МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т J.160

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(11/2005)

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

Проект IPCablecom

Архитектура структуры для предоставления критических во времени услуг по сетям кабельного телевидения с использованием кабельных модемов

Рекомендация МСЭ-Т J.160

Рекомендация МСЭ-Т J.160

Архитектура структуры для предоставления критических во времени услуг по сетям кабельного телевидения с использованием кабельных модемов

Резюме

В настоящей Рекомендации описывается эталонная структура высокого уровня, которая идентифицирует функциональные компоненты и определяет интерфейсы, необходимые для предоставления цифровых голосовых услуг и услуг телефонии. Для реализации данной архитектуры было разработано семейство Рекомендаций (Рек. МСЭ-Т J.161–J.178).

Источник

Рекомендация МСЭ-Т J.160 утверждена 29 ноября 2005 г. 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 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.

Рекомендация МСЭ-Т J.160

Архитектура структуры для предоставления критических во времени услуг по сетям кабельного телевидения с использованием кабельных модемов

1 Сфера применения

В рамках проекта IPCablecom определено семейство Рекомендаций, которые могут быть использованы для разработки оборудования, способного взаимодействовать и имеющего возможность предоставления голосовых услуг, услуг передачи видео и других высокоскоростных услуг мультимедиа на пакетной основе по гибридным волоконно-коаксиальным (HFC) кабельным системам с использованием кабельных модемов в соответствии с семейством Рекомендаций DOCSIS. В дальнейшем данная архитектура будет расширена для того, чтобы включать приложения мультимедиа.

2 Нормативные справочные документы

В перечисленных ниже Рекомендациях МСЭ-Т и другой справочной литературе содержатся положения, которые посредством ссылок на них в этом 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 G.711 (1988), *Pulse code modulation (PCM) of voice frequencies*.

– 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 television services*, plus Annex A (2001), *Digital Video Broadcasting: DVB interaction channel for Cable TV (CATV distribution systems)*, Annex B (2004), *Data-over-cable service interface specifications: Radio-frequency interface specification* and Annex C (2002), *Data-over-cable service interface specifications: Radio-frequency interface specification using QAM technique*.

– ITU-T Recommendation J.161 (2001), *Audio codec requirements for the provision of bidirectional audio service over cable television networks using cable modems*.

– 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.163 (2005), *Dynamic quality of service for the provision of real-time 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.166 (2005), *IPCablecom management information base (MIB) framework*.

– ITU-T Recommendation J.167 (2005), *Media terminal adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems*.

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

– ITU-T Recommendation J.171.0 (2005), *IPCablecom trunking gateway control protocol (TGCP): Profiles overview*.

– ITU-T Recommendation J.178 (2005), *IPCablecom CMS to CMS signalling*.

– ITU-T Recommendation Q.704 (1996), *Signalling network functions and messages*.

– ITU-T Recommendation T.38 (2005), *Procedures for real-time Group 3 facsimile communication over IP networks*.

– IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

– IETF RFC 1119 (1989), *Network Time Protocol*.

– IETF RFC 1889 (1996), *RTP: A Transport Protocol for Real-Time Applications*.

– IETF RFC 1890 (1996), *RTP Profile for Audio and Video Conferences with Minimal Control*.

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

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

– IETF RFC 3260 (2002), *New Terminology and Clarifications for Diffserv*.

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

– IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

– IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

– IETF RFC 3611 (2003), *RTP Control Protocol Extended Reports (RTCP XR)*.

3 Термины и определения

В настоящей Рекомендации определены следующие термины:

3.1 IPCablecom: проект МСЭ-Т, включающий архитектуру и серию Рекомендаций, делающих возможной поставку услуг в режиме реального времени по сетям кабельного телевидения с использованием кабельных модемов.

3.2 кабельный модем: кабельный модем представляет собой оконечное устройство второго уровня, которое завершает соединение DOCSIS со стороны клиента.

3.3 управляемая сеть IP: сеть IP, управляемая одним объектом для целей транспортировки сигнализации IPCablecom и пакетов медиаинформации.

3.4 управляемая магистраль IP: управляемая есть IP, используемая для взаимосвязи доменов IPCablecom.

4 Сокращения и соглашения

4.1 Сокращения

В настоящей Рекомендации используются следующие сокращения:

ANC	Announcement Controller	Контроллер сообщений автоинформатора
ANP	Announcement Player	Проигрыватель сообщений автоинформатора
ANS	Announcement Server	Сервер сообщений автоинформатора
CM	Cable Modem	Кабельный модем
CMS	Call Management Server	Сервер управления вызовами

CPE	Customer Premises Equipment	Оборудование в помещении клиента
DHCP	Dynamic Host Configuration Protocol	Динамический протокол конфигурирования узла
DNS	Domain Name System	Доменная система имен
DTMF	Dual Tone Multi-Frequency	Двухтональный многочастотный сигнал
FQDN	Fully Qualified Domain Name	Полное доменное имя узла
GC	Gate Controller	Контроллер шлюза
HFC	Hybrid Fibre/Coax	Гибридный волоконно-коаксиальный (кабель)
HTTP	HyperText Transfer Protocol	Протокол передачи гипертекста
IEEE	Institute of Electrical and Electronic Engineers	Институт инженеров по электротехнике и радиоэлектронике
IETF	Internet Engineering Task Force	Рабочая группа по стандартам Интернет
IP	Internet Protocol	Протокол Интернет
IPsec	IP security	Безопасность IP
ISTP	Internet Signalling Transport Protocol	Транспортный протокол сигнализации Интернет
ISUP	Integrated Services Digital Network User Part	Пользовательская часть цифровой сети с комплексными услугами
MAC	Media Access Control	Управление доступом к среде передачи
MF	Multi-Frequency	Многочастотный
MG	Media Gateway	Медиашлюз
MGC	Media Gateway Controller	Контроллер медиашлюза
MIB	Management Information Base	Информационная база управления
MMH	Multilinear Modular Hash	Полилинейный модульный хеш
MTA	Media Terminal Adapter	Адаптер медиатерминала
MTP	Message Transfer Part	Подсистема передачи сообщений
NAT	Network Address Translator	Транслятор сетевых адресов
NCS	Network-Based Call Signalling	Сигнализация вызовов на основе сети
OSS	Operations Support System	Система операционной поддержки
PSTN	Public Switched Telephone Network	Коммутируемая телефонная сеть общего пользования
QoS	Quality of Service	Качество обслуживания
RKS	Record Keeping Server	Сервер учетной информации
RTP	Real-Time Transfer Protocol	Протокол передачи режима реального времени
SA	Source Address	Адрес источника
SCCP	Signalling Connection Control Part	Подсистема управления соединением сигнализации
SG	Signalling Gateway	Шлюз сигнализации
SID	System IDentification number	Идентификационный номер системы
SNMP	Simple Network Management Protocol	Простой протокол управления сетью

TCAP	Transaction Capabilities Application Part	Прикладная подсистема возможностей транзакции
TFTP	Trivial File Transfer Protocol	Тривиальный протокол передачи файлов
TGCP	Trunking Gateway Control Protocol	Протокол управления транкинговым шлюзом
TGS	Ticket Granting Server	Сервер предоставления мандата
ToS	Type of Service	Тип услуги
UDP	User Datagram Protocol	Протокол дейтаграмм пользователя

4.2 Соглашения

Применение данной Рекомендации не является обязательным. В случаях ее применения такие ключевые слова как "ДОЛЖЕН", "СЛЕДУЕТ" и "ТРЕБУЕТСЯ" следует понимать как указывающее на обязательную сторону настоящей Рекомендации.

Используемые в тексте данной Рекомендации ключевые слова, которые указывают на определенный уровень значимости специфических требований, приведены ниже:

"ДОЛЖЕН" Данное слово, наречие "НЕОБХОДИМО" или глагол "ТРЕБУЕТСЯ" означает, что данное условие является абсолютным требованием этой Рекомендации.

"НЕ ДОЛЖЕН" Данное словосочетание означает, что на данное условие этой Рекомендацией налагается абсолютный запрет.

"СЛЕДУЕТ" Данное слово или глагол "РЕКОМЕНДУЕТСЯ" означает, что могут существовать веские условия при определенных обстоятельствах, в которых данное условие можно игнорировать, но перед тем как выбрать другой вариант, необходимо получить полное понимание последствий и тщательно взвесить ситуацию.

"НЕ СЛЕДУЕТ" Данное словосочетание означает, что могут существовать веские условия при определённых обстоятельствах, в которых описанный образ действий приемлем или даже полезен, но перед тем как выполнить действия, отмеченные этим обозначением, необходимо получить полное понимание последствий и тщательно взвесить ситуацию.

"МОЖЕТ" Данное слово или наречия "МОЖНО", "НЕОБЯЗАТЕЛЬНО" означает, что данное условие является необязательным. Один поставщик вправе использовать его, потому что этого будет требовать рыночная ситуация или, например, это приведёт к улучшению продукта, а другой поставщик может опустить это условие.

5 IPCablecom

5.1 Архитектура структуры IPCablecom

На очень высоком уровне архитектура IPCablecom состоит из трех сетей: "Сети доступа HCF DOCSIS", "Управляемой сети IP" и КТСОП. Система завершения кабельного модема (CMTS) обеспечивает связь между "Сетью доступа HCF DOCSIS" и "Управляемой сетью IP". Как Шлюз сигнализации (SG), так и Медиашлюз (MG) обеспечивают связь между "Управляемой сетью IP" и КТСОП. Эталонная архитектура IPCablecom показана на рисунке 1.

Сеть доступа HCF DOCSIS обеспечивает высокоскоростной, надежный и безопасный обмен данными между оборудованием в помещении клиента и головным узлом кабельной сети. Данная сеть доступа предоставляет все возможности DOCSIS, включая Качество обслуживания. Сеть доступа HCF DOCSIS включает следующие функциональные компоненты: Кабельный модем (CM), Адаптер мультимедиатерминала (MTA) и Систему завершения кабельного модема (CMTS).

На Управляемую сеть IP возложено несколько функций. Прежде всего, она обеспечивает взаимосвязь между базовыми функциональными компонентами IPCablecom, отвечающими за сигнализацию, медиаинформацию, инициализацию и подготовку к работе, а также установление качества обслуживания в сети доступа. Дополнительно Управляемая сеть IP обеспечивает связь на дальних расстояниях между другими Управляемыми сетями IP и сетями HCF DOCSIS. Управляемая сеть IP включает следующие функциональные компоненты: Сервер управления вызовами (CMS), несколько вспомогательных серверов Систем операционной поддержки (OSS), Шлюз сигнализации (SG), Медиашлюз (MG), а также Контроллер медиашлюза (MGC).

Отдельные компоненты сети, показанные на рисунке 1, детально описаны в пункте 6.

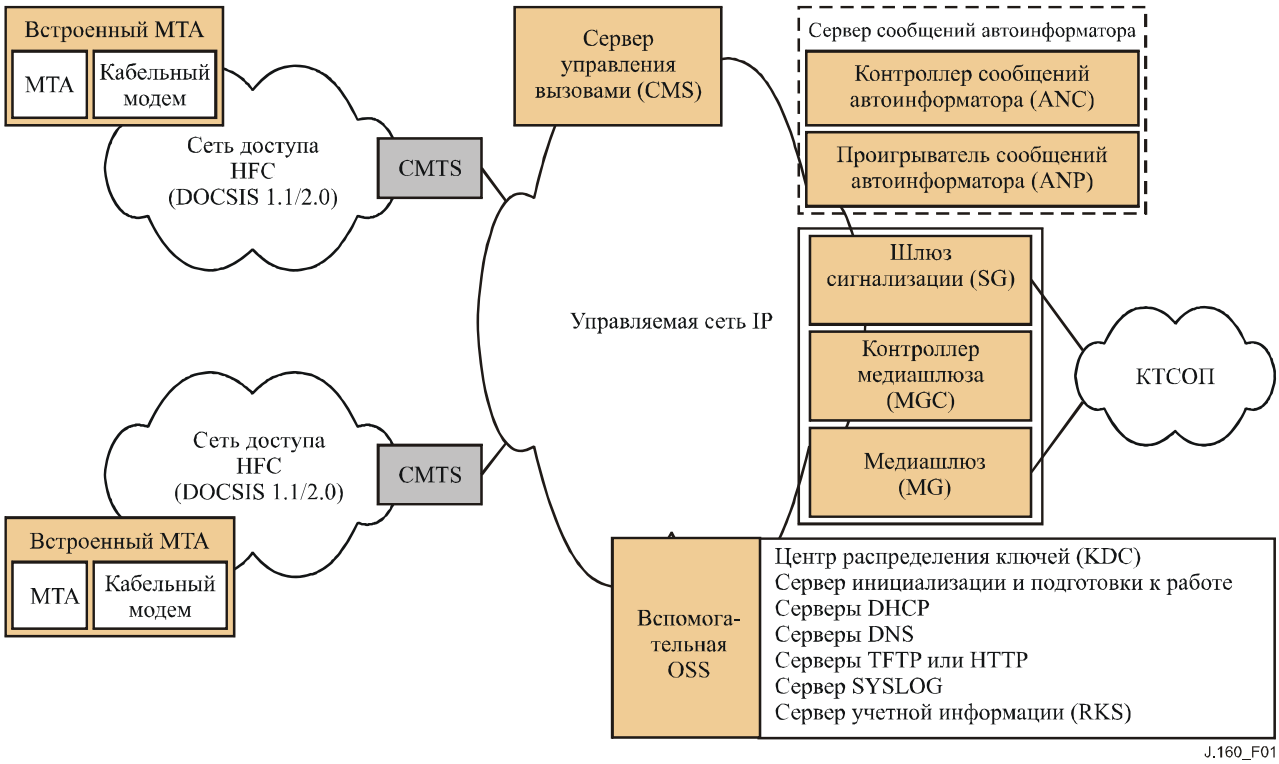


Рисунок 1/J.160 – Эталонная архитектура IPCablecom

5.2 Зоны и домены IPCablecom

Зона IPCablecom состоит из набора MTA в одной или более сетей доступа HCF DOCSIS, которые управляются одним функциональным CMS, как показано на рисунке 2. Интерфейсы между функциональными компонентами внутри одной зоны и между зонами (например, CMS ↔ CMS), определены в Рекомендациях IPCablecom.

