.

Глубина области памяти GateSpec (b) ≥ Размер незапрашиваемого разрешения DOCSIS – 32 байта

202 байта ≥ 234 байта – 32 байта = 202 байта

Скорость области памяти GateSpec (r) ≥ 1/интервал разрешения DOCSIS × (размер незапрашиваемого разрешения DOCSIS – 32)

10,1 кбайт/с ≥ 1/20 мс× (234 байтов – 32 байтов) = 50 пакетов в секунду × 202 байта на пакет = 10,1 кбайт/с

Параметры DOCSIS в нисходящем направлении включают предзаголовок из байта, следующего за HCS по CRC.

Заголовок Ethernet: 14 байтов

CRC: 4 байтов

Полный заголовок нисходящего потока: 18 байтов на пакет

Параметры нисходящего потока услуг DOCSIS:

Максимальный пакет трафика (не меньше 1552) 1552 байта

Максимальная поддерживаемая скорость: 88 000 битов в секунду

Допустимый размер пакета минимальной допустимой скорости: 220 байтов

Минимальная допустимая скорость: 88 000 битов в секунду

Приоритет трафика: 5

Процедура управления авторизацией в CMTS для параметров в нисходящем направлении проводится следующим образом:

Вновь предзаголовок должен быть вычитаем из параметров DOCSIS для осуществления сравнения GateSpec. Процедура (вычитание) является для параметра *Допустимый размер пакета минимальной зарезервированной скорости сети DOCSIS* очень простой. Однако для настройки параметра Минимальной зарезервированной скорости требуется еще один бит.

Минимальный наблюдаемый элемент GateSpec (m) ≥ (Допустимый размер пакета минимальной зарезервированной скорости) – (18 × z) байтов

Например, если число разрешений на интервал равно z = 1

202 байта ≥ 220 байтов – 18 байтов = 202 байта

Скорость области памяти GateSpec (r) ≥ (Минимальная зарезервированная скорость DOCSIS / (8 × Допустимый размер пакета минимальной зарезервированной скорости DOCSIS)) = (Допустимый размер пакета минимальной зарезервированной скорости – 18 × z байтов).

Например, если количество разрешений на интервал = z = 1

10,1 кбайт/ с ≥ (88 кбит/с/ (8 × 220 байтов)) × (220 байтов – 18 байтов/с) = 10.1 кбайт/с

6.2.5 Кодирование блока авторизации

Блок авторизации состоит из строки байтов. Для большей гибкости, блок авторизации ДОЛЖЕН кодироваться путем использования полей значений типа длины (TLV). Поля, содержащие значения TLV, неупорядочены, и могут быть вложенными. Размер (в байтах) поля значений должен быть больше нуля; размеры полей типа и длины – по 1 байту каждый. Обратите внимание, что длина включает только поле значений и не является содержащей полное значение типа длины TVL.

Формат блока авторизации следующий:

Кодирование блока авторизации проекта IPCablecom

Это поле определяет параметры, связанные с блоком авторизации проекта IPCablecom и состоит из вложенных подполей.

Тип	Длина	Значение
1	n	"смотри подполя ниже"

Кодирование ID шлюза

Значение этого поля определяет дескриптор ID шлюза, используемый для авторизации

Тип	Длина	Значение
[1].1	4	ID шлюза

Кодирование ID ресурса

Значение данного поля определяет дескриптор ID ресурса, используемый для уникальной идентификации набора ресурсов, связанного с потоком услуг.

Тип	Длина	Значение
[1].2	4	ID ресурса

Статус подпотока

Тип	Длина	Значение
[1].3	1	статус

Этот байт определяет статус подпотока, который может иметь 4 состояния (0 – Допустимый, 1 – Активный, 2 – Удаление, 3 – Переместить). Байт статуса предназначен для помощи системе CMTS в управлении состоянием различных шлюзов, которые могут присутствовать в отдельном потоке. Этот параметр ДОЛЖЕН быть включен во все инициированные CM запросы DSx, использующие число разрешений за интервал, большее 1.

Допустимый (0) – подпоток в допустимом состоянии

Активный (1) – подпоток в активном состоянии

Удален (2) – шлюз в результате данного DSC должен быть удален

Переместить (3) – подпоток передается новому потоку услуг

Для того, чтобы система CMTS могла правильно связать изменения с данным ID шлюза, MTA ДОЛЖЕН включать в данное DSx только один экземпляр блока авторизации DOCSIS (тип 30). Внутри блока авторизации DOCSIS ДОЛЖНА существовать только одна кодировка блока авторизации IPCablecom (тип 30.1) вместе с требуемым подзначением TLV IDшлюза (тип 30.1.1) и, возможно, другими подзначениями для каждого подпотока из потока. Если используется только одно разрешение на интервал (и, значит, единственный ID шлюза), блок авторизации ДОЛЖЕН существовать, а поле статуса для подпотока ДОЛЖНО быть опущено.

Детали авторизации в CMTS смотрите в пункте 6.1.3

6.2.6 Обработка подавления заголовка полезной нагрузки

В спецификации RFI DOCSIS выведены правила для добавления и удаления правил PHS (в объединении с классификатором). Однако процедура обновления правила PHS, если оно стало неэффективным, неочевидна. Если применение PHS для голосового потока нуждается в изменении.

В случае, если уже существующее подавление PHS становится неэффективным, MTA ДОЛЖЕН осуществить единственную транзакцию одного из следующих типов:

– Добавляет новый классификатор с новым правилом PHS.

– Настраивает диапазон режимов QoS, отражающий новое правило PHS.

– Удаляет старый классификатор и связанное с ним правило PHS.

6.3 Использование интерфейса управляющей службы MAC сети DOCSIS

О параметрах QoS сети DOCSIS для потока услуг, отклоняющихся от описанных в SDP, сигнализируется для установления потока (потоков) услуг. В этом разделе описывается, как это можно сделать, используя интерфейсы управляющей службы MAC сети DOCSIS (Дополнение E к Дополнению B/J.112).

На уровне примитивов Интерфейса управляющей службы MAC сети DOCSIS, встроенный адаптер MTA сигнализирует о ресурсах QoS следующим образом:

1) запрос MAC СОЗДАТЬ ПОТОК УСЛУГ

   Как описано в B.E.3.2/J.112, встроенный MTA может посылать запросы о добавлении потока услуг, используя этот примитив. Этот примитив может также использоваться для определения классификаторов для нового потока услуг, а также как источник наборов параметров Допустимого и Активного QoS потока услуг. Успешное или неудачное завершение запроса с использованием этого примитива отражается в ответном примитиве MAC СОЗДАТЬ ПОТОК УСЛУГ.

2) запрос MAC ИЗМЕНИТЬ ПОТОК УСЛУГ

   С помощью этого примитива встроенный адаптер MTA может инициировать изменения в наборах параметров Допустимого и Активного QoS. Одним из возможных сценариев является блокирование вызывающего абонента. Успех или неудача использования этого примитива отображается в использовании ответного примитива MAC ИЗМЕНИТЬ ПОТОК УСЛУГ.

3) запрос MAC УДАЛИТЬ ПОТОК УСЛУГ

   Когда встроенный адаптер MTA более не нуждается в потоке услуг, он посылает встроенному MTA запрос MAC УДАЛИТЬ ПОТОК УСЛУГ, чтобы обнулить наборы параметров Активного и Допустимого QoS.

Параметры данных примитивов согласуются с параметрами, связанными с сообщениями DSA, DSC и DSD, как это описано в Дополнении B/J.112.

6.3.1 Установление резервирования

Адаптер MTA инициирует резервирование ресурсов QoS, используя примитив запроса MAC СОЗДАТЬ ПОТОК УСЛУГ. MTA ДОЛЖЕН включать в значение TLV блока авторизации ID шлюза. После получения этого сообщения, MAC-уровень модема CM вызывает сигнал DSA, посылая системе CMTS сообщение DSA REQ. CMTS ДОЛЖНА проверить авторизацию на основании ID шлюза (содержащегося в TLV блока авторизации), и отвергнуть запрос, если шлюз указан неправильно, или авторизованных ресурсов недостаточно для выполнения запроса. После получения от CMTS DSA RSP служба MAC уведомляет верхний уровень, используя ответное сообщение MAC СОЗДАТЬ ПОТОК УСЛУГ. Это проиллюстрировано на рисунке 6.

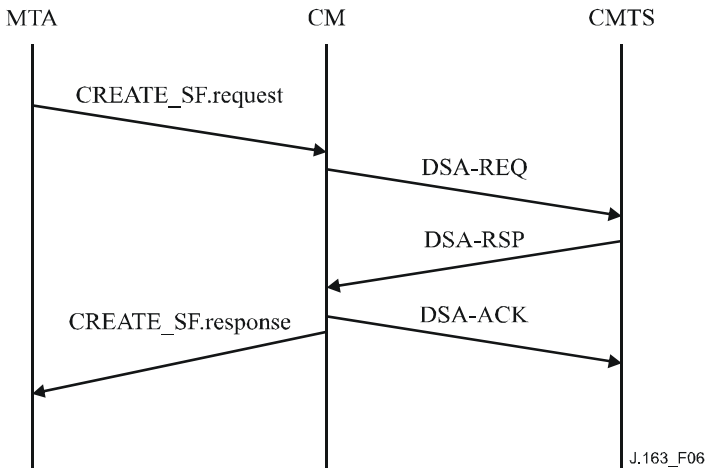


Рисунок 6/J.163 – Установление резервирования

6.3.2 Изменение резервирования

MTA вызывает изменение ресурсов, используя примитив запроса MAC ИЗМЕНИТЬ ПОТОК УСЛУГ. Это иллюстрируется рисунком 7.

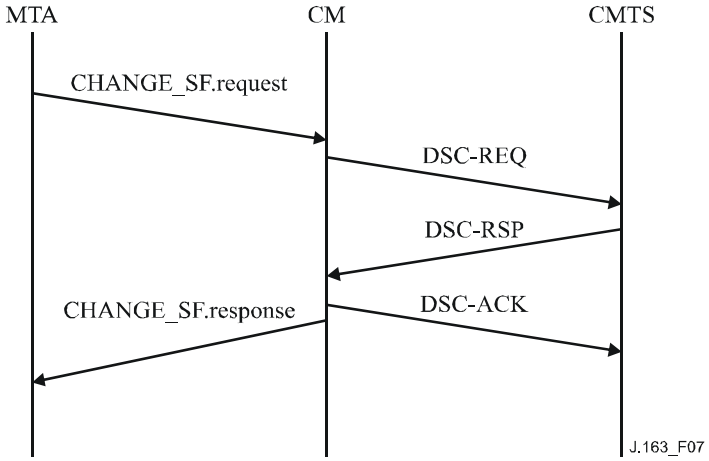


Рисунок 7/J/163 – Изменение резервирования

После получения этого сообщения, MAC – уровень CM вызывает сигнализацию DSC. После получения DSC RSP от CMTS, служба MAC уведомляет верхний уровень, используя ответное сообщение MAC ИЗМЕНИТЬ ПОТОК УСЛУГ.

6.3.3 Удаление резервирования

Адаптер MTA инициирует перераспределение резервирования QoS, используя примитив запроса MAC УДАЛИТЬ ПОТОК УСЛУГ. После получения этого сообщения, уровень MAC вызывает сигнализацию DSD. После получения от CMTS сообщения DSD RSP, служба MAC уведомляет верхний уровень, используя ответное сообщение MAC УДАЛИТЬ ПОТОК УСЛУГ. Это проиллюстрировано на рисунке 8.

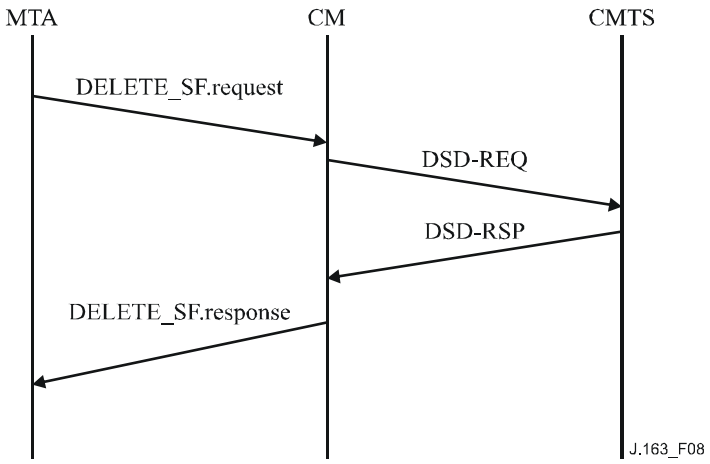


Рисунок 8/J/163 – Удаление резервирования

6.3.4 Рассмотрение случая множественных разрешений на интервал

Добавление пары подпотока

Поскольку в данном DSx-сообщении допускается наличие только одного блока авторизации, то при добавлении классификатора адаптером MTA, последний ДОЛЖЕН использовать значение TLV действия Изменение Динамической Услуги (Dynamic Service Change) (в дополнение к полю статуса подпотока в блоке авторизации), равное 0.

Для того, чтобы добавить пару подпотока, MTA должен выполнить следующие действия:

– Отправить DSC с блоком авторизации, содержащим информацию обо всех шлюзах подпотока.

– Установить поле статуса подпотока для каждого шлюза или в 0 (зарезервировать) или в 1 (зафиксировать).

– Включать в себя классификаторы (восходящего и нисходящего потоков), связанные со шлюзами, включающими значение TLV действия Изменение Динамической Услуги, установленное в 0 – DSC Добавить классификатор. MTA ДОЛЖЕН включать в себя только классификаторы, относящиеся к шлюзу, управляемому полученным сообщением DSC.

– Включать в себя параметры QoS восходящего потока, с числом разрешений на интервал, увеличенным на 1 в случае набора параметров для Допустимого QoS (и, возможно, для набора параметров Активного QoS, если ресурсы еще и фиксируются).

– Обновить параметр LUB для нисходящего QoS для описания всех подпотоков нисходящего потока.

После приема данного DSC CMTS ДОЛЖНА осуществить контроль доступа, как указано в 6.1.3

6.3.4.2 Модифицирование пары подпотока

Когда изменение ресурсов необходимо, MTA НЕ ДОЛЖЕН изменять существующие параметры QoS потока услуг сети DOCSIS. Наоборот, MTA ДОЛЖЕН переместить подпоток к новому потоку услуг или новому подпотоку существующего потока услуг. Для перемещения пары подпотока (обоих потоков, связанные с ID шлюза), MTA ДОЛЖЕН выполнить следующее:

– MTA отправляет DSC-REQ для изменения статуса подпотока на "переместить", устанавливает состояние классификатора в неактивное и отменяет состояние фиксирования для всех активных ресурсов пары подпотока.

– система CMTS посылает DSC-RSP и запускает Допустимый таймер DOCSIS, который ДОЛЖЕН быть установлен в значение таймера T7, задаваемое в GateSet, относящемся к ID шлюза, указанному в DSC-REQ.

– После получения DSC-RSP, MTA посылает DSC-ACK и инициирует перемещение путем отправления либо DSA-REQ (передавая новому потоку услуг), либо DSC-REQ (передавая существующему потоку услуг) для резервирования/фиксирования пару нового потока услуг (с одним и тем же ID шлюза).

– После успешного установления пары нового потока услуг, MTA ДОЛЖЕН немедленно отправить DSQ-REQ для удаления пары старого субпотока
– Если время работы таймера T7 для старого подпотока истекает до получения сообщений DSA-REQ или DSC-REQ с одним и тем же ID шлюза, то система CMTS ДОЛЖНА удалить пару старого подпотока и закрыть шлюз.
– Если таймер T7 для пары старого подпотока заканчивает работу после получения одного из сообщений DSA-REQ или DSC-REQ (с параметрами допустимого QoS) с одним и тем же ID шлюза, но до получения сообщения DSC-REQ, удаляющего пару старого подпотока, то система завершения CMTS ДОЛЖНА удалить старый подпоток и передать шлюз новому потоку.

Удаление пары подпотока

Пары подпотока могут быть удалены как адаптером MTA, так и системой CMTS. Соответствующие процедуры определяются следующим образом:

Инициированные MTA:

Для удаления пары подпотока MTA ДОЛЖЕН выполнить следующее:
– Отправить DSC с блоком авторизации, содержащим информацию обо всех шлюзах подпотока.
– Установить поле статуса подпотока в 2 – "удален" для пары подпотока, который должен быть удален.
– Включить в себя классификаторы (восходящего и нисходящего потока), связанные со шлюзами, для которых TLV действия Изменение Динамической Службы установлено в 2 – DSC Удалить классификатор, для каждого классификатора. MTA ДОЛЖЕН включать только классификаторы, соответствующие шлюзу, управляемому полученным сообщением DSC.
– Включить в себя параметры восходящего QoS с количеством разрешений на интервал, уменьшенным на 1 в случае набора параметров для Допустимого QoS (и, возможно, для набора параметров Активного QoS, если ресурсы были в активном состоянии).
– Заново вычислить LUB для потока в нисходящем направлении, когда поток удален.

После получения данного DSC система завершения CMTS ДОЛЖНА отменить привязку ресурсов, относящихся к данному ID шлюза, удалить шлюз, отправить серверу CMS сообщение Шлюз-Закрыть и послать DSC-RSP.