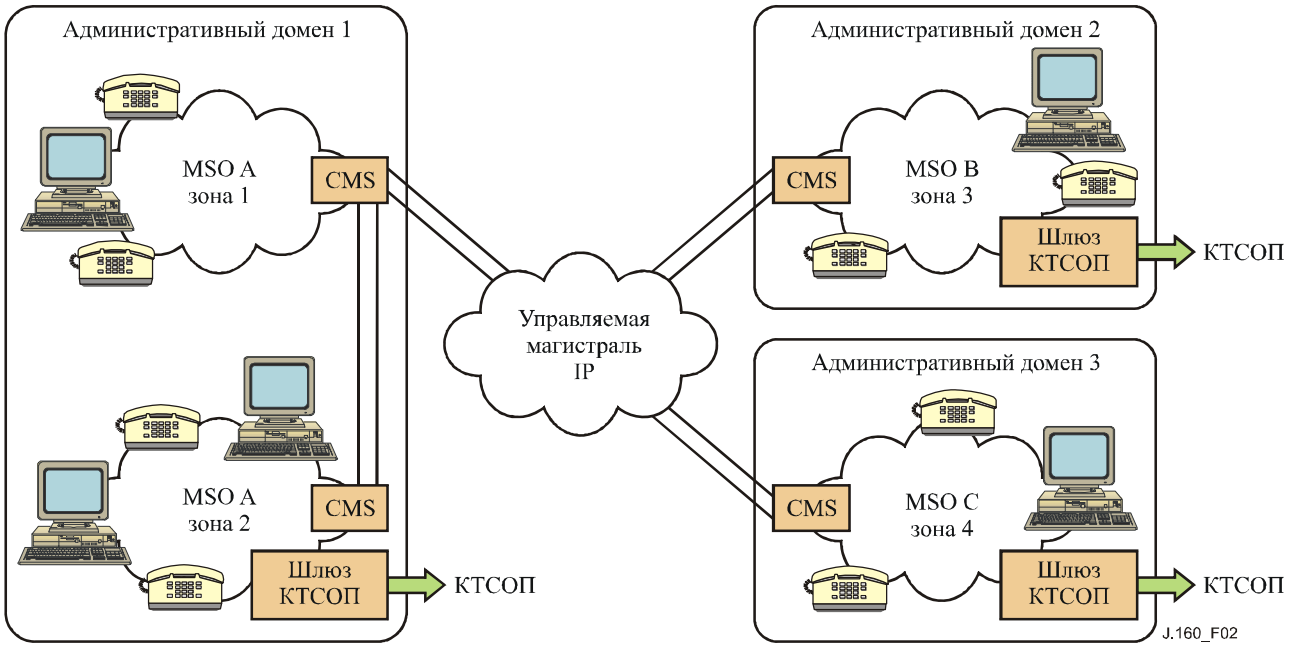


Рисунок 2/J.160 – Зоны и административные домены

Домен IPCablecom состоит из одной или более зон IPCablecom, которые эксплуатируются и управляются одним административным объектом. Домен IPCablecom может также называться административным доменом.

5.3 Рекомендации IPCablecom

Таблица 1/J.160 – Рекомендации IPCablecom

J.160	Архитектура структуры для предоставления критических во времени услуг по сетям кабельного телевидения с использованием кабельных модемов
J.161	Требования к аудиокодекам для предоставления двунаправленных аудиоуслуг по сетям кабельного телевидения с использованием кабельных модемов
J.162	Протокол сигнализации сетевого вызова для предоставления критических во времени услуг по сетям кабельного телевидения с использованием кабельных модемов
J.163	Динамическое качество обслуживания для обеспечения услуг режима реального времени по сетям кабельного телевидения с использованием кабельных модемов
J.164	Требования к Сообщениям о событиях для поддержки услуг, предоставляемых в режиме реального времени по сетям кабельного телевидения с использованием кабельных модемов
J.165	Транспортный протокол сигнализации Интернет IPCablecom (ISTP)
J.166	Структура базы управляющей информационной (MIB) IPCablecom
J.167	Требования к инициализации устройства адаптера медиатерминала (MTA) для поставки услуг в режиме реального времени по сети кабельного телевидения с использованием кабельных модемов
J.168	Свободно. Включено как Приложение E/J.166
J.169	Свободно. Включено как Приложение C/J.166
J.170	Спецификация безопасности IPCablecom
J.171.1	Протокол управления транкинговым шлюзом (TGCP) IPcablecom: Профиль 1
J.171.2	Протокол управления транкинговым шлюзом (TGCP) IPcablecom: Профиль 2
J.172	Механизм управляющих событий IPCablecom
J.173	Поддержка первичной линии E-MTA IPCablecom

Таблица 1/J.160 – Рекомендации IPCablecom

J.174	Междоменное качество обслуживания IPCablecom
J.175	Протокол аудиосервера
J.176	Свободно. Включено как Приложение D/J.166
J.177	Спецификация инициализации абонента CMS IPCablecom
J.178	Сигнализация IPCablecom CMS - CMS
J.179	Поддержка мультимедиа в IPCablecom

5.4 Принципы построения IPCablecom

Для того чтобы сделать возможной мультимедиасвязь в режиме реального времени с использованием инфраструктуры кабельной сети, в Рекомендациях IPCablecom определяются протоколы в следующих областях:

– Сигнализация вызовов;
– Качество обслуживания;
– Транспортировка и кодирование медиапотоков;
– Инициализации и подготовка к работе устройств;
– Сообщения о событиях;
– Безопасность;
– Электронное наблюдение;
– Системы операционной поддержки.

В данном пункте приводятся высокоуровневые цели и концепции построения, используемые при разработке Рекомендаций, определяющих эталонную архитектуру IPCablecom. Для получения детальных требований к протоколам в каждой из этих областей следует обращаться к отдельным Рекомендациям IPCablecom.

5.4.1 Общие цели построения

- Предоставление возможностей передачи голоса с качеством, аналогичным или более высоким, чем в КТСОП, с точки зрения конечного пользователя.
- Предоставление сетевой архитектуры, способной к масштабированию и поддержке миллионов абонентов.
- Обеспечение односторонней задержки для локального доступа IP и выхода IP (т. е. не включая магистраль IP) на уровне менее 45 мс.
- "Усиление" существующих стандартов. Разработчики IPCablecom стремятся устанавливать открытые, одобренные промышленные стандарты, которые широко приняты в коммерческих сетях связи. Это включает стандарты, одобренные МСЭ, IETF, IEEE и другими организациями, занимающимися разработкой стандартов в области связи.
- "Усиление" и принятие в качестве основы транспортных возможностей и возможностей Качества обслуживания, предоставляемых инфраструктурой J.112.
- Определение архитектуры, позволяющей множеству производителей быстро разрабатывать низкозатратные решения, для того чтобы удовлетворять потребности рынка в новых продуктах.
- Обеспечение возможности проектирования сетей таким образом, чтобы вероятность блокировки вызова в час пик дня с наибольшей нагрузкой на сеть составляла менее 1%.
- Обеспечение возможности проектирования сетей таким образом, чтобы прерывания вызовов и дефекты вызовов имели место не чаще, чем один раз на 10 000 выполненных вызовов.
- Поддержка модемов (до V.90 56 кбит/с) и факсов (до 14,4 кбит/с).
- Обеспечение того, чтобы проскальзывание кадров из-за несинхронизированных тактовых генераторов выборки или из-за потерянных пакетов имело место не чаще чем 0,25 в минуту Сигнализации вызова.

5.4.2 Сигнализация вызова

- Определение архитектуры сигнализации на основе сети.
- Предоставление сквозной сигнализации вызовов для следующих моделей вызовов:
  - вызовы, исходящие из КТСОП и оканчивающиеся в кабельной сети;
  - вызовы, исходящие из кабельной сети и оканчивающиеся в кабельной сети;
  - вызовы, исходящие из кабельной сети и оканчивающиеся в КТСОП;
  - вызовы, пересекающие зоны (внутридоменные) и домены (междоменные).
- Предоставление сигнализации для поддержки таких возможностей сигнализации, как:
  - отложенный вызов;
  - отмена отложенного вызова;
  - переадресация вызова (нет ответа, занят, переменная);
  - трехсторонний вызов;
  - индикатор ожидающего сообщения голосовой почты;
  - доставка номера звонящего;
  - доставка имени звонящего;
  - определение номера звонящего в отложенном вызове;
  - блокировка определения номера звонящего;
  - отклонение анонимного вызова;
  - автоматический обратный вызов;
  - автоматический повторный вызов;
  - набор номера/отложенный вызов из электронного списка;
  - выдача автоматически записанного номера абонента, от которого поступил последний вызов по запросу потребителя.
- Поддержка сигнализации, совместимой с существующими стандартами IP-телефонии для использования внутри сети IPCablecom оператора и при соединении с сетью КТСОП.
- Возможность прямого набора любого местного или международного телефонного номера (адрес Рек. МСЭ-Т E.164).
- Возможность приему вызова с любого местного или международного телефонного номера, поддерживаемого КТСОП.
- Обеспечение возможности сохранения абонентом текущего телефонного номера посредством Переносимости местного номера (LNP).
- Возможность использования любого поставщика услуг междугородней (международной) связи по выбору. Это включает предварительную подписку и выбор для каждого отдельного вызова.
- Поддержка ограничений Блокировки вызова/Блокировки платного вызова (например, блокировка вызовов на определенные префиксы).

5.4.3 Качество обслуживания

- Предоставление широкого спектра механизмов политик для того, чтобы сделать возможным обеспечение Качества обслуживания и управление им для услуг IPCablecom, оказываемых по кабельной сети доступа.
- Предоставление механизмов контроля допуска как для восходящих, так и для нисходящих потоков данных.
- Возможность динамического внесения изменений в QoS в ходе выполнения вызовов IPCablecom.
- Минимизация и предотвращение неправильного использования QoS, включая атаки "кражи услуги" и "отказа в обслуживании". Обеспечение того, чтобы политика QoS устанавливалась и исполнялась доверенными сетевыми элементами IPCablecom.
- Предоставление механизма приоритетов для экстренных вызовов и других услуг сигнализации на основе приоритетов.

5.4.4 Кодек и медиапоток

- Минимизация влияния, оказываемого задержкой, потерей пакетов и дрожанием на качество передачи голоса в среде IP-телефонии.
- Определение минимального набора аудиокодеков, которые должны поддерживаться всеми конечными устройствами IPCablecom (MTA и MG). Кодеки отбираются в соответствии с критерием максимальной эффективности в плане качества передачи голоса, использования ширины полосы пропускания и сложности реализации.
- Приспособление к развивающимся узкополосным и широкополосным технологиям сжатия/восстановления.
- Определение механизмов устранения эффекта эха и обнаружения голосовой активности.
- Поддержка прозрачной, безошибочной передачи сигналов DTMF и обнаружения как при помощи внутриполосной передачи, так и с использованием ретрансляции DTMF.
- Поддержка оконечных устройств для глухих и слабослышащих людей.
- Предоставление механизмов переключения кодеков в случае необходимости использования услуг факса или модема.
- Поддержка ретрансляции факса для устойчивой передачи факсимильной информации по сетям IP.
- Поддержка подсчета и выдачи отчетов о параметрах VoIP для отслеживания качества передачи голоса.

5.4.5 Инициализация и подготовка к работе устройств и Система операционной поддержки

- Поддержка статической и динамической инициализации и подготовки к работе оборудования в помещении потребителя (MTA и CM).
- Обычные изменения в ходе инициализации и подготовки к работе не должны требовать перезагрузки MTA.
- Возможность динамического назначение адресов IP устройствам абонента и управления этими адресами.
- Обеспечение того, чтобы инициализация и подготовка к работе, а также конфигурирование MTA в режиме реального времени не сказывались отрицательно на оказании услуг абоненту.
- Определение модулей MIB для управления оборудованием в помещении потребителя при помощи Простого протокола управления сетью (SNMP) IETF.

5.4.6 Безопасность

- Обеспечивать возможность предоставления услуг голосовой связи в домашних условиях с "воспринимаемым" уровнем безопасности, таким же или выше чем в КТСОП.
- Обеспечивать защиту от атак на MTA.
- Защищать оператора кабельной сети от различных атак типа "отказ в обслуживании", "разрыв сети" или "кража услуги".
- Принципы построения включают конфиденциальность, аутентификацию, целостность и контроль доступа.

5.4.7 Электронное наблюдение

- Поддержка возможности осуществления электронного наблюдения путем выдачи отчета о данных и содержании вызова.

6 Функциональные компоненты IPCablecom

В данном пункте описываются функциональные компоненты, содержащиеся в сети IPCablecom (см. рисунок 3). Описание компонентов не призвано определить или предписать требования к реализации продукта, оно лишь показывает функциональную роль каждого из этих компонентов в эталонной архитектуре. Отметим, что отдельные реализации продуктов могут, по необходимости, совмещать функциональные компоненты. Не все компоненты сети IPCablecom являются обязательными.

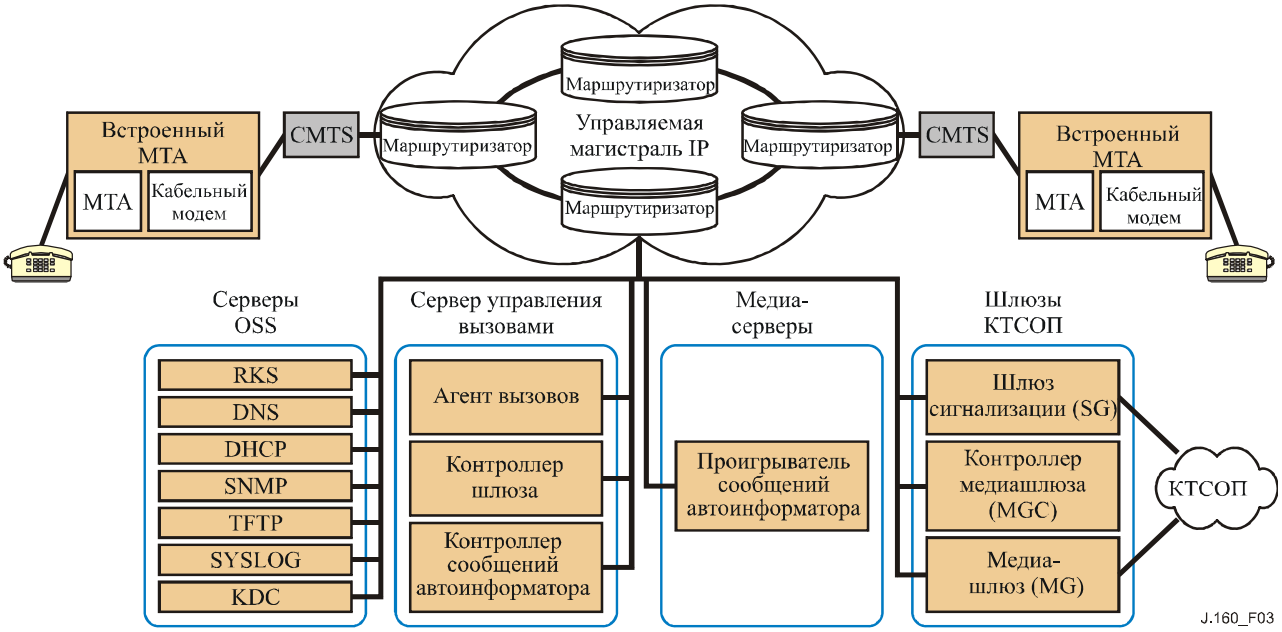


Рисунок 3/J.160 – Эталонная модель компонентов IPCablecom

В архитектуре IPCablecom существуют доверенные и недоверенные элементы. Доверенные сетевые элементы, как правило, располагаются внутри управляемой магистрали Оператора кабельной сети. Недоверенные элементы, такие как CM и MTA, как правило, располагаются дома у абонента и вне оборудования Оператора кабельной сети.

6.1 Адаптер медиатерминала (MTA)

MTA представляет собой клиентское устройство IPCablecom, содержащее абонентскую часть интерфейса с CPE абонента (например, телефоном) и сетевую часть сигнального интерфейса с элементами контроля вызовов в сети. MTA предоставляет кодеки и все функции сигнализации и инкапсуляции, требующиеся для транспортировки медиаинформации и сигнализации вызовов.

MTA располагаются на стороне потребителя и подключены к другим сетевым элементам IPCablecom посредством сети доступа HFC (Рек. МСЭ-Т J.112). От MTA IPCablecom требуется поддержка протокола Сетевой сигнализации вызовов (NCS) (Рек. МСЭ-Т J.162).

Встроенный MTA (E-MTA) представляет собой единое аппаратное устройство, совмещающее кабельный модем и компонент MTA IPCablecom. На рисунке 4 приведена типичная функциональная диаграмма E-MTA.

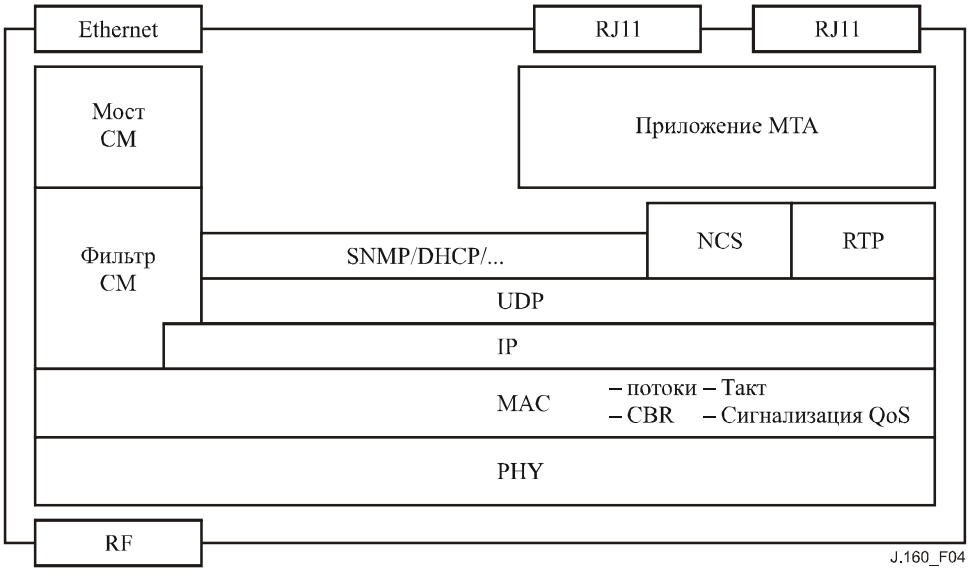


Рисунок 4/J.160 – Концептуальная функциональная архитектура E-MTA

6.1.1 Функциональные требования к MTA

На MTA возложена ответственность за выполнение следующих функций:

- Сигнализация вызовов NCS с CMS.
- Сигнализация QoS с CMS и CMTS.
- Аутентификация, конфиденциальность и целостность некоторых сообщений между MTA и другими сетевыми элементами IPCablecom.
- Распределение медиапотоков по услугам MAC сети доступа DOCSIS.
- Кодирование/декодирование медиапотоков.
- Обеспечение нескольких аудиоиндикаторов для телефонов, таких как тональный сигнал вызова, тональный сигнал отложенного вызова, прерывистый сигнал готовности сети к соединению, готовность сети к соединению и т. п.
- Стандартная сигнализация аналоговой линии КТСОП для аудиосигналов, передачи голоса, сигнализации определения номера звонящего, DTMF и индикаторов ожидающего сообщения голосовой почты.
- Аудиокодеки G.711 и аудиокодеки с низкой частотой дискретизации.
- Один или более аналоговый интерфейс и/или интерфейс ISDN BRI .

Дополнительные функции MTA определены в других Рекомендациях IPCablecom.

6.1.2 Атрибуты MTA

E-MTA характеризуется следующими атрибутами:

- Встроенный MTA имеет два адреса MAC: один для CM и один для MTA.
- Встроенный MTA имеет два адреса IP: один для CM и один для MTA.
- Встроенный MTA имеет два Полных доменных имени узла (FQDN): одно для CM и одно для MTA.
- Как минимум один телефонный номер на каждый сконфигурированный физический порт.
- Возможности устройства.
- Связанный с MTA CMS.

6.2 Кабельный модем

CM представляет собой модулятор/демодулятор, располагающийся в помещении потребителя и обеспечивающий передачу данных по кабельной сети с использованием протокола DOCSIS. В IPCablecom CM играет ключевую роль в обработке медиапотоков и предоставляет такие услуги, как классификация трафика по потокам услуг, формирование скорости передачи и выстраивание очереди на основе приоритетов.

6.3 Сеть доступа HCF

Услуги на основе IPCablecom передаются по гибридной волоконно-коаксиальной (HFC) сети доступа. Сеть доступа представляет собой двунаправленную систему с совместным использованием среды, которая состоит из CM, CMTS, а также уровней доступа MAC и PHY DOCSIS.

6.4 Система завершения кабельного модема (CMTS)

CMTS обеспечивает связь для передачи данных и работы с CM по сети доступа HFC. Она также обеспечивает связь с глобальными сетями. CMTS располагается на головном узле системы кабельного телевидения или в распределительном концентраторе.

CMTS отвечает за выполнение следующих функций:

- Обеспечение CM требуемого QoS на основе запросов DOCSIS, которые проверяются на соответствие политике.
- Распределение ширины полосы пропускания для "восходящего" потока данных в соответствии с запросами CM и политиками QoS сети.
- Классификация всех поступающих от сетевой части интерфейса пакетов и присвоение им уровня QoS на основе определенных спецификаций фильтра.
- Проверка содержимого поля TOS в полученных из кабельной сети пакетах на соответствие политикам для того, чтобы принудительно устанавливать значение поля TOS в соответствии с политикой оператора сети.
- Изменение содержимого поля TOS в заголовках IP "нисходящего" потока данных в соответствии с политикой оператора сети.
- Осуществление формирования трафика и проверки на соответствие политикам, как того требует спецификация потока.
- Перенаправление пакетов "нисходящего" потока данных в сеть DOCSIS с использованием назначенного QoS.
- Перенаправление пакетов "восходящего" потока данных устройствам магистрали с использованием назначенного QoS.
- Преобразование параметров QoS Шлюза в параметры QoS DOCSIS.
- Ведение записей об использовании ресурсов для каждого вызова с использованием Сообщений о событиях IPCablecom.

6.4.1 Шлюз CMTS

CMTS отвечает за распределение и планирование выделения ширины полосы пропускания для "нисходящих" и "восходящих" потоков данных в соответствии с запросами MTA и авторизациями QoS, установленными Контроллером шлюза.

CMTS реализует Динамический шлюз QoS IPCablecom или Шлюз CMTS между кабельной сетью DOCSIS и магистралью IP. Шлюз CMTS представляет собой функциональный компонент CMTS, осуществляющий классификацию трафика и следящий за выполнением политики QoS в медиапотоках в соответствии с указаниями Контроллера шлюза (GC). Шлюз CMTS контролируется Контроллером шлюза (GC), логическим управляющим компонентом QoS внутри CMS, координирующим все действия по авторизации и контролю Качества обслуживания.

6.5 Сервер управления вызовами

Сервер управления вызовами обеспечивает контроль вызовов и услуги, связанные с сигнализацией для MTA, CMTS, и шлюзов КТСОП в сети IPCablecom. CMS является доверенным сетевым элементом и располагается в управляемом сегменте IP сети IPCablecom.

CMS IPCablecom состоит из следующих логических компонентов IPCablecom:

– **Агент вызовов (CMS/CA)** – термины "Агент вызовов" и CMS часто используются как взаимозаменяемые, особенно в MGCP (Протокол контроля медиашлюза). В IPCablecom термином Агент вызовов (CA) обозначается контрольный компонент CMS, отвечающий за предоставление MTA услуг сигнализации с использованием протокола NCS (Рек. МСЭ-Т J.162). В данном контексте обязанности Агента вызовов включают (однако не ограничиваются этим):
  - реализацию функциональных возможностей вызова;
  - поддержание информации о состоянии вызова;
  - использование кодеков внутри абонентского устройства MTA;
  - сбор и предварительную обработку набранных цифр;
  - сбор и классификацию действий пользователя;
  - контроль над использованием MTA параметров VoIP.
– **Контроллер шлюза (CMS/GC)** – Контроллер шлюза (GC) представляет собой логический управляющий компонент QoS внутри CMS, координирующий все действия по авторизации и контролю QoS. Функции Контроллера шлюза определены в Рекомендации по Динамическому качеству обслуживания.

CMS может также содержать следующие логические компоненты:

– **Контроллер медиашлюза** – MGC представляет собой логический компонент управления сигнализацией, используемый для контроля над Медиашлюзами КТСОП. Работа MGC детально описана далее в данном пункте.

CMS может также выполнять следующие функции:

- Управление вызовами и расширенные функциональные возможности;
- Служба каталогов и трансляция адресов;
- Маршрутиризация вызова;
- Ведение записей об использовании услуг переносимости местного номера.

В рамках данной Рекомендации протоколы, реализующие функциональные возможности CMS, указаны как завершающиеся в CMS: в конкретных реализациях данные функциональные возможности могут быть распределены на один или более серверов, расположенных "за" Сервером управления вызовами.

6.6 Шлюз КТСОП

В рамках IPCablecom MTA имеют возможность взаимодействовать с существующей сетью КТСОП при помощи Шлюзов КТСОП.

Для того чтобы дать операторам возможность минимизировать издержки и оптимизировать компоновку их взаимосвязей с КТСОП, Шлюз КТСОП разделен на три функциональных компонента:

- **Контроллер медиашлюза (MGC)** – MGC поддерживает состояние вызова и контролирует общее поведение шлюза КТСОП.
- **Шлюз сигнализации (SG)** – SG предоставляет функцию взаимосвязи сигнализации между сетью сигнализации SS7 КТСОП и сетью IP.
- **Медиашлюз (MG)** – MG завершает путь широкополосного канала и преобразует медиаинформацию, которой обмениваются сеть КТСОП и сеть IP.

6.6.1 Контроллер медиашлюза (MGC)

Контроллер медиашлюза (MGC) принимает и выступает посредником при передаче информации сигнализации вызовов между сетью IPCablecom и КТСОП. Он поддерживает и контролирует общее состояние вызовов для вызовов, требующих взаимосвязи с КТСОП.

MGC контролирует MG путем выдачи ему указаний на создание, изменение и удаление соединений, поддерживающих поток медиаинформации по сети IP. MGC также предписывает MG обнаруживать и создавать события и сигналы, такие, как тоновые сигналы проверки целостности для магистральных линий ISUP. Каждая магистральная линия представлена как конечная точка.

Ниже приводится список функций, выполняемых Контроллером медиашлюза:

- **Функция контроля вызовов** – поддержание и контроль общего состояния вызовов Шлюза КТСОП для тех вызовов, которые проходят через Шлюз КТСОП. Данная функция поддерживает связь с внешними элементами КТСОП, как это необходимо для контроля вызовов Шлюза КТСОП, например, путем создания очередей TCAP.
- **Сигнализация IPCablecom** – завершает и создает входящую и исходящую сигнализацию вызовов IPCablecom-сегмента сети.
- **Контроль MG** – Функция Контроля MG осуществляет общий контроль над конечными точками в медиашлюзе:
  - Обнаружение событий предписывает MG обнаруживать события, например, внутриполосные тоновые сигналы на конечных точках и, возможно, соединениях.
  - Создание сигналов предписывает MG создавать внутриполосные тоновые сигналы и сигналы на конечных точках и, возможно, соединениях.
  - Контроль соединений предписывает MG выполнять базовую обработку входящих и исходящих соединений конечных точек в MG.
  - Контроль атрибутов указывает MG, какие атрибуты применять к конечной точке и/или соединению, например, метод кодирования, использование устранения эффекта эха, параметры безопасности и т. п.
- **Мониторинг внешних ресурсов** – поддерживает осведомленность MGC о видимых вовне ресурсах MG и пакетных ресурсах сети, например, доступности конечных точек и т. п.
- **Маршрутиризация вызовов** – принимает решения, связанные с маршрутиризацией вызовов.
- **Безопасность** – обеспечивает соответствие всех объектов, контактирующих с MGC, требованиям к безопасности.
- **Ведение записей об использовании посредством Сообщений о событиях** – ведет записи об использовании ресурсов для каждого вызова.