Инициированные системой CMTS

Если не рассматривать процесс в целом, в отдельных его звеньях возможно возникновение необходимости для системы CMTS отмены привязки ресурсов как восходящем, так и в нисходящем направлении для ID шлюза (к которому относится полученное сообщение Шлюз-Закрыть). Для того чтобы осуществить данную операцию для подпотока, делящего общий поток с подпотоками, продолжающими работать, система CMTS ДОЛЖНА:
– Отправить DSC, содержащее классификаторы (восходящего и нисходящего потоков), относящиеся к шлюзу, где TLV действия Изменить динамическую услугу установлено в 2 – DSC Удалить классификатор, для каждого классификатора.
– Принять параметры восходящего QoS с количеством разрешений на интервал, уменьшенным на 1.
– Пересчитать LUB для случая потока в нисходящем направлении с удаленным потоком.
– После получения DSC MTA ДОЛЖЕН убрать указанный классификатор и отправить DSC-RSP.

Если убирается последний подпоток, то ДОЛЖНО быть использовано сообщение DSD для удаления потока в целом.

6.3.4.4 Объединение потоков услуг

Подпотоки могут добавляться к существующим потокам услуг с использованием механизма, описанного в пункте 6.3.4.1. Вдобавок, подпотоки могут передаваться от существующего потока услуг новому потоку услуг, используя механизм, определенный в 6.3.4.2. Однако для большей простоты процедуры, существующий поток услуг НЕ ДОЛЖЕН передаваться другому существующему потоку услуг в качестве подпотока.

Кроме того, MTA НЕ ДОЛЖЕН пытаться совместно использовать ресурсы потока услуг иначе, как под управлением сервера CMS, через принятие ID ресурса.

7 Описание интерфейса авторизации (pkt-q6)

В данном разделе описаны интерфейсы между системой CMTS и контроллером шлюза для целей авторизации адаптера MTA, чтобы получать высокое качество обслуживания. Для поддержки управления шлюзом и услуги управления допуском IPCablecom требуется сигнализация между контроллером шлюза и системой CMTS. Кроме того, аккуратное выписывание счетов абоненту требует от системы CMTS указания фактического использования "зафиксированных" ресурсов QoS на основе по каждому сеансу. Этот раздел описывает использование протокола COPS для транспортирования сообщений, определенных качеством QoS проекта IPCablecom, между контроллером шлюза и системой CMTS.

7.1 Шлюзы: структура для управления QoS

"Шлюз" динамического QoS проекта IPCablecom представляет собой объект управления политикой, реализованный в системе CMTS, чтобы управлять доступом к расширенным услугам QoS сети DOCSIS с помощью единственного потока IP. Шлюзы являются однонаправленными в том смысле, что единственный шлюз управляет доступом к потоку либо в восходящем направлении, либо в нисходящем направлении. Шлюзы обеспечивают создание классификаторов потоков услуг, которые, в свою очередь, управляют маршрутизацией пакетов к потокам услуг.

Пока шлюз также обладает классификатором, подобным N-кратному классификатору, он не идентичен классификатору. Система CMTS ДОЛЖНА установить шлюз, когда поток авторизован, пока явно не обеспечено завершение авторизации для потока. Классификатор DOCSIS МОЖЕТ быть установлен и связан со шлюзом. Шлюз МОЖЕТ существовать перед тем, как существует классификатор, который он авторизует, и после него. Шлюз МОЖЕТ рассматриваться как точно связанный с нулем, одним или двумя классификаторами.

Система CMTS, соответствующая этой Рекомендации, НЕ ДОЛЖНА динамически создавать классификатор путем обмена сообщением MAC DOCSIS, пока она не уполномочена сделать это путем существования шлюза для такого классификатора. Идентификатор, называемый GateID, связывается со шлюзами. Идентификатор GateID, локальным образом управляемый с помощью системы CMTS, где существуют шлюзы, МОЖЕТ быть связан с одним или более однонаправленными шлюзами. Для сеанса типа "точка-точка" обычно существуют два однонаправленных шлюза, связанных с единственным идентификатором GateID. Кроме того, классификаторы сети DOCSIS существуют для каждого устанавливаемого однонаправленного потока.

7.1.1 Классификатор

Классификатор является шестикратным:

- Направление (Восходящее/Нисходящее).
- Протокол.
- IP источника.
- IP пункта назначения.
- Порт назначения.
- Порт источника.

Если имеется восходящий поток и связанный (часть того же самого сеанса) нисходящий поток, тогда ДОЛЖНЫ существовать отдельные классификаторы для восходящего потока и нисходящего потока. Классификатор обновляется с помощью резервирования, выполняемого для восходящего и нисходящего потоков. Поток данных сеанса ДОЛЖЕН соответствовать классификатору, чтобы получать качество обслуживания, связанное с резервированием.

Система терминалов CMTS ДОЛЖНА использовать фильтры классификации пакетов в восходящем направлении для пакетов услуг IPCablecom. То есть CMTS ДОЛЖНА отбрасывать пакеты восходящего потока, не удовлетворяющие классификаторам восходящих пакетов для потока услуг.

Фильтрация классификации пакетов восходящего потока является необязательным требованием для системы CMTS в сети DOCSIS 1.1. Данная рекомендация требует ее осуществления для потоков услуг, используемых при передаче носителей информации в проекте IPCablecom. Если в CMTS выбрано использование фильтров классификации восходящего потока только для потоков услуг IPCablecom и только для этих потоков, порядок определения отдельных потоков услуг для IPCablecom является вопросом исключительного ведения владельца или продавца услуг CMTS. Например, одним из решений для CMTS могло бы стать использование пакетной классификации восходящего потока только для первичных восходящих потоков услуг.

7.1.2 Шлюз

Шлюз связывается с однонаправленным потоком и включает в себя следующее:

- Идентификатор GateID (ID шлюза).
- Классификатор прототипа.
- Биты различных флагов, описанные ниже.
- Авторизованный диапазон режимов (FlowSpec).
- Зарезервированный диапазон режимов (FlowSpec).
- Идентификатор Resource-ID.

Идентификатор GateID (описываемый ниже) является локальным 32-разрядным идентификатором, который распределяется из местного пространства в системе CMTS, где находится шлюз. Один и тот же идентификатор GateID (ID шлюза) МОЖЕТ использоваться двумя шлюзами. Обычно идентификатор GateID (ID шлюза) будет указывать единственный поток восходящего потока и единственный поток нисходящего потока и соответствовать единственному мультимедийному сеансу.

Классификатор прототипа состоит из тех же самых шести элементов, что и классификатор, описанный выше. IP источник является адресом IP (как видится в системе CMTS) инициатора потока. В случае шлюза восходящего потока на канале DOCSIS, IP источника является адресом IP местного адаптера MTA. Для нисходящего потока адрес IP источника является адресом IP удаленного адаптера MTA. Для выбранных параметров классификатора прототипа шлюза разрешается групповой символ. В сигнализации мультимедийного вызова порт источника UDP не сообщается, поэтому его значение не должно считаться частью информации шлюза.

Порт источника МОЖЕТ быть трафаретным символом, чтобы поддерживать оба протокола сигнализации вызова IPCablecom (DCS и Рекомендация J.162). Если порт источника является трафаретным символом, его значение в параметрах шлюза будет нулем.

Авторизованные и зарезервированные диапазоны режимов представляют собой части FlowSpecs RSVP (оба T-Spec или R-Spec), как описывается в предыдущих разделах.

Запрос на резервирование ресурсов (как указывается в сообщении Добавить/Изменить динамический поток услуг) ДОЛЖЕН быть проверен по сравнению с тем, что был авторизован для идентификатора GateID (ID шлюза), связанного с направлением для запроса ресурса. Авторизованные ресурсы указываются в авторизованном диапазоне режимов. Проверяется также групповой символ в шлюзе для конкретных записей.

Идентификатор Resource-ID является локальным 32-разрядным идентификатором, который распределяется из местного пространства в системе CMTS, где располагается шлюз. Любое количество шлюзов МОЖЕТ совместно использовать идентификатор resource-ID, и поэтому совместно используют общий набор ресурсов, с ограничением, что только один из этих шлюзов в каждом направлении зафиксировал ресурсы.

7.1.3 Идентификация шлюза

Идентификатор GateID является уникальным идентификатором, который распределяется локальным образом системой CMTS, где располагается шлюз. Идентификатор GateID является 32-разрядным идентификатором. Идентификатор GateID МОЖЕТ быть связан с одним или более шлюзами. В обоих протоколах сигнализации J.162 и DCS, идентификатор GateID (ID шлюза) связывается с каждой фазой вызова и состоит из единственного шлюза восходящего потока и единственного шлюза нисходящего потока.

Идентификатор GateID (ID шлюза) ДОЛЖЕН быть связан со следующей информацией:

- Один или два шлюза, которые ДОЛЖНЫ быть одним из следующих сочетаний:
  - Единственный шлюз восходящего потока.
  - Единственный шлюз нисходящего потока.
  - Единственный шлюз восходящего потока и единственный шлюз нисходящего потока.
- Информация ведения учета и выписки счетов.
  - Адрес: Порт сервера хранения первичных записей (Primary Record-Keeping-Server), которому следует получать записи событий.
  - Адрес: Порт сервера хранения вторичных записей, для использования, если первичная запись не доступна.
  - Флаг, указывающий, должны ли быть посланы в реальном времени сообщения о событиях к серверу хранения записей, или они должны объединяться и посылаться на периодических интервалах.
  - Идентификатор Billing-Correlation-ID [идентификатор-корреляции-выписки-счетов], который передается далее к серверу хранения записей, с каждой новой записью события.
  - Дополнительная информация о выписке счетов, если поставляется, будет использована для порождения сообщений о событиях Call-Answer [ответ-на-вызов] и Call-Disconnect [вызов-рассоединить].
  - Информация о генерации нового события (Event Generation Info Object) пропускается; это означает что для шлюза НЕ ДОЛЖНО осуществляться генерирование сообщения о событии

Идентификатор GateID (ID шлюза) ДОЛЖЕН быть уникальным среди всех текущих шлюзов, распределенных системой CMTS. Значение 32-разрядного числа НЕ СЛЕДУЕТ выбирать из набора малых целых чисел, поскольку обладание значением GateID является ключевым элементом в установлении подлинности сообщений Commit (зафиксировать) от адаптера MTA. Алгоритм, который МОЖЕТ быть использован для назначения значений идентификаторов GateID, является следующим: разделение 32-разрядного слова на две части, на индексную часть и на случайную часть. Индексная часть определяет шлюз путем индексации в малой таблице, в то время как случайная часть оставляет значению некоторый уровень неопределенности. Независимо от выбранного алгоритма, системе CMTS ЖЕЛАТЕЛЬНО попытаться минимизировать возможность неоднозначностей в использовании ID шлюза, обеспечив невозможность использования IDшлюза в течение трех минут с момента его предыдущего закрытия или удаления. Для алгоритма, предложенного ранее, это можно осуществить, просто увеличивая индексную часть каждого следующего назначаемого ID шлюза, вновь обращая его в ноль по достижении максимально возможного значения индексой части.

7.1.4 Диаграмма переходного состояния шлюза

Считается, что шлюзы должны иметь следующие состояния:

- Распределенное – Начальное состояние шлюза, созданное при запросе GC.
- Авторизованное – GC авторизовал поток с определенными пределами ресурсов.
- Зарезервированное – Для потока были зарезервированы ресурсы.
- Зафиксированное – Ресурсы используются.

Система CMTS ДОЛЖНА поддерживать состояния шлюзов и переходы, как показано на рисунке 9 и описано в этом разделе. Все шлюзы, которым системой CMTS назначен тот же самый идентификатор GateID (ID шлюза), ДОЛЖНЫ перейти вместе через состояния, показанные на рисунке 9. Это остается справедливым даже в том случае, когда один из восходящих/нисходящих потоков получает разрешение пройти в трафике. В интересах простоты диаграмма переходов для шлюза на рисунке 9 не описывает полностью все переходы, которые должны быть выполнены, хотя все указанные на рисунке переходы должны происходить в строгом соответствии с рисунком.

Шлюз создается в системе CMTS либо с помощью команды GateAlloc, либо с помощью команды GateSet [шлюз-установить] от контроллера GC. Во всех случаях система CMTS распределяет локальным образом уникальный идентификатор, называемый GateID (ID шлюза), который возвращается к контроллеру GC. Если шлюз создается с помощью сообщения GateSet, то тогда

система CMTS ДОЛЖНА отметить шлюз в состоянии "авторизованное" и ДОЛЖНА запустить таймер T1. Если шлюз был создан с помощью сообщения GateAlloc, то тогда система CMTS ДОЛЖНА отметить шлюз в состоянии "распределенное", запустить таймер T0 и ДОЛЖНА ожидать команду GateSet, в точке которой шлюз ДОЛЖЕН быть отмечен в состоянии "авторизованное". Если таймер T0 заканчивает работу со шлюзом в состоянии "распределенное", или таймер T1 заканчивает работу со шлюзом в состоянии "авторизованное", тогда система CMTS ДОЛЖНА исключить шлюз. Таймер T0 ограничивает количество времени, в котором идентификатор GateID (ID шлюза) будет оставаться действительным без каких-либо указанных параметров шлюза. Таймер T1 ограничивает количество времени, в течение которого авторизация будет оставаться действующей.

Шлюз в состоянии "Распределенное" ДОЛЖЕН быть удален после получения сообщения Шлюз – Удалить. Когда это произойдет, система CMTS ДОЛЖНА ответить сообщением Gate-Delete-Ack и ДОЛЖНА остановить таймер T0. Аналогично, шлюз в состоянии "авторизован" ДОЛЖЕН быть удален по получении сообщения Шлюз – Удалить. Когда это произойдет, система завершения CMTS ДОЛЖНА ответить сообщением Gate-Delete-Ack и ДОЛЖНА остановить таймер T1.

Шлюз в состоянии "авторизованное" ожидает, что абонент сделает попытку зарезервировать ресурсы. Абонент осуществляет это через сообщение интерфейса управляющих служб MAC. При получении этого запроса на резервирование система CMTS ДОЛЖНА проверить, что запрос находится в пределах, установленных для шлюза, и выполнить процедуры управления доступом.

Система CMTS ДОЛЖНА осуществлять, по меньшей мере, две политики управления доступом, одна для нормальной голосовой связи, а другая для срочной связи. Эти две политики ДОЛЖНЫ иметь устанавливаемые параметры, которые, как минимум, указывают:

1) максимальное количество ресурсов, что может быть распределено не только исключительно сеансам этого типа (которое может составлять 100% пропускной способности);
2) количество ресурсов, что может быть распределено исключительно сеансам этого типа (которое может составлять 0% пропускной способности); и
3) максимальное количество ресурсов, что может быть распределено сеансам обоих типов.

Политика управления доступом МОЖЕТ также указывать, может ли новый сеанс такого типа "брать в долг" от классов низшего приоритета, или следует выгрузить некоторый существующий сеанс другого типа, чтобы удовлетворять установкам политики управления доступом.

Если запрос о резервировании направлен на присоединении подпотока к существующему потоку услуг, то ID класса сеанса для шлюза ДОЛЖЕН соответствовать ID класса сеанса шлюзов всех остальных подпотоков, которые уже составляют данный существующий поток услуг. В случае несовпадения с классами сеанса шлюзов остальных подпотоков, CMTS ДОЛЖНА отвергнуть запрос о резервировании.

Если процедуры управления доступом являются успешными и запрашивается только резервирование ресурсов, то шлюз ДОЛЖЕН быть отмечен в "зарезервированном" состоянии. Если процедуры управления доступом являются успешными и запрашивалось одноступенчатое резервирование и фиксация ресурсов, шлюз ДОЛЖЕН быть помечен в "зафиксированном" состоянии, а система CMTS ДОЛЖНА послать сообщение Шлюз – Открыть к контроллеру GC и остановить таймер T1

Если процедуры управления доступом не являются успешными шлюз ДОЛЖЕН оставаться в "авторизованном" состоянии. Отметим, что фактическое резервирование, сделанное абонентом, может быть меньше, чем то, которое авторизовано, например, резервирование только для восходящего потока, когда пара шлюзов была установлена, авторизуя восходящие и нисходящие потоки.

В "зарезервированном" состоянии шлюз ожидает, что абонент зафиксирует ресурсы, таким образом активизируя их.. Команда Commit (зафиксировать) от абонента является успешной транзакцией запроса, активизирующей поток услуг через интерфейс управляющих служб MAC. Если шлюз все еще находится в "зарезервированном" состоянии, а таймер T1 заканчивает работу (т. е. абонент не отдает команду Commit (зафиксировать)), система CMTS ДОЛЖНА разблокировать любые зарезервированные ресурсы и удалить шлюз. Если в "зарезервированном" состоянии получена команда Шлюз – Удалить, система терминалов CMTS ДОЛЖНА ответить сообщением Gate-Delete-Ack, ДОЛЖНА разблокировать все ресурсы, относящиеся к шлюзу и ДОЛЖНА остановить таймер T1.

При изображении на диаграмме переходов для данного состояния, будем считать, что сообщение "Зафиксировать" пришедшее от абонента фиксирует поток в восходящем направлении. Если

системой CMTS получен ассиметричный запрос, такой, что трафик может проходить в нисходящем направлении, но не может в направлении восходящего потока, система CMTS НЕ ДОЛЖНА выходить из состояния "Зарезервировано".Если, с другой стороны, CMTS получает ассиметричный запрос такого рода, что трафик может проходить в направлении восходящего потока, но не нисходящего, то CMTS ДОЛЖНА рассматривать данный запрос как запрос "Зафиксировать" и должна изменить свое состояние в соответствии с описанием, приведенным ниже.

При изображении на диаграмме состояния "Удалить", будем считать, что сообщение "Удалить" со стороны абонента удаляет поток восходящего потока. Если CMTS получает ассиметричный запрос при котором удаляется только поток нисходящего потока, но не нисходящего потока, система CMTS НЕ ДОЛЖНА выходить из наличного состояния. Если, с другой стороны, CMTS получает ассиметричный запрос такого рода, что удаляется поток восходящего потока, но не нисходящего, CMTS ДОЛЖНА рассматривать запрос, как запрос вида "Удалить"в соответствии с правилами перехода для шлюза.

Если таймер T0 системы CMTS заканчивает работу до получения ею от CMS команды Шлюз-Установить, CMTS ДОЛЖНА инициировать сообщение Шлюз-Закрыть используя в качестве кода причины "Завершение работы таймера T0; от CMS не получена команда Шлюз-Установить") и удалить соответствующий шлюз.

Если таймер T1 в CMTS завершает работу до получения от MTA команды "Зафиксировать", то система CMTS ДОЛЖНА высвободить все зарезервированные ресурсы, связанные с соответствующим ID шлюза, инициировать отправление сообщения Шлюз-Закрыть с кодом причины "Завершение работы таймера T1; отсутствие команды "Зафиксировать" от MTA " и удалить соответствующий шлюз (шлюзы).

Если в состоянии "Зарезервировано" CMTS получает от абонента команду "Зафиксировать", CMTS ДОЛЖНА отметить шлюз в состоянии "зафиксированный" остановить таймер T1, и инициировать сообщение Шлюз-Открыть.

Если время таймера T7 истекает в момент использования адаптером MTA многократных разрешений на интервале и любой подпоток потока услуг, связанный со шлюзом (шлюзами) через ссылку соответствующего ID шлюза, не был зафиксирован в системе CMTS, CMTS ДОЛЖНА инициировать сообщение Шлюз-Закрыть, используя код причины "Истечение времени таймера T7; таймаут резервирования потока услуг" и удалить соответствующий шлюз (шлюзы). В противном случае, CMTS ДОЛЖНА установить для зарезервированного диапазона режимов значение, равное зафиксированному диапазону режимов для потоков, связанных со шлюзами через ссылки соответствующих ID шлюзов.

Если время таймера T7 истекает в тот момент, когда MTA не использует многократные разрешения на интервал и поток услуг, связанный со шлюзом (шлюзами) через ссылку соответствующего ID шлюза, не был зафиксирован в системе CMTS, CMTS ДОЛЖНА инициировать сообщение Закрыть шлюз, используя код причины "Истечение времени таймера T7; таймаут резервирования потока услуг" и удалить соответствующий шлюз (шлюзы). В противном случае, CMTS ДОЛЖНА установить для зарезервированного диапазона режимов значение, равное зафиксированному диапазону режимов для потоков, связанных со шлюзами через ссылки соответствующих ID шлюзов.

Если время работы таймера T8 истекает в системе CMTS из-за неактивности потока услуг, CMTS ДОЛЖНА инициировать сообщение Шлюз-Закрыть для каждого шлюза, связанного с потоком, используя код причины "Истечение времени таймера T8, неактивность потока услуг, в направлении восходящего потока" и удалить соответствующий шлюз.

Будучи в состоянии "зафиксированное", шлюз достиг стабильной конфигурации. Ресурсы были активизированы на местных шлюзах. Ресурсы будут продолжать оставаться активированными до тех пор, пока любой из местных абонентов не отправит команду Release (освободить), не истечет время таймера Активного состояния или сервер CMS не отдаст команду Шлюз-Удалить.

Если, в состоянии "зафиксированное", система CMTS получает команду Release от абонента либо через интерфейс управляющих служб MAC, либо из-за неудачи клиента обновить резервирование, или от внутренних механизмов DOCSIS, которые обнаруживают неудачу клиента, то система CMTS ДОЛЖНА деактивировать все ресурсы, зафиксированные для абонента, освободить все

зарезервированные ресурсы, инициировать сообщение GateClose к объекту координации шлюза и исключить шлюз.

Будучи в состоянии "зафиксированное", система CMTS ДОЛЖНА позволить клиенту инициировать изменения в резервировании или активизации ресурса в рамках пределов авторизации и местного управления допуском.

7.1.5 Координация шлюза

Сообщения координации работы шлюза интерфейса управления шлюзом COPS, Шлюз-Открыть и Шлюз-Закрыть обеспечивают механизм незапрашиваемой обратной связи между системой CMTS и сервером CMS с целью синхронизации их работы. Это особенно полезно в случае преждевременной инициализации адаптером MTA запроса о резервировании или фиксации ресурса, не вызванного командой CMS, или в случае сбоя в работе MTA, вызвавшего восстановление ресурса в системе CMTS. В обоих этих возможных случаях внутреннее состояние, содержащееся в памяти CMS, будет обновлено, чтобы правильно отражать изменение состояния системы CMTS, и CMS, основываясь на этой информации, сможет действовать сообразно ситуации.

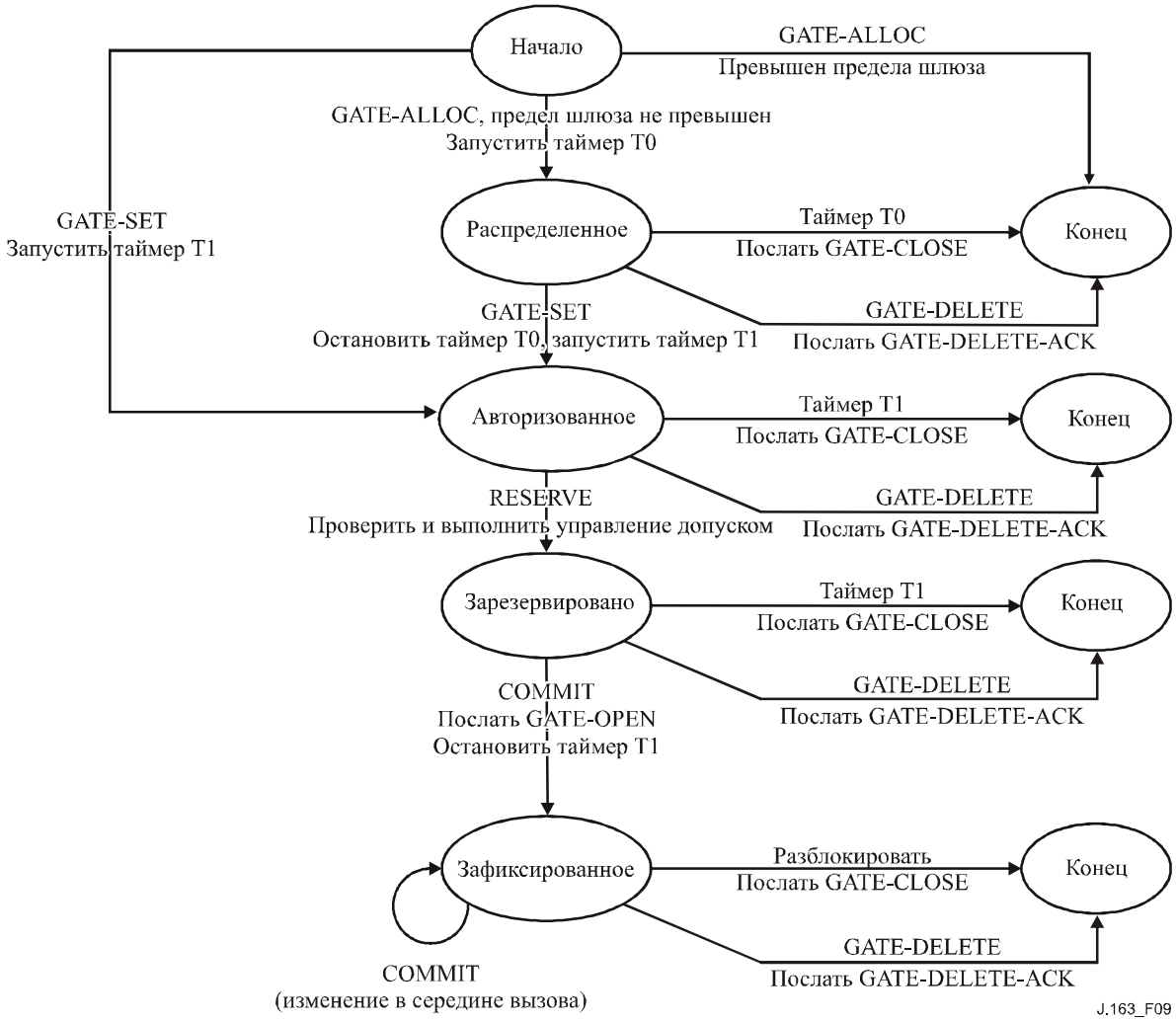


Рисунок 9/J.163 – Диаграмма переходного состояния шлюза

7.2 Профиль COPS для проекта IPCablecom

Управление допуском QoS в протоколе IP является актом управления распределением ресурса QoS, основанным на административных политиках и доступном ресурсе. Услуга управления допуском QoS протокола IP использует архитектуру клиент/сервер. Операционные модули верхнего уровня отображены на рисунке 10. Административные политики хранятся в качестве базы данных политики и управляются сервером COPS. В то время как типовая реализация IntServ из COPS имеет сервер для определения доступных ресурсов, реализация DiffServ толкает политику к клиенту таким образом, чтобы клиент мог принимать решения по управлению доступом.

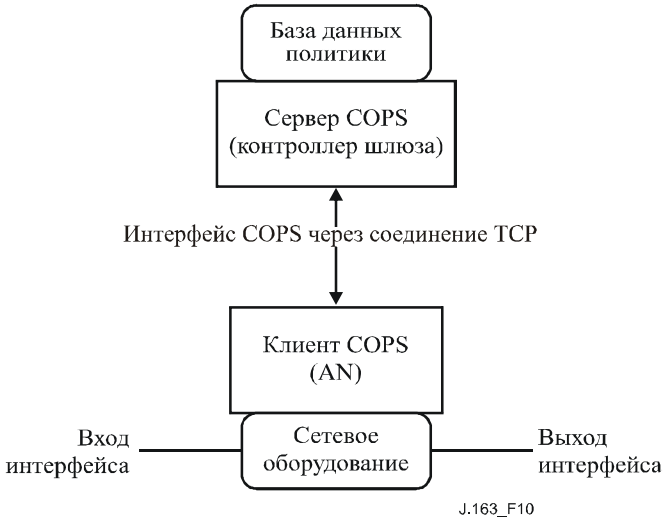


Рисунок 10/J.163 – Схема управления доступом QoS

Решения по управлению доступом QoS, сделанные сервером COPS, ДОЛЖНЫ быть переданы клиенту COPS, используя COPS. Клиент COPS МОЖЕТ делать запросы по управлению доступом QoS к серверу COPS, основанные на сетевых событиях, запущенных или протоколом сигнализации QoS, или через механизмы обнаружения потока. Сетевое событие может также быть необходимым для управления полосой пропускания QoS, например, когда интерфейс, способный к новому качеству QoS, становится действующим.

Решения политики QoS, принятые сервером COPS, МОГУТ быть продвинуты к клиенту COPS на основе внешнего, внеполосного запроса услуги QoS, например запроса от завершающего системы CMTS или контроллера шлюза. Эти решения политики МОГУТ быть сохранены клиентом COPS в точке принятия решения местной политики, и система CMTS может обращаться к такой решающей информации, чтобы принять решения по управлению доступом по входящим запросам сеанса, полученным в системе CMTS.

Поддержка взаимодействия "клиент COPS–сервер COPS" для управления доступом QoS обеспечивается протоколом COPS IETF. Протокол COPS включает в себя следующие операции:

- Client-Open [клиент-открыть] (OPN)/Client-Accept [клиент-принять] (CAT)/Client-Close [клиент-закрыть] (CC). Клиент COPS посылает сообщение OPN, чтобы инициировать соединение с сервером COPS, а сервер откликается сообщением CAT, чтобы принять соединение. Сервер посылает сообщение CC для завершения соединения с клиентом.
- Запрос (REQ). Клиент COPS посылает сообщение REQ к серверу, чтобы запросить информацию решения по управлению доступом или информацию по конфигурации устройства. Сообщение REQ может содержать информацию, характерную для клиента, которую сервер использует вместе с данными базы данных политики допуска к сеансу, чтобы принимать решения, основанные на политике.
- Решение (DEC). Сервер откликается на запросы REQ, отсылая обратно DEC клиенту, что инициировал исходный запрос. Сообщения DEC могут быть посланы в отклике на запрос REQ (т. е. запрашиваемое решение DEC) или в любое время после изменения/обновления предыдущего решения (т. е. незапрашиваемое решение DEC).
- Состояние информирования (RPT). Клиент COPS посылает сообщение RPT к серверу COPS, указывая изменения к запросу состояния в клиенте COPS. Клиент COPS посылает это, чтобы проинформировать сервер COPS о фактическом ресурсе, зарезервированном после того, как серверу COPS был дан допуск. Клиент COPS также может использовать информирование [Report], чтобы периодически информировать сервер COPS о текущем состоянии клиента COPS.
- Исключить запрос состояния (DEL). Клиент COPS посылает сообщение DEL к серверу COPS, чтобы запросить очистку состояния запроса. Это может быть результатом освобождения ресурса QoS клиентом COPS.

- Сохранять действующим (KA). Посылается как клиентом COPS, так и сервером COPS для обнаружения неудачи связи.
- Синхронизировать запрос состояния (SSR)/Состояние синхронизации сделано (SSC). Сообщение SSR посылается сервером COPS, запрашивающим текущую информацию о состоянии клиента COPS. Клиент повторно выпускает вопросы запросов к серверу, чтобы осуществлять синхронизацию, а затем клиент посылает сообщение SSC, чтобы указать, что синхронизация сделана. Поскольку контроллер GC не обладает состоянием, операции SSR/SSC не имеют никакого значения в проекте IPCablecom и не используются системой CMTS или контроллером GC.

Внутри архитектуры IPCablecom контроллер шлюза является объектом точки решения политики COPS (PDP), а система CMTS является объектом точки принуждения политики COPS (PEP).

Подробности протокола COPS предоставляются в документе RFC 2748. Этот документ RFC предоставляет описание основного протокола COPS, не зависящего от типа пользователя. Дополнительные проекты предоставляют информацию для использования COPS для интегрированных услуг с RSVP и для дифференцированных услуг (т. е. обеспечивающих пользователей). Более подробный обзор протокола COPS предоставляется в виде информации в Приложении X.

7.3 Форматы сообщений в протоколе управления шлюзом

Сообщения протокола для управления шлюзом транспортируются внутри сообщений протокола COPS. Услуга COPS использует соединение TCP, установленное между системой CMTS и контроллером шлюза, и использует механизмы, указанные в Рекомендации МСЭ-Т J.170, чтобы защитить тракт связи.

7.3.1 Общий формат сообщения COPS

Каждое сообщение COPS состоит из заголовка COPS, за которым следует ряд типизированных объектов. Контроллер GC и система CMTS ДОЛЖНЫ поддерживать обмен сообщениями COPS, как определяется ниже (см. рисунок 11).

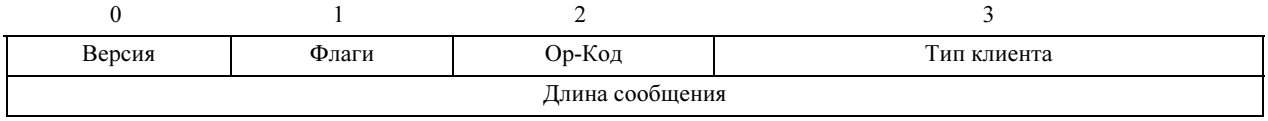


Рисунок 11/J.163 – Общий заголовок сообщения COPS

Версия является 4-разрядным полем, дающим текущий номер версии COPS. Это ДОЛЖНО быть установлено в 1.

Флаг является 4-разрядным полем. Комбинация 0x1 является флагом запрашиваемого сообщения. Когда сообщение COPS посылается в отклике на другое сообщение (например, запрашиваемое решение, посланное в отклике на запрос), этот флаг ДОЛЖЕН быть установлен в 1. В других случаях (например, при незапрашиваемом решении) флаг НЕ ДОЛЖЕН быть установлен (значение = 0). Все другие флаги ДОЛЖНЫ быть установлены в нуль.

Ор-код является 1-байтным полем, которое дает возможность выполнить операцию COPS. Операциями COPS, используемыми в этой спецификации IPCablecom, являются:

1 = Request [Запрос] (REQ)
2 = Decision [Решение] (DEC)
3 = Report-State [Информирование- состояние] (RPT)
6 = Client-Open [Клиент-открыть] (OPN)
7 = Client-Accept [Клиент-принять] (CAT)
9 = Keep-Alive [Сохранить-действующим] (KA)

Тип клиента является 16-разрядным идентификатором. Для использования в проекте IPCablecom тип клиента ДОЛЖЕН быть установлен в клиента IPCablecom (0x8008). Для сообщений Keep-Alive (Ор-код = 9), тип клиента ДОЛЖЕН быть установлен в нуль, поскольку KA используется, скорее, для проверки соединения, чем для проверки сеанса каждого клиента.

Длина сообщения составляет 32-разрядное значение, давая размер сообщения в октетах. Сообщения ДОЛЖНЫ быть выровнены на 4-байтных границах, поэтому длина ДОЛЖНА быть кратна четырем.