6.6.2 Медиашлюз (MG)

Медиашлюз предоставляет соединения широкополосного канала между сетями КТСОП и IP. Каждый широкополосный канал представлен как конечная точка, и MGC предписывает MG устанавливать и контролировать соединения с другими конечными точками в сети IPCablecom. MGC также предписывает MG обнаруживать и создавать сообщения и сигналы, относящиеся к известному состоянию вызова к MGC.

6.6.2.1 Функции медиашлюза

Ниже приводится список функций, выполняемых медиашлюзом:

- Завершение и контроль над физическими схемами в форме широкополосных каналов из КТСОП.
- Обнаружение события на конечных точках и соединениях, как запрашивается MGC.
- Создание сигналов на конечных точках и соединениях, например, проверки целостности, по указанию MGC.
- Создание, изменение и удаление входящих и исходящих соединений с другими конечными точками, как предписывается MGC.
- Контроль и назначение внутренних ресурсов обработки медиаинформации конкретным соединениям по получении запросов от Контроллера медиашлюза.

- Осуществление преобразования медиаинформации между сетями IPCablecom и КТСОП. Это включает все аспекты преобразования, такие как сжатие/восстановление (кодек), устранение эффекта эха и т. п.
- Обеспечение соответствия всех объектов, контактирующих с MG, требованиям к безопасности.
- Определение использования соответствующих ресурсов и связанных с ними атрибутов этих ресурсов (например, количество байт принятой и отправленной медиаинформации).
- Отчет MGC об использовании сетевых ресурсов.

6.6.3 Шлюз сигнализации

В функции Сигнального шлюза входит отправка и прием сигнализации коммутируемой сети на границе сети IPCablecom. Для IPCablecom Шлюз сигнализации поддерживает только "не привязанную к оборудованию" сигнализацию в форме SS7.

6.6.3.1 Функции сигнального шлюза SS7

Ниже приводится список функций, выполняемых Шлюзом сигнализации:

- Завершение физических линий сигнализации SS7 от КТСОП (линии A, F).
- Реализация функциональных возможностей безопасности для обеспечения соответствия безопасности Шлюза требованиям к сетевой безопасности IPCablecom и SS7.
- Завершение уровней 1, 2 и 3 Подсистемы передачи сообщений (MTP).
- Реализация функции управления сетью MTP, как требуется от любой точки сигнализации SS7.
- Осуществление установления соответствия адресов ISUP для поддержки гибкого установления соответствия Кодов точек (как Кодов точек-источников, так и Кодов точек-получателей) и/или комбинаций Код точки/Код CIC, содержащихся в сообщениях ISUP SS7, с соответствующим Контроллером медиашлюза (MGC) (его доменным именем или адресом IP). Адресуемый MGC будет ответственен за контроль над Медиашлюзом, завершающим соответствующие магистральные линии.
- Осуществление установления соответствия адресов TCAP для того, чтобы установить соответствие между комбинациями Код точки/Глобальное наименование/Номер подсистемы SCCP в сообщениях TCAP и соответствующим Контроллером медиашлюза или Сервером управления вызовами.
- Предоставление механизма запроса внешних баз данных КТСОП при помощи сообщений TCAP, отправляемых по сети SS7, некоторым доверенным объектам ("пользователям TCAP") сети IPCablecom, например, Агентам вызовов.
- Реализация транспортного протокола, требующегося для транспортировки информации сигнализации между Шлюзом сигнализации и Контроллером медиашлюза.

6.7 Вспомогательные компоненты Системы операционной поддержки (OSS)

Вспомогательная система OSS включает бизнес-компоненты, компоненты обслуживания и компоненты управления сетью, поддерживающие основные бизнес-процессы. Согласно определению TMN ITU, основными функциональными сферами OSS являются управление сбоями, управление производительностью, управление безопасностью, управление учетом и управление конфигурацией.

В рамках IPCablecom определен ограниченный набор функциональных компонентов и интерфейсов OSS для поддержки инициализации и подготовки к работе устройства MTA и переноса информации, касающейся выставления счетов на оплату за услуги, посредством Сообщений о событиях.

6.7.1 Сервер безопасности – Центр распределения ключей (KDC)

В рамках IPCablecom термин KDC используется применительно к серверу безопасности Kerberos. Для управления ключами на интерфейсах между MTA и CMS и Сервером инициализации и подготовки к работе используется протокол Kerberos с расширением открытого ключа PKINIT.

Вслед за аутентификацией MTA с использованием протокола PKINIT, KDC выдает MTA мандат Kerberos. Мандат содержит информацию для конфигурирования безопасности для сигнализации

вызовов между MTA и CMS (если MTA должен связываться с CMS посредством безопасного интерфейса) и для интерфейса управления между MTA и Сервером инициализации и подготовки к работе (если MTA должен управляться через безопасный интерфейс). Мандаты выдаются:

- В ходе инициализации и подготовки к работе устройства. В случае если MTA перезагружается и сохраненный мандат все еще является действительным, MTA не требуется запускать обмен PKINIT для запроса нового мандата от KDC.
- Когда время действия мандата истекает. В нормальных условиях срок действия мандатов истекает приблизительно раз в неделю.

6.7.2 Сервер Динамического протокола конфигурирования узла (DHCP)

Сервер DHCP является вспомогательным сетевым элементом, используемым в процессе инициализации и подготовки к работе устройства MTA для динамического выделения адресов IP и другой информации по конфигурации клиента.

6.7.3 Сервер Доменной системы именования (DNS)

Сервер DNS представляет собой вспомогательный сетевой элемент, используемый для установления соответствия между доменными именами и адресами IP.

6.7.4 Сервер Тривиального протокола передачи данных или Сервер Протокола передачи гипертекста (TFTP или HTTP)

Сервер TFTP является вспомогательным сетевым элементом, используемым в ходе инициализации и подготовки к работе устройства MTA для загрузки конфигурационного файла в MTA. Вместо сервера TFTP для загрузки конфигурационных файлов на MTA может быть использован сервер HTTP.

6.7.5 Сервер SYSLOG (SYSLOG)

Сервер SYSLOG является необязательным вспомогательным элементом, используемым для сбора сообщений нотификации о событиях, указывающих, что определенные события, например такие, как ошибки устройств, имели место.

6.7.6 Сервер учетной информации (RKS)

RKS является компонентом доверенного элемента сети, получающего Сообщения о событиях IPCablecom от других доверенных сетевых элементов IPCablecom, таких, как CMS, CMTS и MGC. RKS также является, как минимум, краткосрочным хранилищем для Сообщений о событиях IPCablecom. RKS может собирать или связывать Сообщения о событиях в логические наборы (Детальная информация о вызове (CDR)), которые затем делаются доступными для вспомогательных систем, таких как система выставления счетов на оплату или система обнаружения мошенничества.

6.8 Сервер сообщений автоинформатора (ANS)

Сервер объявлений является сетевым компонентом, который управляет информационными тональными сигналами и сообщениями и воспроизводит их в ответ на события, происходящие в сети. Сервер сообщений автоинформатора (ANS) представляет собой логический объект, состоящий их Контроллера сообщений автоинформатора (ANC) и Проигрывателя сообщений автоинформатора (ANP).

6.8.1 Контроллер сообщений автоинформатора (ANC)

ANC инициирует и управляет всеми услугами сообщений автоинформатора, предоставляемыми Проигрывателем сообщений автоинформатора. ANC запрашивает от ANP проигрывание объявлений на основе состояния вызова, определяемого CMS. Когда ANP получает от конечного пользователя информацию, ANC отвечает за ее интерпретацию и управление сеансом в соответствии с полученной информацией. Следовательно, ANC также может управлять состоянием вызова.

6.8.2 Проигрыватель сообщений автоинформатора (ANP)

Проигрыватель сообщений автоинформатора представляет собой сервер медиаресурсов. Он отвечает за получение и интерпретацию команд ANC и за доставку MTA соответствующих(го) сообщений(я)

автоинформатора. ANP также отвечает за прием ввода пользователя и отчет о введенной информации (например, тональных сигналах DTMF). ANP функционирует под контролем ANC.

7 Интерфейсы протокола

Спецификации протокола определены для большинства интерфейсов компонентов архитектуры IPCablecom. В данном пункте приводится обзор каждого интерфейса протокола. Для получения полных требований протоколов следует обращаться к отдельным Рекомендациям IPCablecom.

Возможно, что некоторые из этих интерфейсов не будут присутствовать в реализациях продуктов некоторыми производителями. Например, если несколько функциональных компонентов IPCablecom объединены, возможно, что некоторые из этих интерфейсов будут внутренними для данного компонента.

7.1 Интерфейсы сигнализации вызовов

Для Сигнализации вызовов требуется нескольких интерфейсов внутри архитектуры IPCablecom. Данные интерфейсы показаны на рисунке 5. Каждый интерфейс на диаграмме снабжен меткой и описан в таблице 2, ниже.

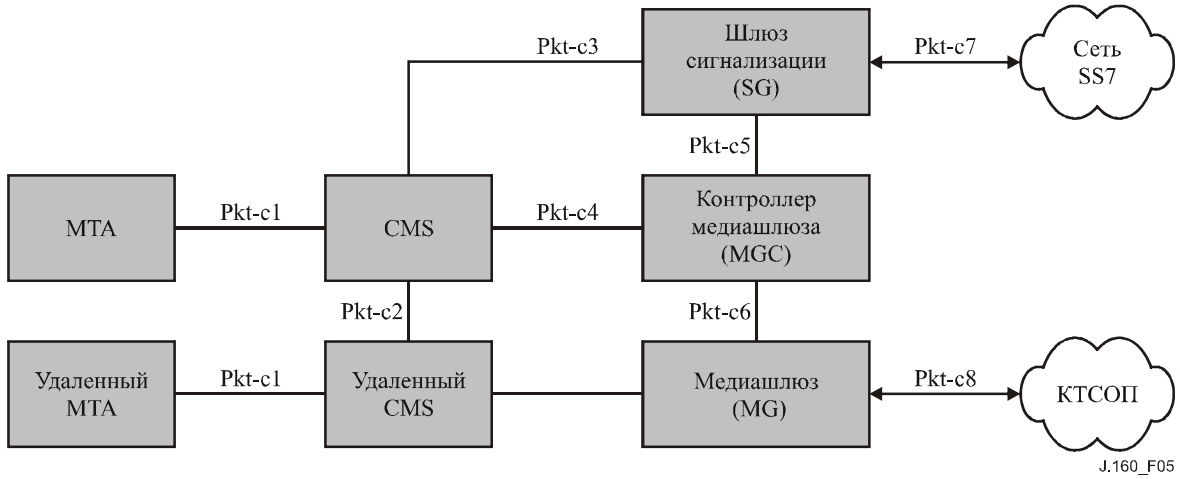


Рисунок 5/J.160 – Интерфейсы сигнализации вызовов

Таблица 2/J.160 – Интерфейсы сигнализации вызовов

Интерфейс	Функциональные компоненты IPCablecom	Описание
Pkt-c1	MTA ↔ CMS	Сообщения Сигнализации вызовов, которыми обмениваются MTA и CMS по протоколу NCS, являющемуся профилем MGCP.
Pkt-c2	CMS ↔ CMS	Сообщения Сигнализации вызовов, которыми обмениваются CMS. Протоколом для данного интерфейса является CMSS (Рек. МСЭ-Т J.178).
Pkt-c3	CMS ↔ SG	Сообщения Сигнализации вызовов, которыми обмениваются CMS и SG.
Pkt-c4	CMS ↔ MGC	Сообщения Сигнализации вызовов, которыми обмениваются CMS и MGC. Протоколом для данного интерфейса является CMSS.
Pkt-c5	SG ↔ MGC	Сообщения Сигнализации вызовов, которыми обмениваются MGC и SG.
Pkt-c6	MGC ↔ MG	Интерфейс для контроля над медиашлюзом с использованием протокола TGCP, который является профилем MGCP, аналогично NCS.

Таблица 2/J.160 – Интерфейсы сигнализации вызовов

Интерфейс	Функциональные компоненты IPCablecom	Описание
Pkt-c7	SG ↔ SS7	SG завершает физические линии сигнализации SS7 от КТСОП (линии A, F). Поддерживаются следующие протоколы: • Интерфейс пользователя ISUP: Предоставляет интерфейс сигнализации ISUP SS7 внешним поставщикам услуг связи КТСОП. • Интерфейс пользователя TCAP: Предоставляет механизм запроса внешних баз данных КТСОП при помощи сообщений TCAP, отправляемых по сети SS7, некоторым доверенным объектам ("пользователям TCAP") сети IPCablecom, например, Агентам вызовов.
Pkt-c8	MG ↔ КТСОП	Данный интерфейс определяет возможность подключения широкополосных каналов от Медиашлюза к КТСОП.

7.1.1 Структура Сигнализации вызовов на основе сети (NCS)

Протокол Сигнализации вызовов на основе сети (NCS) IPCablecom (Pkt-c1) является расширенным вариантом протокола сигнализации вызовов MGCP IETF. В соответствии с архитектурой NCS все состояния вызова и функциональные возможности реализуются в централизованном компоненте – Сервере управления вызовами (CMS), а логический аппарат управления устройством располагается в MTA. MTA передает события устройства CMS и отвечает на команды, которые отдает CMS. CMS, который может состоять из нескольких географически или административно разделенных систем, отвечает за установление и прекращение вызовов, предоставление расширенных услуг (расширенные возможности вызовов), осуществление авторизации вызовов, создание записей о событиях для выставления счетов на оплату и т. п.

Примером разделения функций может служить следующий порядок действий: CMS предписывает MTA проинформировать CMS, когда поднимается телефонная трубка и вводится соответствующий набор цифр DTMF. Когда имеет место данная последовательность событий, MTA оповещает CMS. После этого CMS может предписать MTA создать соединение, зарезервировать ресурсы QoS для ожидающего голосового соединения через сеть доступа, а также воспроизвести локально тональный сигнал обратного вызова. CMS, в свою очередь, связывается с удаленным CMS (или MGC) для того, чтобы установить вызов. Когда CMS обнаруживает ответ на удаленном конце, он предписывает MTA прекратить воспроизведение тонального сигнала обратного вызова, активировать соединение для передачи медиаинформации между MTA и удаленным MTA и начать передавать и принимать пакеты медиапотока.