Следующим за общим заголовком COPS является изменяющееся число объектов. Все объекты следуют тому же самому формату объекта, каждый объект состоит из одного или более 32-разрядных слов с заголовком из четырех октетов, используя следующий формат (см. рисунок 12):

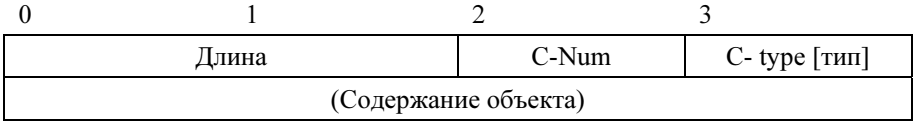


Рисунок 12/J.163 – Общий формат объекта COPS

Длина является значением из двух октетов, которое ДОЛЖНО давать число октетов (включая заголовок), что составляют объект. Если длина в октетах не кратна четырем, то к концу объекта ДОЛЖНА быть добавлена вставка таким образом, что он выравнивается до следующей 32-разрядной границы. На приемной стороне граница последующего объекта ДОЛЖНА быть найдена путем округления ранее установленной длины объекта до следующей 32-разрядной границы.

C-Num определяет класс информации, содержащейся в объекте, а C-type определяет подтип версии для информации, содержащейся в объекте. Стандартные объекты COPS (как определено в RFC 2748), используются в этой спецификации, и их значениями C-num являются:

1 = Handle [дескриптор]

6 = Decision [решение]

8 = Error [ошибка]

9 = Client Specific Info [информация, характерная для клиента]

10 = Keep-Alive-Timer [сохранять-таймер-действующим]

11 = PEP Identification [идентификация]

7.3.2 Дополнительные объекты COPS для управления шлюзом

Как с типами клиентов COPS-PR и COPS-RSVP, тип клиента IPCablecom определяет количество форматов объектов. Эти объекты ДОЛЖНЫ быть размещены в объекте Decision, C-Num = 6, C-Type = 4 (данные решения, характерные для клиента), когда перенесены от контроллера GC к системе CMTS в сообщении решения. Они ДОЛЖНЫ также быть помещены в объекте ClientSI, C-Num = 9, C-Type = 1 (сигнализируемый клиент SI), когда переносятся от системы CMTS к контроллеру GC в сообщении Report. Они кодируются подобно объектам, характерным для клиента, для COPS-PR; подробные схемы кодирования появятся ниже. Как в COPS-PR, эти объекты нумеруются, используя номерное пространство, характерное для клиента, которое является не зависящим от номерного пространства высокоуровневого объекта COPS. По этой причине номера и типы объектов даются, соответственно, как S-Num и S-Type.

Дополнительными объектами COPS, определенными для использования проектом IPCablecom, являются следующие:

7.3.2.1 Идентификатор транзакции Transaction-ID

Идентификатор Transaction-ID [транзакция] содержит маркер, который используется контроллером GC, чтобы согласовать отклики от системы CMTS на предыдущие запросы, а также тип команды, который определяет действие, которое должно быть предпринято, или отклик.

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

Идентификатор транзакции является 16-разрядным числом, которое МОЖЕТ быть использовано контроллером GC для согласования откликов на команды.

Тип команды шлюза ДОЛЖЕН быть одним из следующих:

Gate-Alloc	1
Gate-Alloc-Ack	2
Gate-Alloc-Err	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
Gate-Open	13
Gate-Close	14

7.3.2.2 Идентификатор абонента Subscriber-ID

Идентификатор Subscriber-ID [абонент] определяет абонента для запроса этой услуги. Его главное использование заключается в предотвращении различных атак типа "отказ в обслуживании".

Длина = 8	S-Num = 2	S-Type = 1
Адрес IPv4 (32 бита)		

или

Длина = 20	S-Num = 2	S-Type = 2
Адрес IPv6 (128 битов)		

7.3.2.3 Идентификатор GateID (ID шлюза)

Этот объект определяет шлюз или набор шлюзов, упоминаемых в сообщении команды или назначенных системой CMTS для сообщения отклика.

Длина = 8	S-Num = 3	S-Type = 1
Идентификатор GateID (ID шлюза) (32 бита)		

7.3.2.4 Activitycount (подсчет активности)

При использовании в сообщении GateAlloc, этот объект указывает максимальное количество шлюзов, которые могут быть одновременно распределены к указанному идентификатору subscriber-ID. Этот объект возвращает, в сообщении GateSetAck или GateAllocAck, количество шлюзов, назначенных единственному абоненту. Он является полезным в предотвращении атак типа "отказ в обслуживании".

Длина = 8	S-Num = 4	S-Type = 1
Счет (32 бита)		

7.3.2.5 Gate-spec

Длина = 60		S-Num = 5	S-Type = 1
Направление	Идентификатор ID протокола	Флаги	Класс сеанса
Адрес IP источника (32 битовый)			
Адрес IP пункта назначения (32 битовый)			
Порт источника (16 битовый)		Порт назначения (16 битовый)	
Точка кода DiffServ (DSCP)			
Значение таймераT1		Зарезервировано	
Значение таймера T7		Значение таймера T8	
Скорость маркерной области памяти [r] (32 битовое число IEEE с плавающей точкой)			
Размер маркерной области памяти [b] (32 битовое число IEEE с плавающей точкой)			
Пиковая скорость данных (p) (32 битовое число IEEE с плавающей точкой)			
Минимальный наблюдаемый элемент [m] (32 битовое целое число)			
Максимальный размер пакета [M] (32 битовое целое число)			
Скорость [R] (32 битовое число IEEE с плавающей точкой)			
Пассивный член [S] (32 битовое целое число)			

Направление – или 0 для шлюза нисходящего потока, или 1 для шлюза восходящего потока.

Идентификатор ProtocolID представляет значение для согласования в заголовке IP, или нуль при отсутствии согласования.

Флаги определяются следующим образом:

0x01 Auto-Commit and Commit-Not-Allowed – функциональность, которая ранее указывалась с помощью поля флагов, теперь не играет никакой роли. В результате, биты 1 и 2 резервируются.

Остальные флаги ДОЛЖНЫ быть нулями.

Класс сеанса определяет надлежащую политику управления допуском или параметры, подлежащие применению для этого шлюза. Разрешенными значениями являются:

0x00 Не указанное.

0x01 Сеанс VoIP нормального приоритета.

0x02 Сеанс VoIP высокого приоритета (например, E911).

Все другие значения в настоящее время резервируются.

Адрес IP источника и адрес IP пункта назначения являются парой 32-разрядных адресов IPv4, или нулем при отсутствии согласования (т. е. спецификация трафаретного символа, которая будет согласовывать любой запрос от адаптера MTA).

Порт источника и порт пункта назначения определяют пару 16-разрядных значений, или нуль при отсутствии согласования.

Значения r, b, p, m, M, и R таковы, как описано в 6.1. Вместо определенного в RFC пассивного члена RSVP, значение S представляет собой минимально допустимое дрожание разрешений в восходящем направлении, выраженное в микросекундах и минимально допустимую задержку в нисходящем направлении.

В других разделах приводятся нормативные требования с соответствующими ограничениями для диапазона режимов авторизации, определяемого вышеуказанными параметрами. В частности, обсуждение в разделе 5.6.10 помогает определить верхнюю границу диапазона режимов авторизации,

в то время, как в разделе 7.5 получен набор минимальных требований к вышеуказанным параметрам. Категорически рекомендуется, чтобы использование серверов ограничивало параметры авторизации, поскольку данные параметры являются основополагающими для выработки и реализации политики управления полосой пропускания поставщика услуг.

Поле DS определяется следующей структурой:

0	1	2	3	4	5	6	7
Кодовая точка дифференцированных услуг (DSCP)						Не используется	Не используется

В документе RFS 2474 определено, что Поле дифференцированных услуг должно быть двухчастной битовой маской, состоящей из 6-битового DSCP и 2-х зарезервированных битов. RFC-3168 определяет, что 2 зарезервированных бита должны быть использованы для ECN (*нотификации разбить скопление*). Эти биты используются маршрутизаторами для разбиения скопления (вызовов) и активного управления очередью. CMS ДОЛЖЕН установить биты 6 и 7 в поле DS в ноль. Иначе, система цмтс ДОЛЖНА ответить на сообщение Gate-Set сообщением Gate-Set-Error с кодом ошибки 8 (недопустимое значение поля DS)

Для обратной совместимости с текущими реализациями систем и использования старшинства IP, как определено в документах RFC 2474 IETFи RFC 791 IETF, соответствующие биты байта TOS IPv4, показанные ниже, МОГУТ быть вставлены в поле DS. Однако по-прежнему применяются условия для установки значений битов 6 и 7. Поле TOS IP (биты 3-6) не поддерживается в сетях DiffServ.

0	1	2	3	4	5	6	7
Старшинство IP			IPv4 IP TOS				Не используется

Таймер T1 задается в секундах и используются в диаграмме перехода шлюза, описанной в 7.1.4. Если в единственном сообщении COPS появляются многократные объекты Gate Spec, то значения T1 ДОЛЖНЫ быть идентичны во всех появлениях Gate Spec. Если значения T1 различны для объектов Gate Spec восходящего и нисходящего потоков, система CMTS ДОЛЖНА для управления парой шлюзов использовать значение T1, определенное в объекте Gate Spec восходящего потока.

Таймеры T7 и T8 являются значениями, заданными в секундах и используются для управления временем ожидания (таймаутом) для параметров Допустимого качества QoS и параметров Активного качества QoS соответственно.

7.3.2.6 Remote-Gate-Info

Этот объект более недействителен. Для предотвращения неправильной интерпретации зарезервирован S-Num 6.

Длина 36	S-Num = 6	S-Type = 1
IP-адрес CMTS (32 бита)		
Порт CMTS (16 битов)	Флаги, определенные ниже	
ID удаленного шлюза		
Алгоритм	Зарезервировано	
Ключ безопасности (16 байтов)		

7.3.2.7 Event-Generation-Info

Объект содержит всю информацию, необходимую для поддержки сообщений о событиях, как указано и требуется в Рекомендации МСЭ-Т J.164.

Длина = 44	S-Num = 7	S-Type = 1
Primary-Record-Keeping-Server-IP-Address (32 бита)		
Primary-Record-Keeping-Server-Port	Флаги, см. ниже	Зарезервировано
Secondary-Record-Keeping-Server-IP-Address (32 бита)		
Secondary-Record-Keeping-Server-Port	Зарезервировано	
Идентификатор Billing-Correlation-ID (24 байта)		

Primary-Record-Keeping-Server-IP-Address [IP-адрес-сервера-хранения-первичной-записи] является адресом хранителя записей, к которому посылаются записи о событиях.

Primary-Record-Keeping-Server-Port [порт-сервера-хранения-первичной-записи] является номером порта для посланных записей событий.

Значения флагов являются следующими:

0x01 Индикатор обработки группы. Если он установлен, система CMTS ДОЛЖНА накапливать записи о событиях в качестве части группового файла и посылать к серверу хранения записей, на периодических интервалах. Если он не установлен, то система CMTS ДОЛЖНА посылать записи о событиях к серверу хранения записи в реальном времени.

Остальная часть резервируется и ДОЛЖНА быть нулем.

Secondary-Record-Keeping-Server-IP-Address [IP-адрес-сервера-хранения-вторичной-записи] является адресом вторичного хранителя записи, к которому посылаются записи, если первичный сервер хранения записей является недоступным.

Secondary-Record-Keeping-Server-Port является номером порта для посланных записей событий.

Идентификатор Billing-Correlation-ID [корреляция-выписки-счетов] является идентификатором, назначенным сервером CMS для всех записей, относящихся к этому сеансу.

7.3.2.8 Media-Connection-Event-Info

Данный объект более не требуется. Для предотвращения неправильной интерпретации зарезервировано S-Num 8.

7.3.2.9 IPCablecom-Reason

В данном объекте содержится описание причины, по которой шлюз исключается.

Длина = 8	S-Num = 13	S-Type = 1
Код причины	Подкод причины	

Ниже указаны значения Кода причины, определенные в данной Рекомендации:

0: Операция Gate-Delete

1: Операция Gate-Close

Подкоды причины определяются следующим образом:

Операция Gate-Delete:

0 = Нормальный режим работы (Normal operation)

1 = Координация местного шлюза не завершена

2 = Координация удаленного шлюза не завершена

3 = Авторизация отменена

4 = Неожидаемое открытие шлюза

5 = Неудача действия Закрыть местный шлюз (Local Gate-Close)

127 = Иная ошибка, не определенная выше.

Операция Gate-Close:

0 = Освобождение ресурсов, инициированное клиентом (нормальный режим работы).

1 = Переопределение резервирования (например, для приоритетного сеанса)

2 = Недостаток поддержки резервирования (например, обновления интерфейсов Служб управления MAC)

3 = Недостаточность ответов уровня MAC сети DOCSIS (например поддержки станции)

4 = Истечение таймера T0 при неполучении Gate-Set от CMS

5 = Истечение таймера T1 при неполучении Commit от MTA

6 = Истечение таймера T7; время ожидания резервирования (таймаут) Service Flow

7 = Истечение таймера T8 ; неактивность Service Flow в восходящем направлении

127 = Иная ошибка, не определенная выше

7.3.2.10 Ошибка IPCablecom-Error

Объект ошибки, характерной для клиента, определяется следующим образом:

Длина = 8	S-Num = 9	S-Type = 1
Error-code [код-ошибки]	Error Sub-code [подкод-ошибки]	

Значениями Error-code, определенными в этой Рекомендации, являются:

1 = В настоящее время нет доступных шлюзов.

2 = Неизвестный идентификатор ID шлюза.

3 = Незаконное значение класса сеанса.

4 = Абонент превысил предел шлюза.

5 = Шлюз уже установлен

6 = Отсутствие требуемого объекта.

7 = Неработоспособный объект

8 = Недопустимое значение поля DS

127 = Другая, не указанная ошибка.

Поле подкода ошибки используется для обеспечения более подробной информации об ошибке. В случае кодов ошибки 6 или 7 это 16-битовое поле содержит в качестве 2-х 8-битовых значений S-Num и S-Type недостающего или ошибочного объекта. Порядок расположения значений S-Num и S-Type внутри подкода ошибки ДОЛЖЕН, быть таким же, что и в исходном сообщении. В тех случаях, когда существует несколько возможных вариантов для значения недостающего объекта S-Type, соответствующая часть подкода ошибки должна быть установлена в 0.

7.3.2.11 Параметры электронного наблюдения

Объект Параметры электронного наблюдения содержит всю необходимую информацию для поддержания электронного наблюдения. Данный объект МОЖЕТ включаться в сообщение Gate-Set для обеспечения возможности электронного наблюдения. CMTS ДОЛЖНА воспринимать данный объект в составе Gate-Set и предпринимать соответствующие действия, описанные ниже.

Длина = 20	S-Num = 10	S-Type = 1
Адрес DF-IP для CDC (32 бита)		
Порт DF для CDC (16 битов)	Флаги, определенные ниже	
Адрес DF-IP для CCC (32 бита)		
Порт DF для CCC (16 битов)	Зарезервировано	
Идентификатор CCC (32 бита)		
Идентификатор корреляции выписки счетов (24 байта)		

DF-IP-Address-for-CDC является адресом функции доставки электронного наблюдения, к которой должны быть высланы дублированные сообщения о событии.

DF-Port-for-CDC является номером порта для дублированных сообщений о событиях.

Флаги определяются следующим образом:

0x0001 DUP-EVENT [событие]. Если он установлен, то система CMTS ДОЛЖНА послать дубликат всех сообщений о событиях, относящихся к этому шлюзу, к DF-IP-Address-for-CDC.

0x0002 DUP-CONTENT [содержание]. Если он установлен, то система CMTS ДОЛЖНА послать копии всех пакетов согласования классификатора (классификаторов) для этого шлюза к DF-IP-Address-for-CCC и DF-Port-for-CCC. Формат, специфичный для перехваченных пакетов описывается ниже в данном разделе.

Остальная часть резервируется и ДОЛЖНА быть нулем.

DF-IP-Address-for-CCC [адрес-для-CCC] является адресом функции доставки электронного наблюдения, к которой должны посылаться дублированные пакеты с содержанием вызовов.

DF-Port-for-CCC [порт-для-CCC] является номером порта для дублированного содержания вызовов.

CCCID является идентификатором для дублированных пакетов содержания вызова.

Идентификатор корреляции выписки счета *Billing-Correlation-ID* назначается сервером CMS для всех записей, относящихся к данному сеансу. Формат смотри в Рекомендации МСЭ-Т J.164. Наличие *Billing-Correlation-ID* позволяет избежать включения объекта Event-Generation-Info при отправлении сообщений о событии к DF (см.7.3.2.7.). CMS ДОЛЖЕН обеспечить совпадение идентификаторов выписки счета при одновременном наличии объектов Параметры электронного наблюдения и Event-Generation –Info.

Скопированные пакеты ДОЛЖНЫ быть переданы в качестве потока дейтаграмм UDP/IP, отправленных к адресу IP (DF-IP-Address-for-CCC) и к номеру порта (DF-Port-for-CCC), определенным в объекте Параметры электронного наблюдения. Полезная нагрузка UDP/IP ДОЛЖНА принимать следующий формат:

Таблица 2/J.163 – Полезная нагрузка дейтаграмм соединения содержания вызова.

CCCID (4 байта)
Перехваченная информация (произвольная длина)

Перехваченная информация протокола RTP имеет следующий формат:

Таблица 3/J/163 – Перехваченная информация

Исходный заголовок IP (20 байтов)
Исходный заголовок UDP (8 байтов)
Исходный заголовок RTP (переменная длина, 12-72 байтов)
Исходная полезная нагрузка (произвольная длина)

Отметим, что перехвачены могут быть протоколы, отличные от RTP, такие, как для факсимильной передачи T.38.

7.3.2.12 Параметры описания сеанса (Session-Description-Parameters)

Данный объект более не используется. Для предотвращения неправильной интерпретации резервируется S-Num 11.

Длина =	S-Num = 11	S-Type = 1

7.3.3 Определение сообщений управления шлюзом

Сообщения, которые выполняют управление шлюзом между контроллером GC и системой CMTS, ДОЛЖНЫ быть определены и отформатированы следующим образом. Отметим, что сообщения от контроллера GC к системе CMTS представляют собой сообщения Decision [решение] COPS, а сообщения от системы CMTS к контроллеру GC представляют собой сообщения Report [информирование] COPS.

```
<Gate-Control-Cmd>          := <COPS-Common-Header> <Handle> [общий-заголовок-дескриптор]
                               <Context> [контекст] <Decision Flags>[флаги решений]
                               <ClientSI-Data>
<ClientSI-Data>             := <Gate-Alloc> | <Gate-Set> | <Gate-Info>> |
                               <Gate-Delete>
<Gate-Control-Response>     ::= <COPS-Common-Header> <Handle>
                               <Report-Type> <ClientSI-Object>
<ClientSI-Object>           ::= <Gate-Alloc-Ack> | <Gate-Alloc-Err> |
                               <GateSet-Ack> | <GateSet-Err> |
                               <Gate-Info-Ack> | <Gate-Info-Err> |
                               <Gate-Delete-Ack> | <Gate-Delete-Err>
<Gate-Alloc>                := <Decision-Header> <Transaction-ID> <Subscriber-ID>[<Activity-Count>]
<Gate-Alloc-Ack>            ::= <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                               <GateID (ID шлюза)> <Activity-Count>>

<Gate-Alloc-Err>            ::= <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                                    <IPCablecom-Error>
```

<Gate-Set>	::= <Decision-Header> <Transaction-ID> <Subscriber-ID> [<Activity-Count>] [<GateID (ID шлюза)] [<Event-Generation-Info>] [<Electronic-Surveillance-Parameters>] <Gate-Spec> [<Gate-Spec>]
<Gate-Set-Ack>	::= <ClientSI-Header> <Transaction-ID> <Subscriber-ID> <GateID (ID шлюза)> <Activity-Count>]
<GateSet-Err>	::= <ClientSI-Header> <Transaction-ID> <Subscriber-ID> <IPCablecom-Error>
<Gate-Info>	:= <Decision-Header> <Transaction-ID> <GateID (ID шлюза)>
<Gate-Info-Ack>	:= <ClientSI-Header> <Transaction-ID> <Subscriber-ID> <GateID (ID шлюза)> [<Event-Generation-Info>] [<Electronic-Surveillance-Parameters>] [<Gate-Spec>] [<Gate-Spec>]
<Gate-Info-Err>	::= <ClientSI-Header> <Transaction-ID> <GateID (ID шлюза)> <IPCablecom-Err>
<Gate-Delete>	: = <Decision-Header> <Transaction-ID> <GateID (ID шлюза)> <IPCablecom reason (код причины IPCablecom)>
<Gate-Delete-Ack>	:= <ClientSI-Header> <Transaction-ID> <GateID (ID шлюза)>
<Gate-Delete-Err>	::= <ClientSI-Header> <Transaction-ID> <GateID (ID шлюза)> <IPCablecom-Err>
<Gate-Open>	:: = <ClientSI-Header> <Transaction ID> <Gate ID>
<Gate-Close>	:: = <ClientSI-Header> <Transaction ID> <Gate ID> <IPCablecom reason (код причины IPCablecom)>

Объект Context (C-NUM = 2, C-TYPE = 1) в сообщении Decision COPS имеет значение R-Type (флаг типа запроса), установленное в 0x08 (запрос конфигурации), и M-Type, установленный в нуль. Поле Command-Code в обязательном объекте Decision-Flags [флаги-решения] (C-NUM = 6, C-TYPE = 1) устанавливается в 1 (конфигурация установки). Другим значениям нужно заставлять систему CMTS порождать сообщение Report, указывающее отказ. Объект Report-Type (C-NUM = 12, C-TYPE = 1), включенный в сообщение Report COPS, имеет поле Report-Type, установленное в 1 (успех), или 2 (отказ), в зависимости от результата команды управления шлюзом. Всем сообщениям Report, несущим отклик управления шлюзом, следует иметь бит флага запрашиваемого сообщения, установленный в заголовке COPS. Все сообщения о решении (DEC), кроме первого, желательно должны иметь флаг запрашиваемого сообщения, установленный в значение "ложь" в заголовке COPS. Первое сообщение о решении (decision message), переданное от сервера CMS в систему CMTS должно иметь флаг запрашиваемости, имеющий значение "истина". Значения этого флага устанавливаются так, чтобы согласовываться со спецификацией COPS. Они не должны оказывать влияния на работу протокола управления шлюзом

Если объект, получаемый в сообщении управления шлюзом, содержит нераспознанный S-Num или S-Type, такой объект ДОЛЖЕН быть проигнорирован. Наличие подобного объекта в сообщении управления шлюзом НЕ ДОЛЖНО считаться ошибкой в случае, если после отбрасывания данного параметра все требуемые объекты содержатся в сообщении.

7.4 Работа протокола управления шлюзом

7.4.1 Последовательность инициализации

Когда система CMTS (т. е. COPS PEP) осуществляет исходную загрузку, он ДОЛЖЕН прослушивать входящие соединения COPS на порте номер 2126 (назначенном с помощью IANA). Любой контроллер шлюза, нуждающийся в контакте с системой CMTS, ДОЛЖЕН установить соединение TCP к системе CMTS на таком порте. Ожидается, что многократные контроллеры шлюзов будут устанавливать соединения COPS с единственным системой CMTS. Когда соединение TCP между системой CMTS и контроллером GC устанавливается, система CMTS посылает информацию о себе самом к контроллеру GC в форме сообщения CLIENT-OPEN. Эта информация включает в себя обеспечиваемый идентификатор CMTS-ID в объекте идентификации PEP (PEPID). Системе CMTS СЛЕДУЕТ опустить объект Last PDP Address [последний PDP адрес] (LastPDPAddr) из сообщения CLIENT-OPEN.

В отклике контроллер шлюза посылает сообщение CLIENT-ACCEPT. Это сообщение включает в себя объект Keep-Alive-Timer [сохранять-действующим-таймер], который говорит системе CMTS максимальный интервал между сообщениями Keep-Alive.

Система CMTS затем посылает сообщение REQUEST [запрос], включая объекты Handle [дескриптор] и Context [контекст]. Объект Context (C-NUM = 2, C-TYPE = 1) МОЖЕТ иметь значение R-Type (флаг типа запроса), установленное в 0x08 (запрос конфигурации) и M-Type, установленное в нуль. Объект Handle содержит число, которое выбирается системой CMTS. Единственным ограничением, которое накладывается на это число, является то, что система CMTS НЕ ДОЛЖЕН использовать то же самое число для двух различных сообщений Request на единственном соединении COPS; в конфигурации IPCablecom обработка не имеет другого протокольного значения. Это завершает последовательность установления в начальное положение, которая показана на рисунке 13.

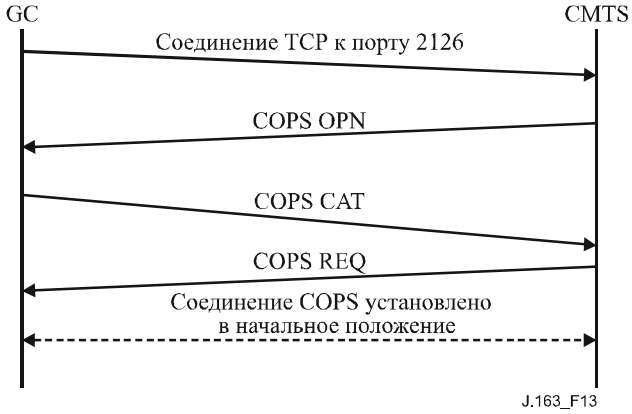


Рисунок 13/J.163 – Установление соединения COPS

Периодически система CMTS ДОЛЖНА посылать сообщение COPS KEEP-ALIVE (KA) к контроллеру GC. При получении сообщения KA COPS сервер CMS ДОЛЖЕН вернуть сообщение KA COPS обратно системе CMTS. Эта транзакция показана на рисунке 14 и полностью отражена в документе RFC 2748 IETF. Это ДОЛЖНО выполняться, по крайней мере, так часто, как указано в объекте Keep-Alive-Timer, возвращенном в сообщении CLIENT-ACCEPT. Сообщение KEEP-ALIVE посылается с объектом Client-Type, установленным в нуль.

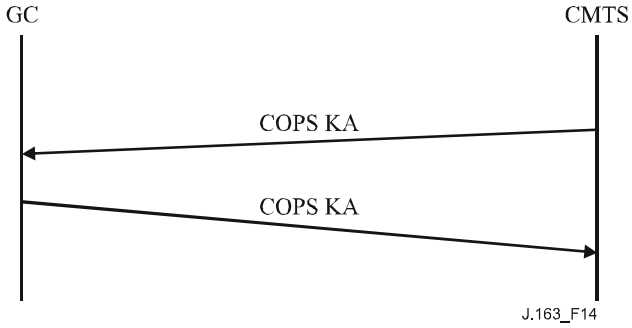


Рисунок 14/J.163 – Обмен сообщением keep-alive COPS

7.4.2 Последовательность работы

Протокол между контроллером шлюза и системой CMTS существует для целей политики управления ресурсами и распределения ресурсов. Контроллер шлюза осуществляет политику распределения и использует такую информацию, чтобы управлять набором шлюзов, осуществленных в системе CMTS. Контроллер шлюза устанавливает в начальное положение шлюзы с конкретным источником, пунктом назначения и ограничениями полосы пропускания, и при установлении в начальное положение адаптер MTA способен запрашивать распределение ресурсов внутри пределов, наложенных контроллером шлюза.

Сообщения, инициированные контроллером шлюза, включают в себя Gate-Alloc, Gate-Set, Gate-Info и Gate-Delete, а сообщения, инициированные CMTS, содержат Gate-Open и Gate-Close. Процедуры для этих сообщений описываются в следующих разделах.

Сообщения, инициированные контроллером шлюза, посылаются, используя объекты, характерные для клиента, внутри объекта решения сообщений COPS DECISION. Отклики на сообщения, инициированные контроллером шлюза, посылаются в качестве сообщений REPORT STATE [сообщить-состояние] с характерными для клиентов объектами в объекте ClientSI системы CMTS. Для сообщений ACK значение типа сообщения COPS ДОЛЖНО быть равным 1 передано как незапрашиваемое сообщение REPORT STATE с ID транзакции, равным 0, с характерными для клиентов объектами в объекте ClientSI и используя в соединении TCP, первоначально создавшем данный шлюз, значение типа сообщения, равное 3. Если данное соединение TCP не является более работоспособным, система CMTS должна игнорировать сообщения контроллера шлюзов.

Сообщения DECISION и сообщения REPORT-STATE ДОЛЖНЫ содержать тот же самый дескриптор, какой используется в исходном сообщении REQUEST, посланном системой CMTS, когда было инициировано соединение COPS.

Сообщение Gate-Alloc проверяет достоверность количества одновременных сеансов, которые разрешено устанавливать из исходящего адаптера MTA, и распределяет идентификатор GateID (ID шлюза), подлежащий использованию, для всех будущих сообщений, касающихся этого шлюза или набора шлюзов.

Сообщение Gate-Set инициализирует и изменяет все политики и параметры трафика для шлюза или набора шлюзов и устанавливает информацию выписки счетов и координации шлюза.

Сообщение Gate-Info является механизмом, с помощью которого контроллер шлюза может обнаруживать все установки текущих состояний и параметров существующего шлюза или набора шлюзов.

Система CMTS ДОЛЖНА периодически посылать сообщение Keep Alive (KA, "еще жив?") к контроллеру GC, чтобы облегчить обнаружение отказов соединений TCP. Контроллер шлюза сохраняет след о том, когда принимаются сообщения KA. Если контроллер шлюза не получил сообщение KA от системы CMTS во время, указанное документом RFC 2748 IETF, или контроллер шлюза не получил индикацию об ошибке от соединения TCP, то тогда контроллер шлюза ДОЛЖЕН разорвать соединение TCP и попытаться повторно установить соединение TCP перед тем, как будет затребовано распределить шлюз из такого системы CMTS.

Сообщение Gate-Delete позволяет контроллеру шлюза исключать недавно распределенный шлюз при определенных обстоятельствах (см. ниже).

Сообщение Gate-Open позволяет системе CMTS информировать контроллер шлюза о том, что ресурсы шлюза зафиксированы. Сообщение Gate-Open, вместе с сообщением Gate-Close, описанном ниже, устанавливают тракт с обратной связью между CMTS и CMS для обеспечения точного управления состоянием вызова сервером CMS.

Сообщение Gate-Close позволяет CMTS информировать контроллер шлюза о том, что шлюз удален благодаря вмешательству или неактивности адаптера MTA.

7.4.3 Процедуры для распределения нового шлюза

Сообщение Gate-Alloc посылается контроллером шлюза к системе CMTS во время, когда сообщение "Call_Set-up" [вызов_установить] посылается от исходящего адаптера MTA, как показано на рис. 14.

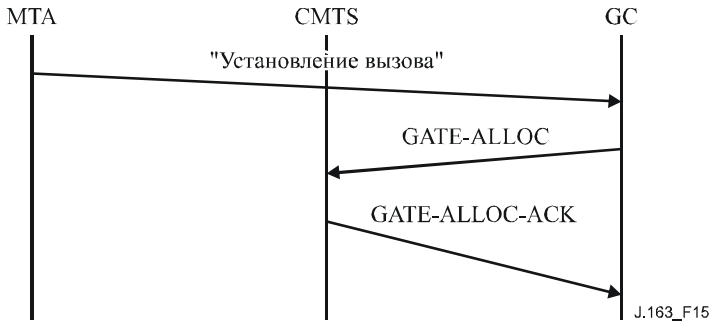
Использование сообщения Gate-Alloc гарантирует, что от данного адаптера MTA одновременно запрашивается не слишком много сеансов. Этот механизм может быть использован для управления при атаке типа "отказ в обслуживании" от адаптера MTA. Система CMTS в своем отклике на сообщение Gate-Alloc сравнивает количество распределенных в настоящее время шлюзов для указанного идентификатора subscriber-ID по сравнению с полем Count из объекта Activity-Count в сообщении Gate-Alloc. Если текущее количество шлюзов больше или равно полю Count в сообщении Gate-Alloc, то тогда система CMTS ДОЛЖНА возвратить сообщение Gate-Alloc-Err. Если текущее количество шлюзов больше, чем поле Count в сообщении Gate-Alloc, то тогда, похоже, абонент был повторно подготовлен для работы с меньшим пределом шлюза, чем раньше. В этом случае текущие

сеансы абонента не затрагиваются, но любые новые сеансы такого абонента будут отклонены системой CMTS, пока счет сеансов абонента не окажется ниже значения, указанного в поле Count.

То, какая величина должна находиться в поле Count, определяется в процессе работы. Она должна быть установлена достаточно большой (для каждого MTA), чтобы не оказывать отрицательного влияния на возможные сценарии узаконивания вызова, будучи, в то же время, достаточно низкой, чтобы предотвратить возникновение опасной атаки типа "отказ в обслуживании".

Если объект Activity-Count не присутствует, то система CMTS не выполняет проверку предела. Контроллер GC, стремясь уменьшить время установления вызова, МОЖЕТ принять решение о выполнении проверки предела шлюза при получении сообщения Gate-Alloc-Ack вместо выполнения проверки системой CMTS, поэтому контроллер GC параллельно может делать операции Gate-Alloc и просмотра политики абонента. Когда результаты обеих операций доступны, контроллер GC может выполнить проверку предела шлюза. Если проверка терпит неудачу, то контроллер GC ДОЛЖЕН послать сообщение Gate-Delete к системе CMTS, чтобы исключить шлюз, что был неправильно распределен (см. 7.4.8). Контроллер GC МОЖЕТ включить объект Activity-Count в соответствующие сообщения Gate-Alloc для такого абонента, как только политика была помещена в быстродействующую память.

Следующая далее диаграмма (см. рисунок 15) является примером сигнализации Gate-Alloc:



ПРИМЕЧАНИЕ. – В качестве примера сообщение "Установление вызова" в этом контексте относится к состоянию "Пригласить без звонка" при использовании DCS.

Рисунок 15/J.163 – Типовая сигнализация Gate-Alloc

Система CMTS ДОЛЖНА откликнуться на сообщение Gate-Alloc либо сообщением Gate-Alloc-Ack (указывающим успех), либо сообщением Gate-Alloc-Err (указывающим отказ). Идентификатор Transaction-ID в отклике ДОЛЖЕН соответствовать идентификатору транзакции в запросе.

Об ошибках в распределении шлюзов сообщают с помощью отклика Gate-Alloc-Err. Объект IPCablecomError содержит один из следующих кодов ошибок (Error-Codes):

1 = В настоящее время нет доступных шлюзов.