При помощи централизации состояния вызова и обработки услуг в CMS поставщик услуги имеет возможность централизованно управлять надежностью оказываемых услуг. Дополнительно поставщик услуг получает полный доступ к программному и аппаратному обеспечению в случае возникновении дефекта, влияющего на абонентские услуги. Программное обеспечение может централизованно контролироваться и обновляться в течение коротких циклов отладки и разрешения проблем, что не требует нахождения специалистов по эксплуатации в помещении потребителя. Дополнительно поставщик услуг имеет прямой контроль над предлагаемыми услугами и связанными с ними потоками доходов.

7.1.2 Структура сигнализации КТСОП

Интерфейсы сигнализации КТСОП обобщены в таблице 2 (от Pkt-c3 до Pkt-c8). Данные интерфейсы предоставляют доступ к услугам на базе КТСОП и к абонентам КТСОП из сети IPCablecom.

Структура сигнализации КТСОП IPCablecom состоит из шлюза КТСОП, который подразделяется на три функциональных компонента:

- Контроллер медиашлюза (MGC);
- Медиашлюз (MG);

- Шлюз сигнализации (SG).

Контроллер медиашлюза и Медиашлюз аналогичны, соответственно, CMS и MTA в структуре NCS. Медиашлюз предоставляет возможность подключения широкополосных каналов и внутриполосной сигнализации к КТСОП. Контроллер медиашлюза реализует логический аппарат и все состояния вызовов и контролирует работу Медиашлюза посредством протокола TGCP (J.171) (Pkt-c6). Это включает создание, изменение и удаление соединений. TGCP является расширенным вариантом протокола сигнализации вызовов MGCP IETF. Вариант TGCP очень близок к NCS.

Как CMS, так и MGC могут отправлять маршрутиризационные запросы (например, поиск бесплатного номера, поиск LNP) Контрольным точкам услуг SS7 посредством SG (Pkt-c3 и Pkt-c5). MGC также обменивается сигнализацией ISUP посредством SG с объектами SS7 КТСОП для целей контроля и управления магистральными линиями.

7.1.3 Структура сигнализации CMS-CMS

В рамках IPCablecom поддерживается как междоменная, так и внутридоменная сигнализация CMS-CMS и CMS-MGC, как определено в Рекомендации CMSS, Рек. МСЭ-T J.178. Архитектура сигнализации CMSS основана на Протоколе инициации сеанса (SIP) IETF (IETF RFC 3261). CMSS определяет протокол сигнализации вызовов. Он не касается маршрутиризации в сети.

CMS включает Клиента агента пользователя (UAC) и Сервер агента пользователя (UAS) SIP. Агент пользователя поддерживает состояние вызова в течение "жизни" вызова и отслеживает MTA на предмет изменений в состоянии, влияющих на вызов. Интерфейсом между CMS и MTA является NCS. Сообщения CMSS для создания нового вызова или изменения атрибутов или участников активного вызова создаются по инициативе CMS. CMS, в свою очередь, обычно делает это вследствие получения сигнализации от MTA, например, в результате получения сообщения NCS, информирующего о введенных цифрах. CMS включает функцию Контроллера шлюза (GC). Часть CMS, являющаяся Агентом пользователя, принимает участие в сигнализации CMSS, а часть, являющаяся Контроллером шлюза, принимает участие в сигнализации DQoS. Совместно они контролируют координацию сигнализации для установления вызовов и управления ресурсами.

7.2 Медиапотоки

Для транспортировки всех медиапотоков в сети IPCablecom используется стандартный RTP IETF (RFC 1889, *RTP: A Transport Protocol for Real-Time Applications (Транспортный протокол для приложений режима реального времени)*). В рамках IPCablecom используется профиль RTP для аудио- и видеопотоков, как определено в IETF RFC 1890 (*RTP Profile for Audio and Video Conferences with Minimal Control (Профиль RTP для аудио- и видеоконференций с минимальным контролем)*).

Основные пути медиапотоков в архитектуре сети IPCablecom показаны на рисунке 6 и описаны ниже.

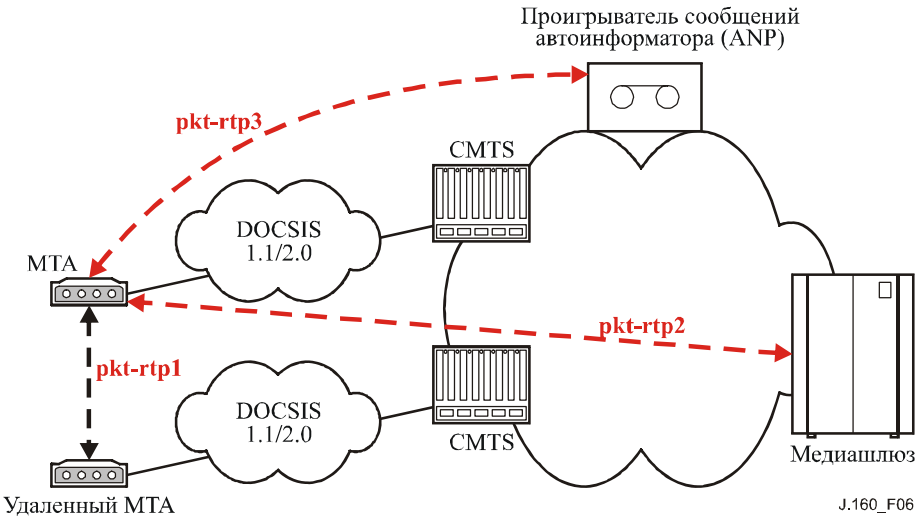


Рисунок 6/J.160 – Движение медиапотоков RTP в сети IPCablecom

Таблица 3/J.160 – Движение медиапотоков RTP

Интерфейс	Функциональные компоненты IPCablecom	Описание
pkt-rtp1	MTA ↔ MTA	Медиапоток между MTA. Включает, например, кодированную голосовую или факсимильную информацию.
pkt-rtp2	MTA ↔ MG	Медиапоток между MG и MTA. Включает, например, тональные сигналы, сообщения автоинформатора и медиапоток КТСОП.
pkt-rtp3	MTA ↔ ANP	Медиапоток между ANP и MTA. Включает, например, тональные сигналы, сообщения автоинформатора, отправляемые MTA Проигрывателем сообщений автоинформатора.

RTP кодирует один канал мультимедийной информации в одном направлении. Внутри каждого заголовка RTP 7-битное поле Payload Type (Тип полезной нагрузки, PT) указывает, какой алгоритм кодирования (например, G.711) используется внутри пакета полезной нагрузки. Большинство наиболее распространенных аудиоалгоритмов назначены конкретным значениям типов полезной нагрузки в диапазоне от 0 до 95. Диапазон от 96 до 127 зарезервирован для "динамических" типов полезной нагрузки RTP, где связь между алгоритмом кодирования и типом полезной нагрузки устанавливается посредством сигнализации.

Формат пакета данных RTP, по IP по Ethernet показан на рисунке 7.

Рисунок 7/J.160 – Формат пакета RTP

Длина полезной нагрузки RTP, а также частоты, с которой передаются пакеты, зависит от алгоритма кодирования, заданного полем Payload Type.

Сеансы RTP устанавливаются динамически задействованными конечными точками, так что "всем известного" номера порта UDP для приема информации RTP нет. Для передачи конкретного адреса IP и порта UDP, используемого в ходе данного сеанса RTP IETF, был разработан Протокол описания сеанса (SDP). SDP используется как NCS, так и TGCP.

Объем служебной информации заголовка пакета для Ethernet, IP, UDP и RTP значителен по сравнению с типичным размером полезной нагрузки RTP, которая может иметь размер в 10 байт для пакетизированной голосовой информации. В Рекомендациях DOCSIS для данного случая предусмотрена возможность Скрытия заголовка полезной нагрузки для сокращения обыкновенных заголовков.

Для транспортировки факсимильной медиаинформации в сети IPCablecom также используется Рек. МСЭ-Т Т.38, для получения дополнительной информации см. п. 8.7.

7.2.1 Транспортный протокол режима реального времени (RTCP)

RTCP определен в IETF RFC 1889. Он основан на периодической передаче контрольных пакетов всем участникам сеанса с использованием того же механизма распределения, что и для пакетов данных. RTCP посредством обратной связи предоставляет информацию о качестве распределения данных. Это является неотъемлемой частью роли RTP как транспортного протокола и относится к функциям контроля потоков и перегрузок других транспортных протоколов. В рамках IPCablecom использование RTCP поддерживается всеми конечными точками.

Для того чтобы точнее оценивать качества передаваемой голосовой информации и более эффективно диагностировать сетевые проблемы, существуют расширения RTCP. Данные расширения называются Расширенными отчетами RTCP (RTCP XR) и определены в IETF RFC 3611. RTCP XR содержит многочисленные наборы параметров. В рамках IPCablecom на всех конечных точках поддерживаются только параметры голоса RTCP XR.

7.3 Инициализация и подготовка к работе MTA

Инициализация и подготовка к работе устройства MTA позволяет MTA регистрироваться в сети оператора и предоставлять абонентам услуги по сети HFC. Инициализация и подготовка к работе включает функции инициализации, аутентификации и регистрации, требуемые для инициализации и подготовки к работе устройства MTA. Рекомендация по Инициализации и подготовке к работе также включает определение атрибутов, требующихся в конфигурационном файле MTA. (См. рисунок 8.)

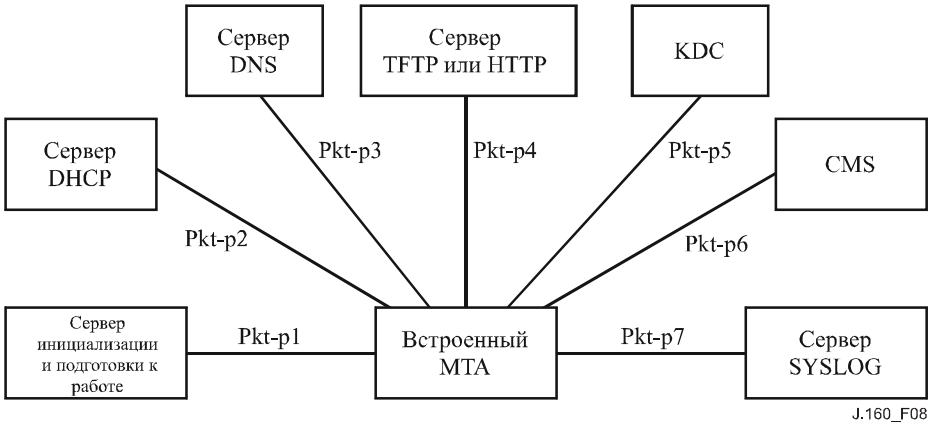


Рисунок 3/J.160 – Интерфейсы инициализации и подготовки к работе IPCablecom

В таблице 4 описаны интерфейсы инициализации и подготовки к работе, показанные на рисунке 8.

Таблица 4/J.160 – Интерфейсы инициализации и подготовки к работе устройства

Интерфейс	Функциональные компоненты IPCablecom	Описание
Pkt-p1	MTA ↔ Сервер инициализации и подготовки к работе (PROV)	Интерфейс для обмена информацией о возможностях устройств, а также информацией устройства MTA и конечной точки между MTA и Сервером инициализации и подготовки к работе с использованием протокола SNMP. MTA также отправляет оповещение о том, что инициализация и подготовка к работе завершены, а также статус успех/неудача по протоколу SNMP.
Pkt-p2	MTA ↔ Сервер DHCP	Интерфейс DHCP между MTA и Сервером DHCP, используемый для назначения MTA адреса IP и для предоставления дополнительной информации низкого уровня, используемой MTA при подключении к сети.
Pkt-p3	MTA ↔ Сервер DNS	Интерфейс DNS между MTA и Сервером DNS, используемый для получения адреса IP сервера IPCablecom, при условии, что известно его полное доменное имя.
Pkt-p4	MTA ↔ Сервер HTTP или TFTP	Конфигурационный файл MTA загружается на MTA с сервера TFTP или сервера HTTP.
Pkt-p5	MTA ↔ KDC	MTA получает мандат Kerberos от Центра распределения ключей, используя протокол Kerberos.
Pkt-p6	MTA ↔ CMS	MTA устанавливает Безопасное соединение по протоколу IPsec с CMS, используя протокол Kerberos.
Pkt-p7	MTA ↔ SYSLOG	Интерфейс, используемый MTA для отправки оповещений о событиях сети серверу SYSLOG, включая информацию, касающуюся статуса инициализации и подготовки к работе устройства.

7.4 Интерфейсы уровня управления элементами SNMP

В рамках IPCablecom требуется, чтобы SNMP связывал MTA с системами управления элементами для инициализации подготовки к работе устройства MTA. Для обработки событий поддерживаются прерывания (traps) и информационные сообщения (informs) SNMPv3, а для инициализации и подготовки к работе – установки (sets) и получения (gets) SNMPv3. MIB NCS IPCablecom содержит информацию по Сигнализации вызовов сети для инициализации и подготовки к работе как для отдельного устройства, так и для отдельной конечной точки. MIB MTA содержит данные для инициализации и подготовки устройства к работе, а также для поддержки подготовленных к работе функций, например, ведения журнала событий. Более подробная информация по MIB приводится в Рекомендации IPCablecom по структуре MIB (Рек. МСЭ-Т J.166).

7.5 Интерфейсы сообщений о событиях

7.5.1 Структура системы сообщений о событиях

Сообщение о событии представляет собой запись данных, содержащую информацию об использовании сети и ее деятельности. Отдельное Сообщение о событии может содержать как полный набор данных, касающихся использования сети, так и только часть всей информации. Будучи объединена на Сервере учетной информации (RKS), информация, содержащаяся в нескольких Сообщениях о событиях, формирует полную запись об обслуживании, предоставленном данному вызову. Данная полная запись часто называется Детальной информацией о вызове (CDR). Сообщения о событиях или CDR могут быть отправлены одному или нескольким вспомогательным приложениям, таким как система выставления счетов на оплату, система обнаружения мошенничества или обработчик предоплаченных услуг.