4 = Абонент превысил предел шлюза.

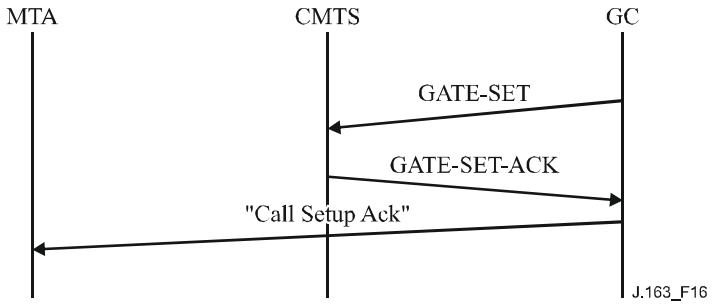
6 = Отсутствие требуемого объекта.

7 = Неработоспособный объект.

127 = Другая, не указанная ошибка.

7.4.4 Процедуры для авторизации ресурсов через шлюз

Сообщение Gate-Set посылается контроллером шлюза к системе CMTS, чтобы установить в начальное положение или изменить эксплуатационные параметры шлюза (шлюзов). Рисунок 16 иллюстрирует пример сигнализации Gate-Set.



ПРИМЕЧАНИЕ. – В качестве примера, сообщение "Call Setup Ack" в этом контексте относится к сообщению "2000 OK", возвращенному из состояния "Пригласить без звонка" при использовании DCS.

Рисунок 16/J.163 – Типовая сигнализация Gate-Set

Если в сообщении Gate-Set присутствует объект GateID (ID шлюза), то тогда запрос должен изменить существующий шлюз. Если объект GateID (ID шлюза) опущен из сообщения Gate-Set, то тогда есть запрос на распределение нового шлюза, и МОЖЕТ присутствовать объект Activity-Count таким образом, что система CMTS может определить, превысил ли абонент максимальное количество одновременных шлюзов (см. 7.4.3).

Сообщение Gate-Set ДОЛЖНО содержать в точности один или два объекта Gate Spec, описывая нуль или один шлюз восходящего потока и нуль или один шлюз нисходящего потока.

Система CMTS ДОЛЖНА откликнуться на сообщение Gate-Set либо сообщением Gate-Set-Ack (указывая успех), либо сообщением Gate-Set-Err (указывая неудачу). Идентификатор Transaction-ID в отклике ДОЛЖЕН соответствовать идентификатору транзакции ID в запросе.

Об ошибках в распределении или авторизации шлюзов сообщают с помощью отклика Gate-Set-Err. Объект IPCablecom-Error содержит один из следующих кодов ошибок (Error-Codes):

1 = В настоящее время нет доступных шлюзов.

2 = Неизвестный идентификатор GateID (ID шлюза).

3 = Незаконное значение класса сеанса.

4 = Абонент превысил предел шлюза.

5 = Шлюз уже установлен.

6 = Отсутствует требуемый объект

7 = Неработоспособный объект

127 = Другая, не указанная ошибка.

В обработке запроса на резервирование от адаптера MTA система CMTS ДОЛЖНА определять соответствующий шлюз путем использования значения TLV блока авторизации. Система CMTS ДОЛЖНА проверить, что запрос на резервирование находится внутри авторизованных пределов, указанных для шлюза.

Система CMTS затем обновляет запрос на резервирование, основанный на параметрах шлюза. Если набор параметров качества QoS является Допустимым (2), то система завершения CMTS ДОЛЖНА установить таймаут для параметров Допустимого качества QoS в значение таймера T7. CMTS ДОЛЖНА использовать кодовую точку DiffServ или значение TOS из объекта GateSpec для того, чтобы переписать октет Тип услуги IP перед отправлением пакетов.

Система CMTS ДОЛЖНА выполнить функцию управления доступом, основанную на предоставляемых параметрах политики и значения класса сессии шлюза.

Отметим, что сообщение Gate-Set может быть использовано вместо сообщения Gate-Alloc, чтобы распределить (и установить) шлюз. В таких ситуациях оказывается возможным, что номер порта, который используется удаленным шлюзом для сообщений координации приемного шлюза, не является доступным контроллеру шлюза. Если это так, то параметр CMTS-port в объекте Remote-Gate-Info (переносимый в сообщении Gate-Set) устанавливается в нуль. Это заставляет систему CMTS игнорировать номер порта координации шлюза. Однако, когда контроллер шлюза (позже) узнает о номере порта, который используется удаленным шлюзом, он должен послать другое сообщение Gate-Set (с номером порта в объекте Remote Gate Info), чтобы проинформировать систему CMTS относительно этого порта.

Роль Gate-Set состоит в том, чтобы для управления доступом при перемещении шлюза из состояния Авторизован в состояние Зарезервирован использовались последние из полученных параметров. Как только ресурсы зарезервированы, для адаптера MTA гарантированно будет выполнена любая операция фиксирования внутри диапазона режимов резервирования. После этого момента (т. е. когда шлюз уже находится в состоянии Зарезервирован или Зафиксирован) шлюз ДОЛЖЕН оставаться в данном состоянии. Любое сообщение Gate-Set, полученное для зарезервированного или зафиксированного шлюза ДОЛЖНО быть отвергнуто системой CMTS. Если из-за внешнего события (например, смены кодека, порта RTP или адреса IP и т. д.) параметры шлюза становятся неудовлетворительными для передачи поступающего потока данных, контроллер шлюза ДОЛЖЕН предпринять попытку создания нового шлюза для обработки измененного потока информации.

7.4.5 Процедуры для опроса шлюза

Когда контроллер шлюза желает обнаружить текущие установки параметров шлюза, он посылает системе CMTS сообщение Gate-Info. Система CMTS ДОЛЖНА откликнуться на сообщение Gate-Info с помощью либо сообщения Gate-Info-Ack (указывающего успех), либо с помощью сообщения Gate-Info-Err (указывающего неудачу). Идентификатор TransactionID в отклике ДОЛЖЕН соответствовать идентификатору ID транзакции в запросе. Объект (или объекты) GateSpec ДОЛЖНЫ быть включены в сообщение Gate-Info-Ack, если они перед этим были получены системой CMTS в контексте связи со шлюзом.

Об ошибках в опрашивании шлюзов сообщают с помощью отклика Gate-Info-Err. Объект Error содержит один из следующих кодов ошибок:

2 = Неизвестный идентификатор GateID (ID шлюза).

127 = Другая, не указанная ошибка.

7.4.6 Процедуры для фиксирования шлюза

Если адаптером MTA успешно осуществлена первоначальная операция Зафиксировать (так, как это описано в 6.2.1 для встроенных MTA) для шлюза, CMTS ДОЛЖНА отправить сообщение Gate-Open.

7.4.7 Процедуры для закрытия шлюза

При получении определенного сообщения от клиента MTA о высвобождении ресурсов (как это описано в 6.3.3 для встроенных MTA), или, если системой CMTS установлено, что клиент более не генерирует активно пакеты или не обновляет поток, связанный со шлюзом, CMTS ДОЛЖНА освободить все ресурсы, связанные со шлюзом, удалить шлюз, удалить все потоки (поток) услуг, связанные с сообщением DSD сети DOCSIS и отправить сообщение Gate-Close.

7.4.8 Процедуры для удаления шлюза

В потоке нормального вызова шлюз исключается системой CMTS, когда она получает сообщение DSD-REQ. Система CMTS также исключает шлюз при получении сообщения Gate-Close

Если зарезервированы или зафиксированы шлюзы в восходящем и нисходящем потоках одновременно, то действия CMTS должны подчиняться следующим правилам:

– Для сообщения DSD-REQ, инициированного E-MTA, включающего действующие идентификаторы восходящего и нисходящего потоков услуг, связанные с действующим шлюзом, CMTS должна удалить как восходящий, так и нисходящий потоки услуг и освободить все ресурсы, связанные со шлюзом.

– Для сообщения DSD-REQ, инициированного E-MTA, включающего действующий идентификатор восходящего потока услуг, связанный с действующим шлюзом и не включающего идентификатор нисходящего потока услуг, CMTS должна удалить как восходящий, так и нисходящий потоки услуг. CMTS должна отправить сообщение DSD-REQ для нисходящего потока услуг, связанного с адаптером E-MTA и освободить все ресурсы, связанные со шлюзом.

– Для сообщения DSD-REQ, инициированного E-MTA, включающего только действующий идентификатор потока услуг в нисходящем направлении, связанный с действующим шлюзом, и не включающего идентификатор восходящего потока услуг, связанный с действующим шлюзом, CMTS ДОЛЖНА удалить только нисходящий поток услуг. Система CMTS должна дождаться истечения времени связанного с восходящим потоком таймера T8, если в момент получения сообщения он еще работает или дождаться получения сообщения DSD-REQ для восходящего потока, или дождаться освобождения ресурсов, связанных со шлюзом.

Контроллер шлюза обычно не инициирует операцию исключения шлюза. Однако могли быть определенные ненормальные ситуации, где контроллер шлюза мог бы иметь желание исключить шлюз в системе CMTS. Например, если контроллер шлюза узнает (при получении отклика Gate-Alloc-Ack), что абонент превысил свой предел, он мог бы иметь желание исключить недавно распределенный шлюз в системе CMTS. В таких сценариях для контроллера шлюза ЖЕЛАТЕЛЬНО послать сообщение Gate-Delete к системе CMTS (вместо разрешения шлюзу поставить выдержку времени). Здесь могли быть другие ситуации, в которых функциональные возможности исключения были бы полезны.

Система CMTS ДОЛЖНА откликнуться на сообщение Gate-Delete сообщением Gate-Delete-Ack (указывающим успех) или сообщением Gate-Delete-Err (указывающим неудачу). Идентификатор Transaction-ID в отклике ДОЛЖЕН соответствовать идентификатору Transaction-ID в запросе. Об ошибках в исключении шлюзов сообщают с помощью отклика Gate-Delete-Err. Объект Error содержит один из следующих кодов ошибки (Error-Codes):

2 = Неизвестный идентификатор GateID (ID шлюза).

127 = Другая, не указанная ошибка.

7.4.9 Последовательность завершения

Когда система CMTS закрывает свое соединение TCP к контроллеру GC, он МОЖЕТ сначала послать сообщение DELETE REQUEST STATE (включая объект обработки, используемый в сообщении REQUEST). Система CMTS МОЖЕТ следовать этому с помощью сообщения CLIENT CLOSE. Эти сообщения являются необязательными, поскольку контроллер GC не имеет состояния, а также потому, что протокол COPS требует от сервера COPS автоматически исключать любое состояние, связанное с системой CMTS, когда соединение TCP завершается.

Когда контроллер шлюза собирается закрываться, ему СЛЕДУЕТ послать сообщение Client Close (CC) COPS системе CMTS. В сообщении CC COPS контроллеру шлюза НЕ СЛЕДУЕТ посылать объект адреса перенаправления PDP <PDPRedirAddr>. Если система CMTS получает сообщение CC COPS от контроллера шлюза с объектом <PDPRedirAddr>, система CMTS при обработке сообщения CC COPS ДОЛЖЕН игнорировать <PDPRedirAddr>.

7.4.10 Сценарий неудачного соединения

Когда система CMTS устанавливает, что потеряно соединение TCP или COPS с контроллером GC, например, в случае полного сбоя в работе контроллера GC, система терминалов CMTS ДОЛЖНА сохранить в неприкосновенности все установленные шлюзы. Одним из методов поддержания состояния соединения TCP или COPS является использование сообщений COPS Keep-Alive (Поддержание функционирования). В этом случае, если CMTS не получает не получает ответа Keep-Alive от сервера CMS в течение отведенного для этого ответа интервала, CMTS ДОЛЖНА рассматривать соединение COPS как утраченное и начать прослушивание с целью возобновления отсека TCP для порта 2126.

Шлюзы, которые к этому моменту были зафиксированы, останутся зафиксированными, а шлюзы, находящиеся в любом другом состоянии, останутся в этом состоянии до тех пор, пока их состояние не будет активным образом изменено или не истечет время для соответствующего таймера.

Поддержание состояний шлюзов во время сбоев GC/CMS позволит любому критичному потоку (например, срочному вызову) остаться в прежнем состоянии.

7.5 Использование CMS протокола шлюза

CMS ДОЛЖЕН обеспечивать включение всех кодеков, выбранных во время процедуры согласования, в диапазон режимов ресурсов, запрошенный от CMTS, использующей установление связи через шлюзы. CMS ДОЛЖЕН использовать алгоритм LUB, задаваемый в 6.1.1 для определения значений b, r, p, m, и M.

CMS ЖЕЛАТЕЛЬНО убедиться, что сообщение Gate Control, передаваемое в CMTS, содержит подходящие адреса IP и порты конечных точек, такие, на которые ссылаются конечные точки вызова и что кража услуг предотвращена.

CMS ДОЛЖЕН установить пассивный член в значение, равное 800 мкс для восходящего потока, если не отправляет MTA восходящий параметр дрожания разрешений. В противном случае, значение, используемое в шлюзе, должно быть меньше, чем отправляемое MTA для использования в качестве параметра Допустимого Дрожания Разрешений DOCSIS. Для нисходящего потока, CMS ДОЛЖЕН установить данное значение к ноль.

7.6 Координация шлюзов

Контроллер шлюзов сохраняет состояние каждого шлюза. Контроллер шлюзов создает шлюз в системе CMTS используя сообщение Gate-Alloc или Gate-Set. Контроллер шлюза может исключить шлюз, используя команду Gate-Delete или может запросить у CMTS информацию о конкретном шлюзе, используя сообщение Gate-Info. CMTS информирует контроллер GC об изменениях состояния, которые происходят, которые следуют после получения сообщений адаптера MTA или вследствие неактивности после использования сообщений Gate-Open и Gate-Close.

Сообщение Gate-Open генерируется системой CMTS, когда MTA фиксирует ресурсы QoS, таким образом давая начало вызову. Сообщение Gate-Close сигнализирует о закрытии шлюза в CMTS и высвобождении соответствующих ресурсов QoS. Как Gate-Open так и Gate-Close являются информативными сообщениями, относящимися к изменениям состояния CMTS, связанным с определенным шлюзом, и не требуют обратной связи от сервера CMS.

События Gate-Open и Gate-Close в местном и удаленном конечном пунктах должны быть синхронизированы для предотвращения сценариев возможной кражи услуг. Такая синхронизация осуществляется с использованием как встроенной логики сервера CMS, так и, при наличии многих серверов, путем сигнализации от CMS к CMS.

7.6.1 Соединение при вызове

Успешное соединение при обычном вызове требует выполнения трех тесно связанных между собой процессов:

- Сервер CMS запрашивает о фиксировании ресурсов локальным адаптером MTA;
- CMTS указывает, что ресурсы были зафиксированы локальным MTA;
- Координация фиксации местного и удаленного ресурса происходит в плоскости сигнализации.

См. рисунок 17.

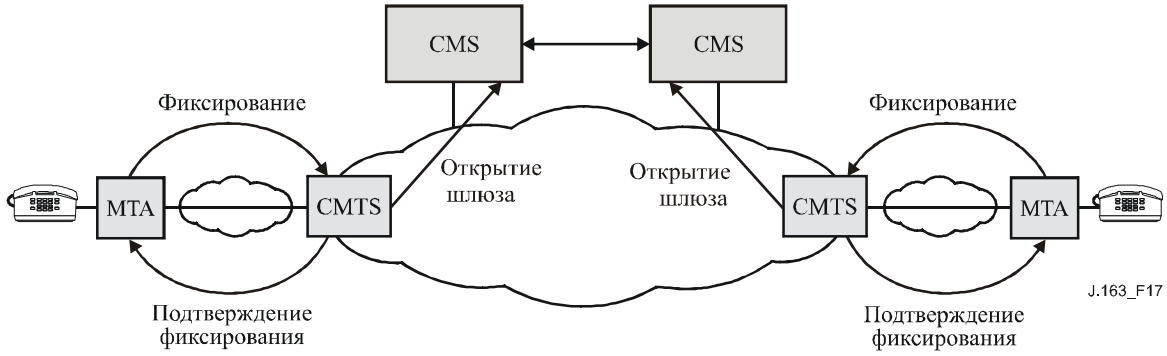


Рисунок 17/J.163 - Координация соединения при вызове.

Если CMS получает сообщение Gate-Open для шлюза, который еще не связан с ресурсами, которые надо зафиксировать, то CMS ДОЛЖЕН удалить шлюз с кодом причины "Неожиданная команда Gate-Open".

7.6.2 Прерывание вызова

Прерывание вызова, так же как и установление соединения, требует осуществления трех событий в течение короткого промежутка времени.

- CMS запрашивает о высвобождении ресурсов локальным адаптером MTA;
- Система CMTS устанавливает, что ресурсы были высвобождены локальным MTA;
- Координирование высвобождения местного и удаленного ресурсов происходит посредством сигнализации.

См. рисунок 18.

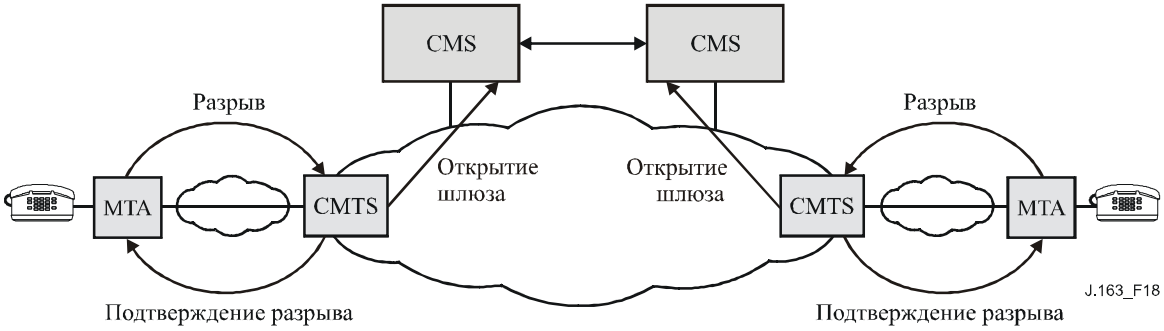


Рисунок 18/J.163 – Координация прерывания вызова

Когда сервер CMS посылает к MTA сообщение об удалении соединения, CMS ДОЛЖЕН включить таймер для периода времени T5. Если, ко времени завершения работы таймера система CMTS не зафиксировала закрытие шлюза, то CMS ДОЛЖЕН отдать команду Gate-Delete для удаления шлюза в системе CMTS с кодом причины "Неудача закрытия местного шлюза".

Когда CMS получает сообщение Gate-Close, он должен обновить свое внутреннее состояние, отражающее удаление шлюза в CMTS.

Приложение A

Определения таймеров и их значения

В данной Рекомендации упоминаются несколько таймеров. В данном Приложении содержится перечень этих таймеров и их рекомендованные значения.

Таймер-T0

Этот таймер осуществляется в системе CMTS в машине состояния шлюза и ограничивает период времени, которое может быть распределено шлюзу без установки параметров шлюза. Это дает возможность системе CMTS восстанавливать ресурсы идентификатора GateID, когда система управления вызовом терпит неудачу в завершении последовательности сигнализации для нового сеанса.

Этот таймер запускается, когда распределяется шлюз.

Этот таймер переустанавливается, когда устанавливаются параметры шлюза.

При окончании работы этого таймера система CMTS ДОЛЖНА рассматривать назначенный идентификатор GateID как недействующий.

РЕКОМЕНДОВАННОЕ значение этого таймера составляет 30 секунд.

Таймер-T1

Этот таймер осуществляется в системе CMTS в машине состояния шлюза и ограничивает период времени, который может произойти между тем, когда осуществляется авторизация и фиксация.

Этот таймер запускается всякий раз, когда устанавливается шлюз.

Этот таймер переустанавливается всякий раз, когда шлюз переходит в состояние ЗАФИКСИРОВАН.

При окончании работы этого таймера система CMTS ДОЛЖНА высвободить все ресурсы, зарезервированные в CMTS для данного шлюза, аннулировать любое резервирование, сделанное адаптером MTA, что было авторизовано этим шлюзом, сигнализируя CM, с помощью сообщений DSC или DSD об освобождении ресурсов, которые он зарезервировал и инициировать сообщение Gate-Close для этого шлюза.

Таймер-T1 ДОЛЖЕН быть установлен в значение, заданное в сообщении Gate-Set [шлюз-установить]. Если значение, заданное в сообщении Gate-Set, является нулем, то тогда таймер-T1 ДОЛЖЕН быть установлен в предварительное значение по умолчанию. РЕКОМЕНДОВАННОЕ значение этого умолчания находится в диапазоне 200-300 секунд.

Если значение таймера T1 в сообщении Gate-Set равно 0, система CMTS ДОЛЖНА возвратить или предусмотренное значение CMTS T1 или 0 для T1 в объекте GateSpec сообщения Gate-Info-Ack. В данном случае предпочтительным является предусмотренное (обусловленное) значение T1.

Таймер-T2

Данный таймер более не используется.

Таймер-T3

Данный таймер более не используется.

Таймер-T4

Данный таймер более не используется.

Таймер-T5

Данный таймер осуществляется в CMS.Он управляет синхронизацией высвобождения ресурсов локальным MTA и подтверждения системой CMTS закрытия местного шлюза.

Когда сервер CMS посылает к MTA сообщение об удалении соединения, CMS ДОЛЖЕН убедиться, что шлюз в системе CMTS был закрыт в промежутке T5. Этот таймер возобновляется, когда CMS получает с помощью сообщения Gate-Close подтверждение закрытия местного шлюза

После окончания работы этого таймера, CMS удаляет шлюз в системе терминалов CMTS, используя сообщение Gate-Delete с кодом причины "Неудача закрытия местного шлюза".

РЕКОМЕНДОВАННОЕ значение этого таймера составляет 5 с.

Таймер-T6

Таймер T6 более не используется

Таймер T7

Система CMTS ДОЛЖНА установить время ожидания (таймаут) для параметров допустимого качества QoS для потока услуг в значение, определенное для этого таймера. В случае потока с многократными подпотоками, таймаут потока для параметров допустимого QoS устанавливается в значение таймера T7 из самого последнего сообщения Gate-Set для любого из подпотоков данного потока. таймаут для параметров Допустимого качества QoS ограничивает период времени, который в течение которого система CMTS должна сохранять ресурсы для набора параметров Допустимого качества QoS потока услуг, пока число этих параметров больше, чем для набора параметров Активного качества QoS. За деталями использования таймаута для параметров Допустимого QoS, пожалуйста, обращайтесь к Дополнению C Дополнения B/J.112.

Для того, чтобы адаптер EMTA смог обновить таймер, CMTS ДОЛЖНА информировать EMTA о значении таймаута (времени ожидания) для параметров Допустимого QoS в ответе на запрос EMTA о резервировании (т. е. в сообщении DSA-RSP).

Рекомендуемое значение данного таймера по умолчанию 200 секунд.

Таймер T8

Система CMTS ДОЛЖНА установить время задержки для параметров Активного качества QoS потока услуг в значение, определенное для данного таймера. В случае потока с многократными подпотоками таймаут потока для параметров допустимого QoS устанавливается в значение таймера T8 из самого последнего сообщения Gate-Set для любого из подпотоков данного потока. таймаут для параметров Активного QoS ограничивает период времени, когда ресурсы остаются неиспользуемыми активным потоком услуг. За деталями использования таймаута для параметров Активного QoS, пожалуйста, обращайтесь к Дополнению C Дополнения B/J.112.

Для того, чтобы адаптер EMTA смог обновить таймер, CMTS ДОЛЖНА информировать EMTA о значении таймаута (времени ожидания) для параметров Активного QoS в ответе на запрос EMTA о резервировании (т. е. в сообщении DSA-RSP).

Значением по умолчанию для данного таймера является 0, что указывает CMTS не опрашивать поток услуг об активности.

Дополнения I-VIII и XI

Оставлено свободным.

Дополнение IX

Сценарии кражи услуг

Здесь выделены несколько возможных сценариев кражи услуг (пиратства), чтобы высветить необходимость в динамической авторизации, необходимость в протоколе 2-фазного резервирования ресурса, необходимость в шлюзах и необходимость в координации шлюзов. Проектирование систем возлагает на абонентов большую долю управления безопасностью сеанса, где ее легко можно увеличить с помощью новых технологий и предоставлять новые и передовые услуги. В то время как эта "корректировка на будущее" является целью разработки, нужно признать, что это оставляет открытым широкий диапазон возможностей для мошенничества. Это Приложение обсуждает некоторые из таких возможностей, и как архитектура сигнализации QoS предотвращает их.

Основное предположение состоит в том, что адаптер MTA не является невосприимчивым к вмешательству клиента, и что существенный стимул для бесплатного обслуживания будет вести к некоторым очень сложным попыткам сорвать любые средства управления сетью, возложенные на адаптер MTA. Это вмешательство клиента включает (но не ограничено только этим) открывание устройства и замену устройств постоянной памяти (ROM), замену интегральных микросхем, зондирование и инженерный анализ разработки адаптера MTA и даже полную замену адаптера MTA специальной версией "черного" рынка. В то время как существуют технические решения по физической защите адаптера MTA (например, постановка ловушки путем наполнения коробки смертоносным газом), они не считаются приемлемыми.

Так как адаптер MTA можно характеризовать только его процессом передачи информации по сети DOCSIS, оказывается возможным, и весьма вероятным, что будет написано программное обеспечение персонального компьютера, которое будет подражать поведению адаптера MTA. Такой персональный компьютер может быть неразличим от реального адаптера MTA. Поведение программного обеспечения в этом случае находится под полным управлением клиента.

Далее планируется, что в MTA будут осуществлены новые услуги, и что программное управление такими новыми услугами будет обеспечено множеством фирм-поставщиков. Это обновленное программное обеспечение будет нагружено в адаптер MTA, оставляя открытой возможность клиентов по загрузке из главной системы специальных урезанных версий, которые обеспечивают бесплатное обслуживание. Здесь не касаются проблемы "троянских коней" в таком загружаемом программном обеспечении, поскольку это считается идентичным сегодняшней проблеме клиентов, отдающих номера своих кредитных карточек и/или персональные идентификационные номера (PIN). Здесь обеспокоены клиентом, преднамеренно загружающим специальное программное обеспечение, которое делает только то, что служит его/ее наилучшим интересам.

IX.1 Сценарий № 1: Клиенты, сами устанавливающие соединения с высоким QoS

Адаптер MTA с достаточным интеллектом может помнить прошлые набранные пункты назначения и адрес пункта назначения, или использовать некоторый другой механизм, чтобы определить IP адрес пункта назначения. Он может тогда сигнализировать такому пункту назначения непосредственно (с некоторым сотрудничеством другого клиента), и согласовывать соединение высокого качества обслуживания через интерфейс сети DOCSIS для встроенного клиента. Так как в инициировании сеанса никакой агент сети не используется, то не будет производиться запись для выписки счета. Предотвращение этого сценария осуществляется затребованием динамической авторизации в системе CMTS; без авторизации попытка получить высокое качество обслуживания будет терпеть неудачу.

Вышеупомянутый сценарий требовал сотрудничества двух видоизмененных адаптеров MTA. Подобная кража услуги могла быть совершена только с видоизменяемым инициатором. Если исходящий адаптер MTA для установления сеанса использовал агента сети, тем самым в стандартной манере информируя пункт назначения о входящем сеансе, но опять сам согласовал высокое качество обслуживания, то не была бы порождена запись для выписки счета, и инициатор получил бы

бесплатный сеанс. Снова решение состоит в том, чтобы требовать использование шлюзов в терминалах CMTS.

IX.2 Сценарий № 2: Клиенты, использующие предоставляемое QoS для неречевых приложений

Статически обеспечиваемое качество QoS может определять клиента только как заказчика, которому разрешено высокое качество обслуживания. Нет никакого ограничения на использование услуги. В частности клиент, который подписался на коммерческую услугу голосовой связи и поэтому уполномочен активировать широкополосные соединения с низким запаздыванием через сеть DOCSIS, может использовать эту способность для перемещения по всемирной сети (web surfing) или для других приложений персонального компьютера. Предотвращение этого сценария осуществляется путем запроса динамической авторизации в системе CMTS; попытка получить высокое качество обслуживания без проверки полномочий будет терпеть неудачу.

IX.3 Сценарий № 3: Адаптер MTA, меняющий адрес пункта назначения в речевых пакетах

Другим примером является случай, когда два адаптера MTA, которые находятся далеко друг от друга, каждый устанавливает местный сеанс. Как только полоса пропускания и соединение установлены, адаптеры MTA затем изменяют IP адреса в RTP потоках, чтобы указывать друг друга. Система выписки счетов продолжает начисление оплаты каждому из них для местного сеанса, в то время как клиенты фактически заняты в сеансе дальней связи. Это требует, чтобы в системе CMTS имелись механизмы, которые обеспечивают доступ к более высокому качеству QoS, основанный только на предварительно разрешенных фильтрах пакетов. Таким образом, в дополнение к 2-фазному управлению ресурсом, этот сценарий мотивирует потребность в фильтрах пакетов в шлюзах.

IX.4 Сценарий № 4: Использование половинных соединений

Это пример кражи услуги, которая могла бы произойти в отсутствие координации шлюза. Предположим, что один клиент в сеансе фиксирует ресурсы сеанса, а другой – нет. Например, скажем, что завершающий клиент фиксирует ресурсы сеанса, но терпит неудачу в отправке надлежащего сообщения сигнализации, поэтому фиксирует свои ресурсы только инициатор. В этом случае открывается только один шлюз, а пользователи и сеть остались с половинным соединением. Задаваясь тем, что инициатор не фиксировал свои ресурсы, сеть не может законно начислять оплату пользователю за половинное соединение. Однако оказывается возможным для двух тайно сговаривающихся клиентов устанавливать два половинных соединения (ни на одно из которых не выписывается счет), которые могут быть объединены, чтобы дать полное соединение между этими двумя участниками. Это приводит к бесплатному сеансу. Мошенничество этого типа может быть предотвращено только путем синхронизации операций двух шлюзов.

IX.5 Сценарий № 5: Раннее завершение, после которого осталось половинное соединение

Координация шлюзов требуется также при завершении сеанса. Предположим, что адаптер MTA_O вызывает адаптер MTA_T и платит за сеанс. Поскольку адаптеру MTA_O начисляется плата за сеанс, он, несомненно, имеет стимул выпустить сообщение Release к системе $CMTS_O$, чтобы закрыть свой шлюз и остановить начисление оплаты. Однако, если адаптер MTA_T не выпускает сообщение Release, чтобы закрыть шлюз в системе $CMTS_T$, то остается половинное соединение. В этом случае адаптер MTA_T может продолжить посылать голос и/или данные к адаптеру MTA_O без выписки счета за сеанс. Следовательно, от шлюза исходящей стороны в системе $CMTS_O$ должно быть выпущено сообщение Gate-Close, чтобы закрыть шлюз завершающей стороны в системе $CMTS_T$.

IX.6 Сценарий № 6: Поддельные сообщения координации шлюза

Каждый адаптер MTA знает отличительную черту своей системы CMTS, и знает 5-кратную группу взаимосвязанных элементов данных, которые его система CMTS использует для определения идентификатора GateID. Адаптеры MTA могут выполнять различные виды сквозного согласования перед запросом ресурсов; в частности, они могут легко обмениваться информацией о своих идентификаторах GateID. Затем адаптер MTA может фальсифицировать сообщение Gate-Open, посылаемое концу, который не платит, и получить одностороннее соединение, на которое не выписывается счет. Осуществив это дважды, получают полное соединение, на которое не выписывается счет. Одно решение этой проблемы для GateController состоит в том, чтобы дать

системе CMTS ключ, используемый для сообщений между системами CMTS, на основе по каждому сеансу (или по каждому шлюзу).

IX.7 Сценарий № 7: Обман, направленный против нежелательных вызывающих пользователей

Благодаря подробностям последовательности установки вызова возможно, что авторизация полосы пропускания в пункте назначения будет более щедрой, чем это делается в источнике. Задаваясь этим, оказывается возможным для вызываемого участника резервировать и распределять полосу пропускания значительно выше окончательной согласованной величины, что приводит к начислению оплаты на вызывающего участника, которое выше, чем ожидается. Будучи доступным, это, похоже, использовалось бы против специалистов по телемаркетингу, сопротивляясь нежелательным вызовам в течение обеда.

При условии, что ресурсы сеанса авторизованы сервером CMS до получения запроса адаптера MTA о таких ресурсах, мы страхуемся от того, что CMTS разрешит запрос о большем количестве ресурсов, чем было авторизовано.

Дополнение X

COPS (Общая открытая служба политики)

X.1 Процедуры и принципы COPS

В данном Дополнении представлено краткое описание процедур и принципов COPS, и как COPS относится к другим протоколам, таким как LDAP.

Протокол Общей открытой службы политики (*COPS*) является протоколом "клиент/сервер", определенным для использования в управлении доступом в сетях QoS RSVP/IntServ и DiffServ. Обслуживание COPS выполняется посредством TCP/IP, с использованием хорошо известного порта номер 3288. Объекты COPS могли бы размещаться на пограгичных сетевых устройствах и сервере политики. Для rap-структуры определяются три функциональных объекта:

- Точка решения политики (PDP) – Объект сервера в услуге COPS, который принимает окончательное решение по допуску или отклонению сеанса, основанное на информации политики, к которой он имеет доступ. Ожидается, что это должно быть осуществлено как приложение в устройстве автономного сервера.
- Точка принуждения политики (PEP) – Объект клиента в службе COPS, который консультируется с точкой PDP, чтобы осуществить решения политики или получить информацию политики, которую он может сам использовать для осуществления решений по управлению доступом; точка PEP может получать запросы на услугу и инициировать вопрос к точке PDP, что приведет к отклику вида "идти/не-идти", или точка PEP может информировать точку PDP, что она желает получать на незапрашиваемой основе решения и информацию, относящиеся к политике.
- Точка местного решения (LDP) – Местная версия точки PDP, которая может принимать решения, основанные на местной информации или на информации, которую запомнили из предыдущих решений. Решение точки PDP всегда обладает превосходством над решением точки LDP.

Последовательность COPS, как используется в конфигурации RSVP/IntServ, показана ниже.