В Рекомендации по Сообщениям о событиях IPCablecom (Рек. МСЭ-Т J.164) определяется структура записи данных Сообщения о событиях, а также определяется RADIUS в качестве транспортного протокола. Структура записи данных Сообщения о событии организована таким образом, чтобы иметь возможность расширяться и гибко подстраиваться под условия, необходимые для передачи информации об использовании широкого спектра сетевых услуг. На рисунке 9 представлена типичная архитектура Сообщений о событиях.

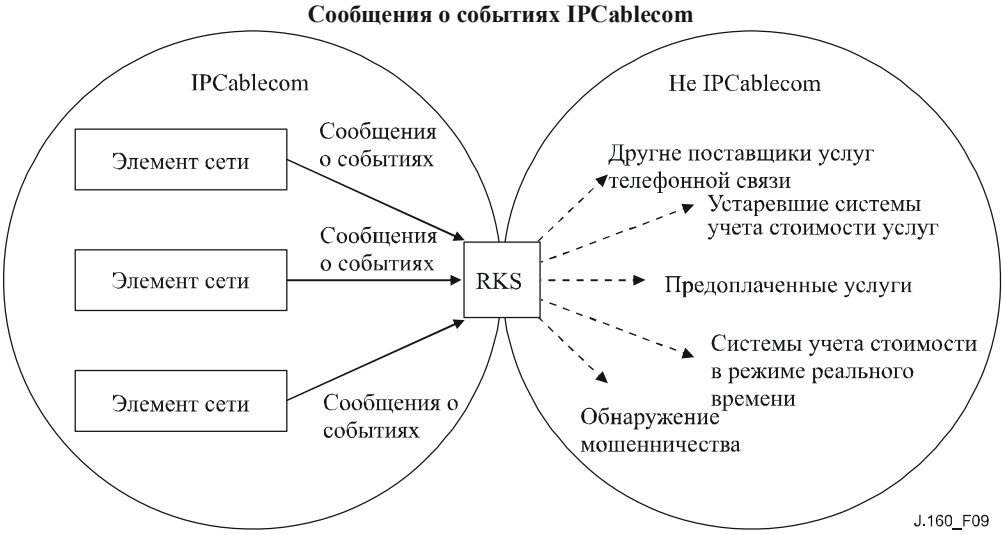
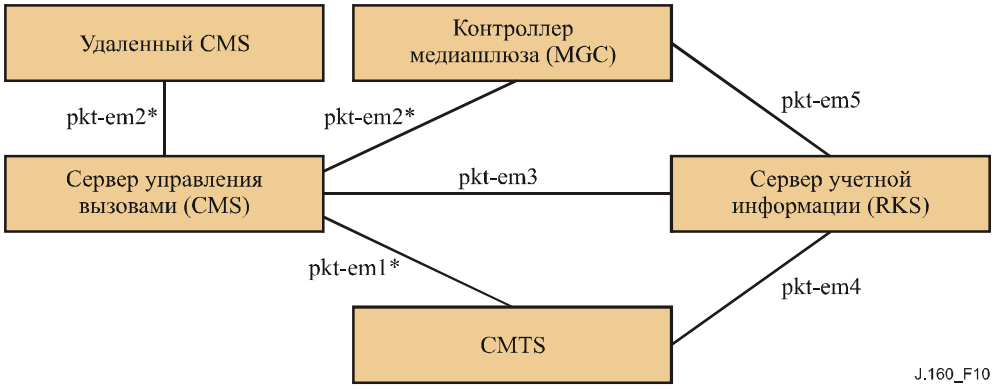


Рисунок 9/J.160 – Типичная архитектура Сообщения о событиях

В таблице 5 описаны интерфейсы, показанные на рисунке 10.

Таблица 5/J.160 – Интерфейсы Сообщений о событиях

Интерфейс	Функциональные компоненты IPCablecom	Описание
Pkt-em1	CMS ↔ CMTS	Сообщения Set Шлюза DQoS, несущие Идентификатор расчетной взаимосвязи (Billing Correlation ID) и другие данные, требующиеся для отправки CMTS Сообщений о событиях в адрес RKS.
Pkt-em2	CMS ↔ MGC CMS ↔ CMS	Протоколом для данного интерфейса является CMSS. Используется для переноса Идентификатора расчетной взаимосвязи и других данных, необходимых для выставления счетов на оплату.
Pkt-em3	CMS ↔ RKS	Протокол RADIUS, переносящий Сообщений о событиях IPCablecom.
Pkt-em4	CMTS ↔ RKS	Протокол RADIUS, переносящий Сообщений о событиях IPCablecom.
Pkt-em5	MGC ↔ RKS	Протокол RADIUS, переносящий Сообщений о событиях IPCablecom.



ПРИМЕЧАНИЕ. – * Указывает, что существующий сигнальный интерфейс используется для переноса данных, используемых для других интерфейсов Сообщений о событиях.

Рисунок 10/J.160 – Интерфейсы Сообщений о событиях

7.6 Качество обслуживания (QoS)

7.6.1 Структура QoS

Структура QoS IPCablecom представлена на рисунке 11:

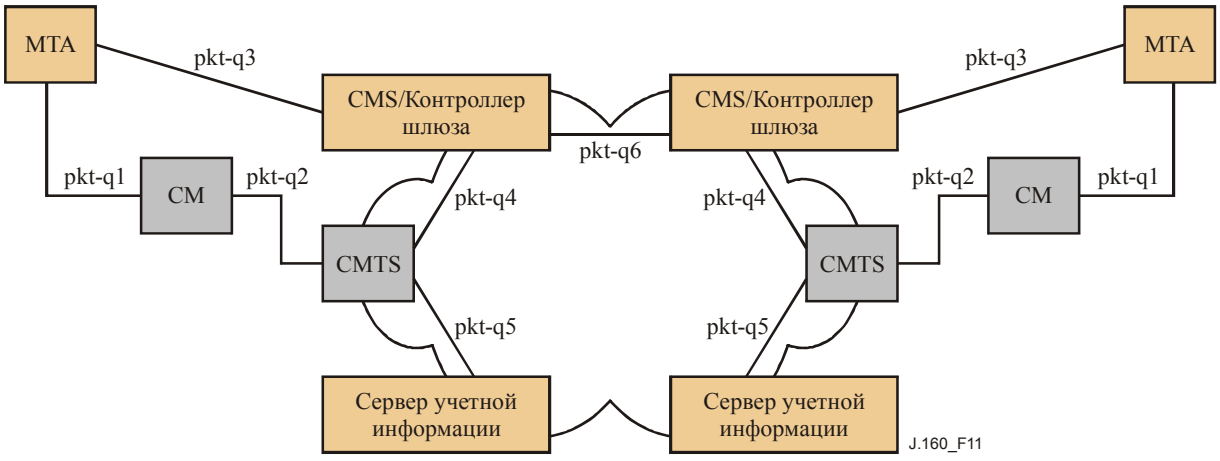


Рисунок 11/J.160 – Интерфейсы сигнализации QoS IPCablecom

В таблице 6 вкратце описаны все интерфейсы и то, каким образом каждый из интерфейсов используется в Рекомендации по Динамическому QoS (DQoS/Рек. МСЭ-Т J.163).

Таблица 6/J.160 – Интерфейсы QoS

Интерфейс	Функциональные компоненты IPCablecom	Описание DQoS
Pkt-q1	MTA ↔ CM	E-MTA, Интерфейс сервиса контроля MAC
Pkt-q2	CM ↔ CMTS	J.112, инициируется CM
Pkt-q3	MTA ↔ CMS	NCS
Pkt-q4	GC ↔ CMTS	Управление шлюзом
Pkt-q5	CMTS ↔ RKS	Выставление счетов на оплату
Pkt-q6	CMS ↔ CMS	Установление сеанса

Функции каждого из интерфейсов QoS описаны в таблице 7, ниже.

Таблица 7/J.160 – Интерфейсы QoS

Интерфейс	Функциональные компоненты IPCablecom	Описание
Pkt-q1	MTA ↔ CM	Данный интерфейс подразделяется на три подинтерфейса: *Контроль*: используется для управления потоками услуг DOCSIS и связанными с ними параметрами трафика и правилами классификации QoS. *Синхронизация*: используется для синхронизации пакетов и планирования с целью минимизации задержки и дрожания. *Транспорт*: используется для обработки пакетов в медиапотоке и осуществления соответствующей обработки QoS для каждого пакета. Интерфейс MTA/CM концептуально определен в Рек. МСЭ-Т J.112.
Pkt-q2	CM ↔ CMTS	Это интерфейс QoS DOCSIS (контроль, планирование и транспорт). Следует отметить, что, с точки зрения архитектуры, выполнение контрольных функций может быть инициировано только CM. CMTS является последней инстанцией в разрешении конфликтов, связанных с политиками, и принимает окончательные решения относительно допуска в сеть доступа DOCSIS. В рамках IPCablecom используются следующие возможности MAC DOCSIS: • Множественные потоки услуг, каждый со своим классом "восходящего" трафика, как с одним, так и с несколькими голосовыми соединениями на один поток услуги DOCSIS. • Классификация потоков трафика в потоки услуг с приоритетами. • Планирование с гарантированной минимальной/постоянной битовой скоростью передачи. • Планирование с постоянной битовой скоростью передачи с услугой обнаружения активности трафика (планированием замедления, ускорения, остановки и перезапуска). • Скрытие заголовков пакетов DOCSIS для увеличения плотности вызова. • Классификация потоков голосовой информации в потоки услуг DOCSIS. • Синхронизация CODEC (уплотнения/восстановления) с тактовым генератором и Интервалом предоставления (канала) CMTS. • Двухфазная активация ресурсов QoS. • Маркировка пакетов TOS на уровне сети. • Гарантии относительно уровня задержки и дрожания. • Внутренняя подуровневая сигнализация между CM и MTA IPCablecom (Встроенный MTA). Дальнейшее определение данного интерфейса приводится в Рек. МСЭ-Т J.112.

Таблица 7/J.160 – Интерфейсы QoS

Интерфейс	Функциональные компоненты IPCablecom	Описание
Pkt-q3	MTA ↔ CMS	Интерфейс сигнализации между MTA и CMS. Посредством данного интерфейса сигнализируются многие параметры, такие, как медиапоток, адреса IP, номера портов, а также выбор Кодека и пакетизации.
Pkt-q4	CMS ↔ CMTS	Данный интерфейс используется для управления динамическими шлюзами для сеансов медиапотоков. Этот интерфейс позволяет IPCablecom запрашивать и авторизовывать QoS.
Pkt-q5	CMTS ↔ RKS	Данный интерфейс используется CMTS для доклада об изменениях в ресурсах QoS, используемых вызовом. Этот интерфейс определен в Рекомендации по Сообщениям о событиях.
Pkt-q6	CMS ↔ CMS	Данный интерфейс используется для установления внтуридоменных и междоменных сеансов. Этот интерфейс включает функциональные возможности, позволяющие удостовериться в доступности ресурсов QoS на обоих концах соединения прежде, чем вызов будет установлен.

7.6.2 Динамическое качество обслуживания

Система Динамического качества обслуживания IPCablecom (DQOS) использует информацию сигнализации вызова в момент осуществления вызова с целью динамической авторизации ресурсов для вызова. Динамическое качество обслуживания позволяет предотвратить различные виды атак типа "кража услуги" путем интеграции обмена сообщениями QoS с другими протоколами и сетевыми элементами. Сетевые элементы, необходимые для контроля над Динамическим качеством обслуживания, показаны на рисунке 11.

Логический объект внутри CMTS, определяющий классификацию трафика и политику QoS для медиапотоков, называется Шлюзом. Элемент Контроллер шлюза CMS управляет Шлюзами для медиапотоков IPCablecom. В сигнализацию между GC и CMTS включается следующая ключевая информация:

Максимально допустимая граница QoS – Максимально допустимая граница QoS определяет максимальный объем ресурсов QoS (например, 2 предоставления по 160 байт за 10 мс), который MTA позволено запросить для широкополосного канала данного медиапотока. В случае, если MTA запрашивает значение большее, чем параметры, содержащиеся в данном ограничении, в выполнении запроса будет отказано.

Идентификационная информация конечных точек медиапотока – CG/CMS авторизует участников потока широкополосного канала медиапотока. Используя данную информацию CMTS может контролировать соответствие потоков данных политикам с тем, чтобы удостовериться в том, что как источник потока, так и его получатель авторизованы.

Получатель информации о стоимости услуг – GC/CMS сообщает CMTS идентификационную информацию первичного и вторичного Серверов учетной информации для данного вызова и предоставляет уникальный расчетный идентификатор, позволяющий связать записи, поступающие от нескольких элементов сети.

Роль каждого из компонентов IPCablecom в реализации DQoS описана ниже:

Сервер управления вызовами/Контроллер шлюза – CMS/GC отвечает за авторизацию QoS. Авторизация QoS может зависеть от типа вызова, типа пользователя или других параметров, определяемых политикой. CMS/GC также использует CMSS для того, чтобы удостовериться в том, что ресурсы QoS доступны на обоих концах вызова в случае выполнения внутридоменного или междоменного вызова.

CMTS – Используя информацию, полученную от CMS/GC, CMTS осуществляет контроль допуска запросов QoS и затем осуществляет контроль соблюдения допущенными потоками политик для того, чтобы удостовериться, что источник и получатель потока данных совпадают с участниками, которые

были авторизованы как конечные точки для данного потока. CMTS взаимодействует с сегментом CM MTA и с RKS. По отношению к каждому из этих элементов CMTS отвечает за:

- **CMTS – Сервер учетной информации** – CMTS оповещает Сервер учетной информации (RKS) каждый раз, когда происходят изменения в QoS между CMTS и MTA для конкретного вызова.
- **CMTS – MTA** – MTA выполняет динамические запросы на создание и изменение параметров трафика QoS, связанных с Динамическими потоками услуг DOCSIS, переносящих трафик широкополосного канала. Когда CMTS получает запрос, он проверяет, вписываются ли запрошенные характеристики в авторизованные границы QoS, а также авторизованы ли конечные точки медиапотока для переноса трафика. Если проверка заканчивается успешно, CMTS соответствующим образом создает или изменяет Динамические потоки услуг.