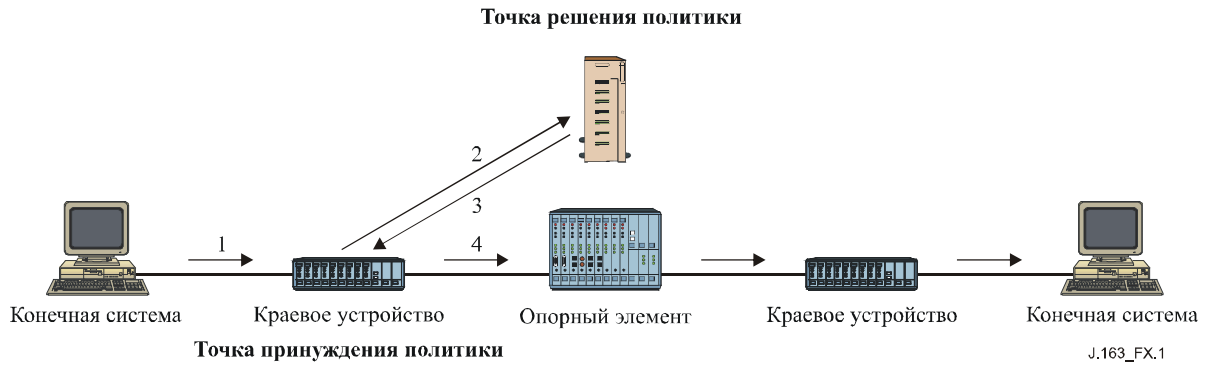


Рисунок X.1/J.163 – Протокол COPS

В последовательности COPS клиент точки PEP является ответственным за первоначальное установление сеанса с точкой PDP, используя информацию, которая либо конфигурирована в точке PEP, либо определена некоторыми другими средствами. Как только сеанс установлен, если пограничное сетевое устройство получает сообщение (1) RSVP, оно порождает запрос для обработки к точке PDP (2), что описывает контекст запроса и переносит информацию о запросе. Точка PDP затем откликается (3) решением принять или отклонить запрос, и если он допускается, то пограничное сетевое устройство продолжает действовать, направляя сообщение RSVP далее в сеть (4).

Каждый сеанс поддерживается сообщением Keep Alive [поддерживать действующим], которое контролирует, что сеанс является активным в случае, когда в последнее время не было получено никакого сообщения. Каждый запрос RSVP или другой запрос определяется дескриптором, который может быть использован, чтобы объединить отклик, последующие незапрашиваемые отклики и отбой.

Сообщения протокола расширяемы на другие задачи. Они состоят из кода Op, определяющего, является ли сообщение типа Request [запрос], Response [отклик] или другого типа, сопровождаемого самоопределяющимися объектами, каждый из которых содержит класс объекта и идентификатор версии. Каждый объект включает в себя номер класса, который определяет, чем является объект, например, объект таймера или объект решения, плюс тип класса, который определяет подтип или версию класса, который используется

Другие классы объектов включают в себя данные распределения полосы пропускания, необходимые для определения ресурсов, запрашиваемых пользователем, и объекты политики, которые могут быть пересланы вниз от точки PDP для включения в сообщение RSVP, когда оно отсылается в сеть.

X.2 Сравнение COPS и LDAP для политики

И услуга COPS, и протокол LDAP связаны с управлением, основанным на политике, однако они должны обеспечивать очень непохожие функции.

Услуга COPS разрабатывается для клиента, чтобы запрашивать решение от точки решения политики и взаимодействовать с точкой PDP для активного участия в управлении политикой и в вопросах, связанных с политикой. Точка PEP, которая делает запрос, может не иметь никакого фактического знания о политике и полагается на точку PDP, чтобы принять решения, основанные на ее знании политики. Протокол позволяет точке PEP пересылать информацию о запросе к точке PDP, а точке PDP – пересылать назад решение о том, позволять или отклонять запрос.

Протокол LDAP разработан для клиента, чтобы запрашивать справочную запись от справочника. Функция для использования записи зависит от клиента, который должен быть способен понимать извлеченную запись и принимать решение, как использовать информацию. Сервер должен быть способен к нахождению правильной записи, основанной на информации в запросе, который может вовлечь функцию поиска или извлечения многократных записей.

И услуга COPS, и протокол LDAP могут быть использованы в контексте управления доступом RSVP. Услуга COPS была бы использована между точками PEP и PDP, чтобы направлять запрос для анализа на основе политики. Протокол LDAP был бы использован между точкой PDP и сервером Справочника, чтобы осуществлять поиск и выборку записей политики, связанных с исходящими адресами и адресами пункта назначения для запроса RSVP. Точка PDP затем принимала бы решение,

основанное на извлеченной информации политики, и использовала услугу COPS, чтобы пересылать такое решение обратно к точке PEP. См. рисунок X.2.

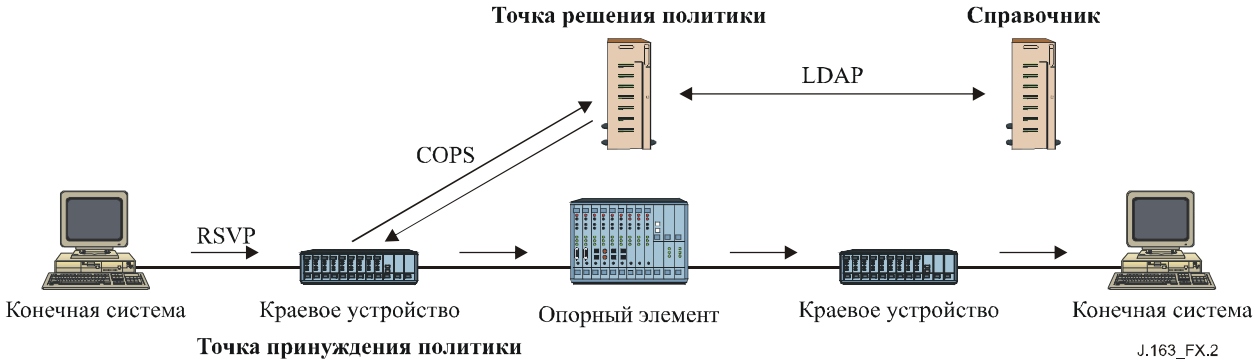


Рисунок X.2/J.163 – Модель COPS и LDAP

Дополнение XII

Анализ TCP

В данной Рекомендации описан интерфейс между контроллером шлюза (*GC*) и Системой оконечного устройства кабельного модема (*CMTS*), подлежащий использованию для авторизации шлюза, которое главным образом поддерживает протокол, основанный на транзакции, где каждая транзакция является независимой. Протокол TCP может быть использован в качестве транспорта для этого обмена сообщениями. Однако возникло некоторое беспокойство относительно последствий использования протокола TCP. В данном Дополнении исследуются некоторые из этих поводов для беспокойства и предлагаются некоторые потенциальные решения, которые могут обеспечить приемлемый транспорт путем оптимизации реализации и настройки реализации протокола TCP.

При разработке сети следует поддерживать желаемую степень надежности и рабочих характеристик в режиме реального времени.

XII.1 Требования

Рассмотрим сначала требования по транспортному протоколу для взаимодействия между контроллером GC и системой CMTS:

1) Требуется надежная доставка сообщений для сообщений, которыми обмениваются между контроллером GC и системой CMTS.

2) В нормальном случае (без потери пакета) обмену сообщениями следует иметь низкое запаздывание (порядка миллисекунд). Нужно иметь достаточно низкое запаздывание даже при потере пакета (порядка десятков миллисекунд).

3) Желательно, чтобы многократные запросы не выполнялись одновременно. Это вызвано тем, что установление многократных вызовов, похоже, будет проходить одновременно.

4) Если есть вероятность, что должна быть блокировка заголовка линии (HOL), то этого следует избегать.

5) Вероятно, будет продолжительная установившаяся ассоциация (по крайней мере, порядка нескольких минут) между контроллером GC и системой CMTS. Однако, когда имеется отказ контроллера GC, процесс установления нового соединения к системе CMTS не должен занимать чрезмерное время. Это особенно верно, когда установление нового соединения происходит в течение времени, когда устанавливается вызов.

XII.2 Рекомендуемые изменения

Коротко изменения, которые рекомендуются для несложной реализации протокола TCP, являются следующими:

1) Изменить механизм выдержки времени для установления соединения (сделать его более активным).

2) Позволить большее окно после установления соединения.

3) Иметь многократные соединения TCP на каждую пару GC- CMTS, чтобы отработать потенциальные проблемы HOL (например, использовать их на циклической основе).

4) Снизить дискретность 500 мс выдержки времени.

5) Выключить алгоритм Nagle на передающем конце, чтобы уменьшить запаздывание.

6) Иметь не блокирующийся интерфейс между приложением и стеком протокола TCP.

Оставшаяся часть этого Приложения дает подробности того, как эти изменения могут быть осуществлены.

XII.3 Установление соединения TCP, воздействующее на задержку после набора номера

Установление соединения протокола TCP использует вхождение в связь тремя этапами следующим образом (см. рисунок XII.1).

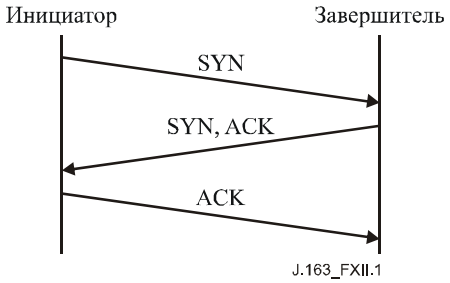


Рисунок XII.1/J.163 – Установление соединения TCP

Протокол TCP осуществляет повторную передачу сегментов, которые предполагаются утерянными, на основе оценки времени передачи в прямом и обратном направлении (по шлейфу) A и среднего отклонения D от A. Значение выдержки времени повторной передачи (*RTO*) обычно вычисляется с использованием формулы:

$$RTO = A + 4D,$$

но начальное значение RTO вычисляется с использованием формулы:

$$RTO = A + 2D,$$

где A и D первоначально устанавливаются, соответственно, в 0 и 3 секунды. Когда происходит повторная передача, к текущему значению RTO применяется экспоненциальный возврат, использующий множитель 2. Таким образом, для первого сегмента значение RTO вычисляется как:

$$RTO = 0 + 2 \times 3 = 6.$$

Таким образом, если начальный сегмент SYN утерян, то повторная передача не будет иметь места раньше задержки 6 секунд. В такое время значение RTO будет вычисляться как:

$$RTO = 0 + 4 \times 3 = 12$$

и применяется экспоненциальный возврат 2, приводя к новому значению выдержки времени для повторной передачи в 24 секунды. Таким образом, если повторная передача также будет потеряна, то протечет сумма в 30 секунд прежде, чем происходит третья повторная передача.

Важность этой проблемы полностью зависит от частоты, с которой установление соединения GC $\rightarrow$ CMTS попадает во время периода задержки после набора номера. В предполагаемых настоящее время сценариях этому появлению в значительной степени следует быть больше исключением, чем правилом. Задержка установления соединения, сильно воздействующая на задержку после набора номера, является важной причиной, чтобы избегать установления соединения в период задержки после набора номера. Услуга DiffServ, маркирующая пакеты, чтобы уменьшить как время запаздывание, так и вероятность потери, аналогично тому, что сегодня сделано с

маршрутизацией трафика, могла быть использована для уменьшения задержек установки соединения из-за потерянных пакетов.

XII.4 Необходимость низкой задержки для пакетов между GC и CMTS, даже при потерях

Требование (2), которое имеет дело с восстановлением потерянных пакетов, нуждается в нескольких доступных для TCP средствах, чтобы быстро оправиться от потери. Когда имеются только несколько передаваемых пакетов, и приемник не способен произвести достаточное количество дублированных сообщений ACK, восстановление от потери пакета осуществляется из выдержки времени повторной передачи. Алгоритм повторной передачи TCP основывается на сглаженном усреднении наблюдаемого времени передачи туда и обратно (*RTT, round-trip time*) A и сглаженного усреднения среднего отклонения в RTT. Как описано выше, значение выдержки времени при повторной передаче тогда устанавливается в:

$$RTO = A + 4D$$

и если таймер заканчивает работу, то рассматриваемый сегмент повторно передается, а значение RTO замедляется экспоненциально, используя для значения RTO множитель 2^8 до верхнего предела 64 секунд. Как только сегмент был переслан к TCP, сегмент либо успешно передается к пункту назначения, либо соединение закрывается после того, как прошел некоторый период времени (обычно большой период времени, например от 2 до 9 минут).

В то время как вышеупомянутая стратегия повторной передачи считается желательной, должны рассматриваться две вероятных (связанных) проблемы для рассматриваемого интерфейса:

1) Если сегмент не доставляется успешно в пределах небольшого периода времени, то вызов, который находится в процессе установления, должен быть, наиболее вероятно, прекращен, и поэтому следует иметь возможность прервать транзакцию.

2) Ограничение в 64 секунды на выдержку времени повторной передачи является неподходящим для осуществления связи в реальном времени, и его следует установить намного ниже.

Отдельной, но связанной проблемой является степень детализации значения RTO. В то время как спецификация TCP сама не определяет степень детализации значения RTO, обычно в коммерческих операционных системах принято иметь степень детализации 500 мс. Таким образом, потерянный сегмент в общем случае не будет обнаруживаться в пределах менее 500 мс, а два потерянных сегмента не будут обнаружены в пределах менее 500 мс + 1000 мс = 1, 5 секунды.

Чтобы быстро восстанавливаться при потере пакета в последовательности пакетов (не имея необходимости зависеть от многократных дублированных сообщений ACK, чтобы запускать быструю повторную передачу и ожидать, пока таймер RTO не прекратит работу), может оказаться желательным реализовать команду TCP-SACK, которая помогает восстановлению даже в том случае, если порог быстрой повторной передачи не был достигнут. Также рекомендуется, чтобы реализация TCP использовала меньшую степень детализации таймера (возможно, меньше чем 500 миллисекунд).

XII.5 Блокирование заголовка строки

Блокирование заголовка строки относится к факту, что протокол TCP обеспечивает услугу упорядоченной доставки данных, где потерянный сегмент может блокировать более поздние сегменты для доставки приложению. Таким образом, если сегменты 1 и 2 посылаются от A к B, и сегмент 1 потерян, то сегмент 2 не может быть доставлен приложению до тех пор, пока сегмент 1 не был успешно повторно передан.

Для рассматриваемого интерфейса это блокирование заголовка строки может быть, вероятно, преодолено достаточно разумным образом, устанавливая многократные соединения TCP между контроллером GC и системой CMTS, а затем используя набор соединений TCP для транзакций, например, в циклической манере. Таким образом, если сегмент потерян на одном соединении, то это не будет затрагивать сегменты, т. е. транзакции, посланные на других соединениях.

---

[8] Протокол TCP далее использует дублированные сообщения ACK, чтобы запустить повторную передачу потенциально утерянных сегментов, однако это будет игнорироваться для данной части обсуждения.

Нижняя сторона к этому подходу состоит в том, что потерянный сегмент вряд ли должен передаваться повторно до тех пор, пока его таймер повторной передачи не прекращает работу (в противоположность получаемому дубликату ACK), поскольку до этого времени не должны быть никакие дополнительные сегменты для передачи.

XII.6 Медленный старт протокола TCP

Способность протокола TCP начинать передачу потока пакетов данных иногда ограничивается медленным стартовым механизмом протокола TCP, особенно тогда, когда поток является малым числом пакетов данных (более 1). Желательно выбирать начальное окно, которое больше, чем 1 (как в начале жизни соединения, так и после восстановления от перегрузки при отдельной потере пакета). Желательным считается выбор начального размера окна от 2 до 4 MSS. Важно, однако, гарантировать, что это начальное окно не превышает 4 MSS, из-за потенциальной возможности самому вызвать перегрузку.

XII.7 Задержка пакетов: алгоритм Nagle

Протокол TCP/IP был первоначально разработан для того, чтобы поддержать многократные сеансы пользователей на медленной сети. Чтобы оптимизировать использование сети, для пользователей, осуществляющих ввод с клавиатуры, был введен алгоритм Nagle. По существу, этот алгоритм задерживает передачу пакета, пока не будет накоплен буфер передачи, или в течение некоторого периода времени (обычно около 200 миллисекунд).

Из-за природы реального времени этого трафика желательно выключать алгоритм Nagle для осуществления связи GC- CMTS. На большинстве платформ, основанных на Unix, алгоритм Nagle может быть выключен путем выпуска следующего системного вызова на дескрипторе файла гнезда:

Пример 1: Установка варианта выбора TCP_NODELAY

```
/* set TCP No-delay flag (disable Nagle algorithm) */
int flag = 1;
setsockopt(fd, IPPROTO_TCP, TCP_NODELAY, &flag,
                    sizeof(flag));
```

Большинство других языков и платформ обладают подобным свойством выключения алгоритма Nagle, обычно известным как вариант выбора TCP_NODELAY option.

XII.8 Интерфейс без блокировки

По умолчанию, большинство операционных систем предоставляют блокирующий интерфейс для TCP/IP гнезд. Хотя он может позволить улучшенную схему исправления ошибок, он оказывает воздействие на показатели качества канала связи.

По существу, такой системный вызов, как send() с блокирующим интерфейсом, никогда не возвращается, пока операционная система не подтверждает, что сообщение было успешно сохранено в буфере передачи.

Может быть желательным использовать интерфейс без блокировки, чтобы улучшить показатели качества и поддерживать асинхронные события, используя вызов функции select() на архитектуре, основанной на UNIX. Интерфейс гнезда без блокировки может быть установлен, используя следующий вызов к заново созданному гнезду.

Пример 2: Установка варианта выбора O_NONBLOCK

```
/* set the socket to non blocking */
fcntl(fd, F_SETFL, O_NONBLOCK);
```

Большинство других языков и платформ обладают подобным свойством.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	**Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов**
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	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 межсетевого протокола и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2007 г.