Сервер учетной информации (RKS) – RKS получает каждое событие (в форме Сообщения о событии), отправленное CMTS. Обычно RKS снабжен интерфейсом с одной или несколькими вспомогательными системами и переформатирует полученную от CMTS информацию и отправляет ее этим системам.

MTA – MTA представляет собой объект, с которым CMTS предоставляется Соглашение уровня услуг. MTA отвечает за правильное использование канала связи QoS (а CMTS отвечает за то, чтобы в принудительном порядке обеспечивать это правильное использование, поскольку MTA не является доверенным устройством). Если MTA пытается превысить установленные для трафика Соглашением уровня услуг границы, CMTS отвечает за то, чтобы MTA не получил запрошенный сверх ограничения уровень QoS.

7.7 Инициализация и подготовка к работе абонента CMS

Рекомендация по Инициализации и подготовке к работе абонента CMS предоставляет средства для автоматической активации услуг, определяя интерфейс между Сервером инициализации и подготовки к работе (или авторизованным вспомогательным компонентом) и CMS. Структура Инициализации и подготовки к работе абонента CMS показана на рисунке 12.

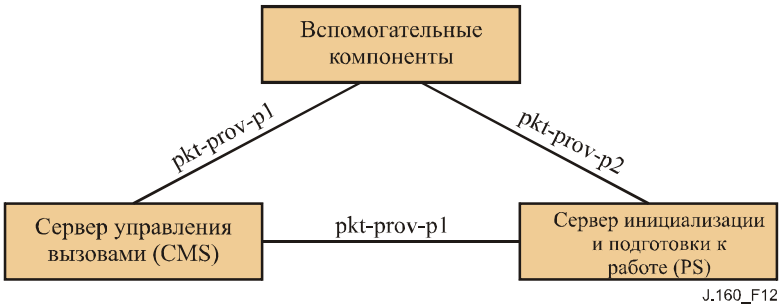


Рисунок 12/J.160 – Интерфейсы инициализации и подготовки к работе абонента CMS

Работа каждого из Интерфейсов инициализации и подготовки к работе абонента CMS описана в таблице 8, ниже.

Таблица 8/J.160 – Интерфейсы инициализации и подготовки к работе абонента CMS

Интерфейс	Функциональные компоненты IPCablecom	Описание
pkt-prov-p1	PS-CMS Back-office-CMS (Вспомогательные системы – CMS)	Это интерфейс Инициализации и подготовки к работе абонента CMS. Информация об абоненте может быть доставлена CMS либо PS, либо авторизованным вспомогательным компонентом.
pkt-prov-p2	Back-office-PS (Вспомогательные системы – PS)	Данный интерфейс позволяет вспомогательным компонентам обмениваться информацией с Сервером инициализации и подготовки к работе. Этот интерфейс не определен в рамках IPCablecom.

Инициализация и подготовка к работе абонента состоит из:

- **Поддержки ведения записей/выставления счетов на оплату** – Создание записи по абоненту, содержащей информацию, необходимую для доставки услуг, выставления счетов на оплату и приема платежей от потребителя. Создание записи потребителя/выставлении счетов на оплату является частью приложения вспомогательной системы OSS и в настоящий момент выходит за рамки IPCablecom.
- **Установка/конфигурирование оборудования** – Это может включать физическую установку и/или подключение оборудование, а также любое необходимое для реальной доставки услуг потребителю обновление программного обеспечения и/или баз данных. В плане Интерфейса Инициализации и подготовки к работе абонента CMS установка оборудования затрагивает CMS. Инициализация и подготовка к работе самого CMS может быть подразделена на две основные области:
  - **Базовая Инициализация и подготовка к работе Простой старой телефонной системы (POTS) (BPP)** – BPP предоставляет CMS минимальный набор данных, необходимый для маршрутиризации простых услуг телефонии (POTS) в сети IPCablecom. Данный минимальный набор состоит из телефонного номера, поставленного в соответствие с его FQDN MTA, и идентификатора конечной точки CMS. Эти данные используются для создания таблиц преобразования, позволяющих CMS маршрутиризировать вызовы к соответствующим устройствам/портам на основе предоставленного ему телефонного номера. Инициализация и подготовка к работе BPP для каждого потребителя требуется для того, чтобы этот потребитель мог получать вызовы в сети IPCablecom.
  - **Инициализация и подготовка к работе возможностей вызова (CFP)** – В дополнение к BPP осуществляется CFP для того, чтобы потребитель мог воспользоваться возможностями вызова. CFP более сложна, чем BPP, поскольку передаваемые параметры могут быть различными для разных возможностей, а также могут зависеть от особенностей реализации, определяемых производителем.

7.8 Электронное наблюдение

Система электронного наблюдения IPCablecom позволяет осуществлять Законодательно санкционированное электронное наблюдение (LAES) в сетях IPCablecom. В рамках IPCablecom поддерживается доставка данных о вызове и содержания вызова правоохранительным органам (LEA). Данные о вызове и содержание вызова доставляются от различных компонентов сети Средству доставки (Delivery Function, DF). DF отвечает за обобщение данных о вызове и содержания вызова, а также за последующую их доставку соответствующим правоохранительным органам. Правоохранительные органы работают со Средством сбора (Collection Function), которое отвечает за прием данных о вызове и содержания вызова от DF.

В рамках IPCablecom определяются только механизмы для осуществления электронного наблюдения. Здесь не определяется порядок административной обработки указания на осуществление электронного наблюдения (например, как оно принимается оператором IPCablecom и как впоследствии выполняется в сети).

Структура электронного наблюдения IPCablecom показана на рисунке 13.

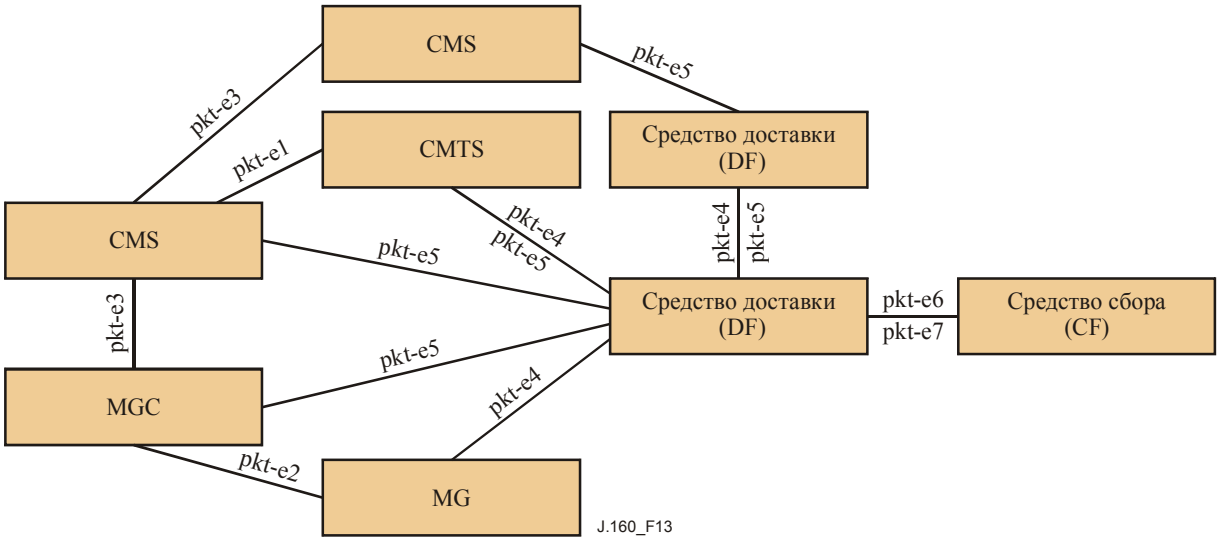


Рисунок 13/J.160 – Интерфейсы электронного наблюдения

Работа каждого из интерфейсов электронного наблюдения описана в таблице 9, ниже.

Таблица 9/J.160 – Интерфейсы электронного наблюдения

Интерфейс	Функциональные компоненты IPCablecom	Описание
pkt-e1	CMS ↔ CMTS	Это интерфейс DQoS COPS, позволяющий CMS включать наблюдение за данными о вызове и содержанием вызова.
pkt-e2	MGC ↔ MG	Данный интерфейс использует протокол TGCP, позволяющий MGC отдавать MG команду на начало электронного наблюдения.
pkt-e3	CMS ↔ CMS CMS ↔ MGC	Данный интерфейс использует протокол CMSS, поддерживающий возможность передачи для нужд электронного наблюдения в случае определенных внутридоменных или междоменных сценариев вызова.
pkt-e4	CMTS ↔ DF MG ↔ DF DF ↔ DF	Данный интерфейс основан на Сообщениях о событиях IPCablecom и используется для доставки данных о вызове от компонентов IPCablecom к DF или от DF к DF.
pkt-e5	CMTS ↔ DF MGC ↔ DF DF ↔ DF CMS ↔ DF	Данный интерфейс используется для доставки содержания вызова в форме инкапсулированных пакетов RTP от компонентов IPCablecom к DF или от DF к DF.
pkt-e6	DF ↔ CF	Данный интерфейс используется для доставки данных о вызове CF.
pkt-e7	DF ↔ CF	Данный интерфейс используется для доставки содержания вызова CF.

7.9 Безопасность

7.9.1 Обзор

Каждый из интерфейсов IPCablecom подвергается угрозам, которые могут повлечь за собой возникновение рисков, связанных с безопасностью, как в отношении абонента, так и в отношении поставщика услуг. В связи с наличием такого рода угроз в архитектуре IPCablecom предусмотрены базовые механизмы безопасности (такие, как IPsec) для каждого из определенных интерфейсов протокола, предоставляющие протоколу интерфейс с требующимися ему возможностями безопасности.

В рамках IPCablecom для большинства интерфейсов требуется использование определенных механизмов безопасности; для некоторых интерфейсов архитектурой допускается использование небезопасных соединений, хотя, поступая так, оператор подвергает абонентов и себя самого атакам, которые пресекаются, если соединения сделаны безопасными при помощи механизмов, определенных в Рекомендации по безопасности IPCablecom (Рек. МСЭ-Т J.170).

К числу услуг безопасности, доступных посредством основного уровня услуг IPCablecom, относятся аутентификация, контроль доступа и конфиденциальность. В интерфейсе протокола IPCablecom могут быть реализованы одна или несколько из перечисленных услуг, либо они могут не быть реализованы вообще, в зависимости от его конкретных потребностей в безопасности.

Безопасность IPCablecom выполняет требования к безопасности для каждого из входящих в систему интерфейсов протоколов путем:

- идентификации модели угрозы, характерной для каждого из входящих в систему интерфейсов протоколов;
- идентификации услуг безопасности (аутентификация, авторизация, конфиденциальность, целостность и неотказуемость), требующихся для нейтрализации идентифицированных угроз;
- указания конкретного механизма безопасности, предоставляющего требуемые услуги безопасности.

Механизмы безопасности включают как протокол безопасности (например, IPsec, безопасность уровня RTP или безопасность SNMPv3), так и поддерживающий протокол управления ключами (например, IKE или PKINIT/Kerberos).

На рисунке 14 приведена обобщенная схема интерфейсов безопасности IPCablecom.

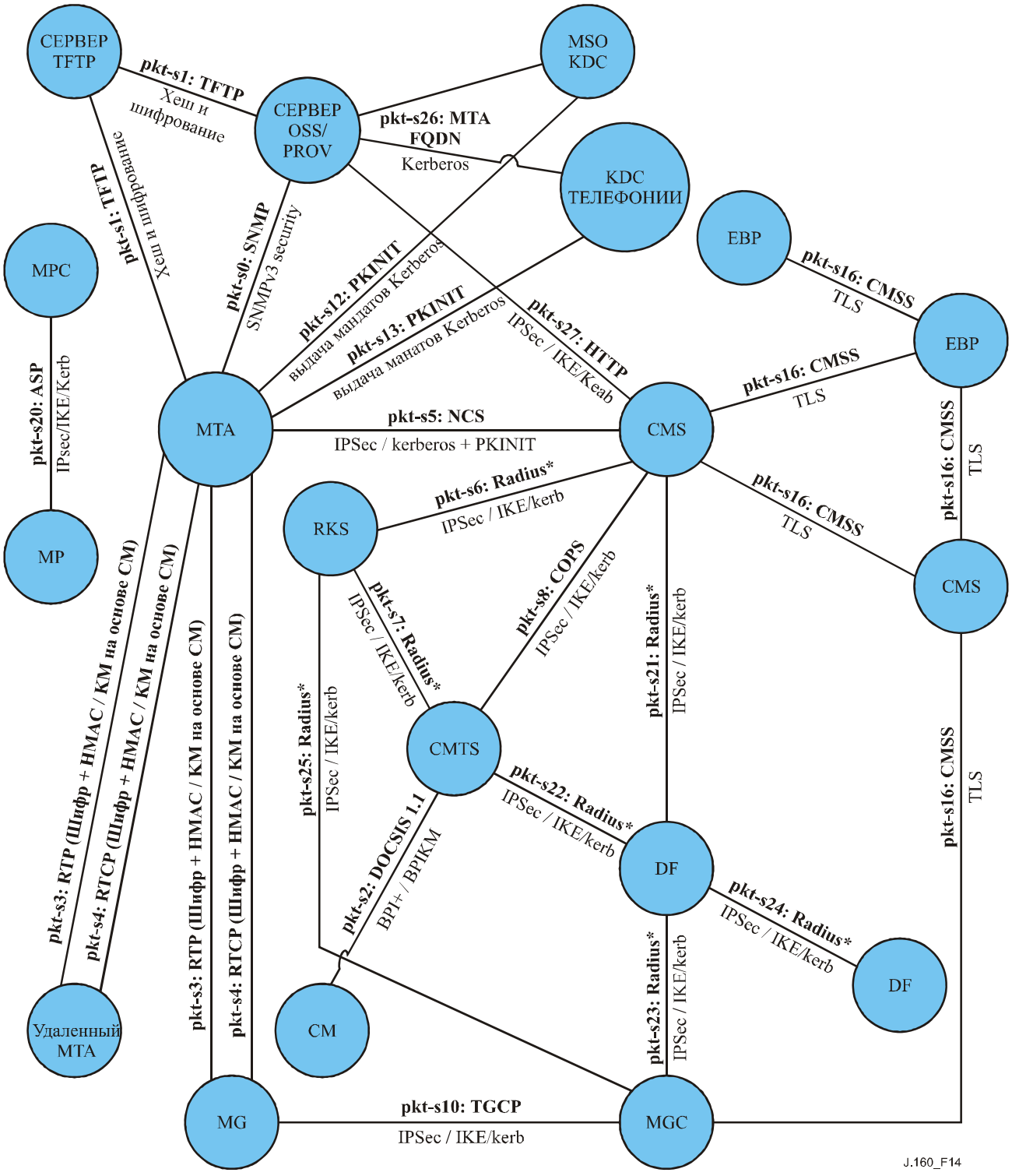


Рисунок 14/J.160 – Интерфейсы безопасности IPCablecom

На рисунке 14 каждый интерфейс обозначен следующим образом:

<метка>: <протокол> { <протокол безопасности> / <протокол управления ключами > }

Если протокол управления ключами отсутствует, это означает, что он не требуется для данного интерфейса. Интерфейсы IPCablecom, не требующие безопасности, не показаны на рисунке 14.

В таблице 10 описан каждый из интерфейсов, показанных на рисунке 14.

Таблица 10/J.160 – Интерфейсы безопасности

Интерфейс	Функциональные компоненты IPCablecom	Описание
Pkt-s0	MTA ↔ PS/OSS	Сразу после выполнения последовательности DHCP в ходе Безопасного процесса инициализации и подготовки к работе MTA осуществляет управление ключами на основе Kerberos с Сервером инициализации и подготовки к работе для установки ключей SNMPv3. В ходе выполнения Базового и Гибридного процессов инициализации и подготовки к работе MTA пропускает SNMPv3, использующий Kerberos, и применяет SNMPv2.
Pkt-s1	MTA ↔ TFTP или PS/OSS	Загрузка конфигурационного файла MTA. Когда Сервер инициализации и подготовки к работе в ходе выполнения Безопасного процесса инициализации и подготовки к работе отправляет MTA команду SNMP Set, он включает как имя конфигурации, так и хеш файла. Впоследствии, когда MTA загружает этот файл, он аутентифицирует конфигурационный файл, используя значение хеша. Конфигурационный файл может быть зашифрован (необязательно). Вместо TFTP может использоваться HTTP.
Pkt-s2	CM ↔ CMTS	Безопасность данного интерфейса должна быть обеспечена при помощи BPI+ с использованием управления ключами BPI. Секретность с использованием BPI+ предоставляется на канале связи HFC.
Pkt-s3	MTA ↔ MTA MTA ↔ MG	RTP: "Сквозные" пакеты медиаинформации между двумя MTA или MTA и MG. Пакеты RTP шифруются напрямую с использованием выбранного шифра. Целостность сообщения обеспечивается (необязательно) MAC MMH. Ключи генерируются случайным образом, и две конечные точки обмениваются ими, отправляя их внутри сообщений сигнализации при помощи CMS или другого сервера приложений.
Pkt-s4	MTA ↔ MTA MTA ↔ MG	Контрольный протокол RTCP для RTP. Целостность сообщения и шифрование при помощи выбранного шифра. Ключи RTCP выводятся с использованием того же секрета, согласованного в ходе управления ключами RTP. Никаких дополнительных сообщений управления ключами не требуется и не применяется.
Pkt-s5	MTA ↔ CMS	NCS. Целостность сообщения и секретность при помощи IPsec. Управление ключами осуществляется на основе Kerberos с использованием расширения PKINIT (первоначальная аутентификация открытого ключа).
Pkt-s6	RKS ↔ CMS	RADIUS: Как для целостности сообщений, так и для секретности используется IPsec. Управление ключами – на основе IKE или Kerberos.
Pkt-s7	CMTS ↔ RKS	RADIUS. Как для целостности сообщений, так и для секретности используется IPsec. Управление ключами – на основе IKE или Kerberos.
Pkt-s8	CMS ↔ CMTS	Связь между GC и CMTS по протоколу COPS используется для загрузки авторизации QoS на CMTS. Как для целостности сообщений, так и для секретности используется IPsec. Управление ключами – на основе IKE или Kerberos.
Pkt-s10	MGC ↔ MG	TGCP: Интерфейс между IPCablecom и Медиашлюзом КТСОП. Как для целостности сообщений, так и для секретности используется IPsec. Управление ключами – на основе IKE или Kerberos.
Pkt-s12	MTA ↔ MSO KDC	PKINIT: KDC отправляется сообщение AS-REQ, при этом для аутентификации используется шифрование методом открытого ключа. KDC проверяет сертификат и выдает либо мандат на обслуживание, либо мандат на выдачу мандатов (TGT) в зависимости от содержания запроса AS. В возвращаемом KDC сообщении AS Reply (ответ) содержится цепочка сертификатов и цифровая подпись, которые используются MTA для аутентификации данного сообщения. В случае если KDC возвращает TGT, MTA далее отправляет KDC сообщение

Таблица 10/J.160 – Интерфейсы безопасности

Интерфейс	Функциональные компоненты IPCablecom	Описание
		TGS Request (запрос), на которое KDC отвечает сообщением TGS Reply, содержащим мандат на обслуживание. Сообщения Reply/Request TGS аутентифицируются с использованием симметричного ключа сеанса внутри TGT.
pkt-s13	MTA ↔ KDC телефонии	PKINIT: См. pkt-s12. Данный интерфейс показан отдельно, поскольку для предоставления услуг аутентификации системе телефонии может использоваться отдельный KDC.
pkt-s16	CMS ↔ CMS CMS ↔ MGC CMS ↔ EBP EBP ↔ EBP	SIP: Как для целостности сообщений, так и для секретности используется TLS. Для взаимной аутентификации в ходе квитирования TLS используются сертификаты.
pkt-s20	MPC ↔ MP	ASP: Как для целостности сообщений, так и для секретности используется IPsec. Управление ключами – на основе IKE или Kerberos.
pkt-s21	DF ↔ CMS	RADIUS: Как для целостности сообщений, так и для секретности используется IPsec. Управление ключами – на основе IKE или Kerberos.
pkt-s22	DF ↔ CMTS	RADIUS: Как для целостности сообщений, так и для секретности используется IPsec. Управление ключами – на основе IKE или Kerberos.
pkt-s23	DF ↔ MGC	RADIUS: Как для целостности сообщений, так и для секретности используется IPsec. Управление ключами – на основе IKE или Kerberos.
pkt-s24	DF ↔ DF	RADIUS: Как для целостности сообщений, так и для секретности используется IPsec. Управление ключами – на основе IKE+.
pkt-s25	RKS ↔ MGC	RADIUS: Как для целостности сообщений, так и для секретности используется IPsec. Управление ключами – на основе IKE или Kerberos.
pkt-s26	OSS/Сервер Инициализации и подготовки к работе (PROV) ↔ MSO KDC OSS/ Сервер Инициализации и подготовки к работе (PROV) ↔ KDC телефонии	KDC использует Kerberos для установления соответствия между адресом MAC MTA и его FQDN для целей аутентификации MTA перед выдачей мандата.
Pkt-s27	CMS ↔ PS/OSS	HTTP: Как для целостности сообщений, так и для секретности используется IPsec. Управление ключами – на основе IKE или Kerberos.

7.9.2 Безопасность при инициализации и подготовке к работе устройства

В рамках IPCablecom инициализация и подготовка к работе устройства может производиться как в безопасном, так и в небезопасном режиме. В рамках IPCablecom также допускается небезопасное управление SNMPv2 после того, как устройство MTA было инициализировано и подготовлено к работе в безопасном режиме. Поскольку данный раздел настоящей Рекомендации посвящен безопасности, предполагается, что сеть работает в безопасном режиме.

В рамках архитектуры безопасности IPCablecom инициализация и подготовка к работе устройства подразделяется на три отдельных действия: регистрация абонента, инициализация и подготовка устройства к работе и авторизация устройства.

7.9.2.1 Регистрация абонента

В результате регистрации абонента создается постоянный лицевой счет абонента для целей выставления счетов на оплату, который уникальным образом идентифицирует MTA для CMS посредством адреса MAC MTA. Данный лицевой счет также используется для идентификации MTA услуг, на которые подписался абонент.

Регистрация абонента может выполняться как внутриполосно, так внеполосно. Спецификация реального процесса регистрации абонента выходит за рамки IPCablecom, и этот процесс может быть различным для каждого отдельного поставщика услуг.

7.9.2.2 Инициализация и подготовка к работе устройства

Устройство MTA аутентифицируется в KDC, используя расширение Kerberos PKINIT. После того как KDC проверит аутентификационную информацию и удостоверится, что данный MTA известен вспомогательной системе инициализации и подготовки к работе, он выдает мандат для Сервера инициализации и подготовки к работе. MTA использует данный мандат для обмена ключами SNMPv3 по безопасному соединению с Сервером инициализации и подготовки к работе. Когда установлен безопасный сеанс связи по протоколу SMNPv3, MTA запрашивает свой конфигурационный файл (который аутентифицирован и может быть зашифрован) с сервера TFTP или HTTP.

7.9.2.3 Динамическая инициализации и подготовка к работе

Для динамической инициализации и подготовки к работе, а также для управления возможностями голосовой связи и других аспектов работы MTA используются средства безопасности протокола SNMPv3.

7.9.2.4 Авторизация устройства

Авторизация устройства происходит, когда устройство MTA аутентифицируется на Сервере управления вызовами по окончании инициализации и подготовки к работе, и устанавливает безопасное соединение с этим сервером, прежде чем стать полностью функциональным. Авторизация устройства позволяет защитить последующую сигнализацию вызовов посредством установленного безопасного соединения.

Устройство MTA аутентифицируется в KDC, используя расширение PKINIT к протоколу Kerberos. После того как KDC проверит аутентификационную информацию и удостоверится, что данный MTA известен вспомогательной системе инициализации и подготовки к работе, он выдает мандат для CMS. MTA использует данный мандат для установления безопасного канала связи с CMS по протоколу IPsec. Канал связи IPsec может не использовать шифрование, в этом случае сообщения сигнализации NCS проходят через данный интерфейс в незашифрованном виде.

7.9.2.5 Безопасность сигнализации

Весь трафик сигнализации, включая сигнализацию QoS, сигнализацию вызовов и сигнализацию с Интерфейсом шлюза КТСОП, проходит по каналам IPsec. Управление безопасными соединениями IPsec осуществляется с использованием некоторой комбинации Kerberos и IKE. Kerberos с расширениями PKINIT используется для обмена ключами между MTA-клиентами и их сервером CMS; IKE или, необязательно, Kerberos, используется для управления всеми остальными безопасными соединениями сигнализации IPsec.

7.9.2.6 Безопасность медиапотоков

В процессе установления вызова MTA согласовывают конкретный алгоритм шифрования для потока широкополосного канала. Требуется, чтобы устройства поддерживали, как минимум, работу без использования шифрования и шифрование AES. Шифрование применяется к полезной нагрузке пакетов RTP, но не к ее заголовку.

Каждый пакет RTP может содержать необязательный код аутентификации сообщения (MAC), основанный на алгоритме MMH. Вычисление MAC затрагивает незашифрованный заголовок пакета и зашифрованную (или незашифрованную) полезную нагрузку.

Ключи для шифрования и вычисления MAC выводятся при помощи секрета, которым обмениваются отправляющий и принимающий MTA как частью сигнализации в ходе установления вызова. Таким образом, обмен ключами для безопасности медиапотока сам защищен на уровне безопасности, предоставляемом протоколом IPsec, защищающим сигнализацию вызовов.

7.9.2.7 Безопасность OSS и системы расчета и выставления счетов на оплату

Агенты SNMP в MTA IPCablecom реализуют SNMPv3, когда работают в безопасном режиме. Модель безопасности пользователя SNMPv3 (RFC 3414) предоставляет услуги аутентификации и секретности

для трафика SNMP. Для контроля доступа к объектам MIB может быть использован контроль доступа на основе представлений SNMPv3 (RFC 3415).

Для установки ключей шифрования и аутентификации между Сервером учетной информации (RKS) и каждым из сетевых элементов IPCablecom, создающим Сообщения о событиях, используется протокол управления ключами IKE или Kerberos. Требуется, чтобы устройства, отвечающие требованиям Рекомендации по безопасности PacketCable, реализовывали IKE с предварительными общими ключами; они также могут реализовывать либо IKE с сертификатами, либо Kerberos, которые позволяют производителям реализовывать полностью автоматические механизмы смены ключей. Сообщения о событиях отправляются CMS и CMTS в адрес RKS с использованием транспортного протокола RADIUS, который, в свою очередь, защищен при помощи IPsec.

8 Руководящие принципы построения сети

8.1 Вопросы отсчета времени и отчетов

Для поддержания качества обслуживания настоятельно рекомендуется поддерживать значения внутренних часов всего сетевого оборудования в границах 200 миллисекунд от Всеобщего координированного времени (UTC). Устройства, отправляющие Сообщения о событиях, должны синхронизировать время при помощи Протокола сетевого времени (NTP) (согласно RFC 1119).

Рекомендуется, чтобы в сетях IPCablecom присутствовал сервер NTP, время которого установлено в границах указанного интервала от Всеобщего координированного времени (UTC).

8.2 Распределение времени для выравнивания буфера проигрывания и скорости кодирования

Оборудование, отвечающее за генерирование и обработку пакетов, обычно работает с автономными часами. Проблемы могут возникнуть в случае предоставления изохронных услуг в связи с плезиохронной природой этих часов. Разница в скоростях хода часов между этими плезиохронными объектами как правило проявляется в недогрузке или переполнении буферов проигрывания.

Для того чтобы минимизировать такого рода случаи, всем CMTS следует привязать свою скорость передачи данных в "нисходящих" потоках к значению времени, полученному из источника, отражающего значение времени часов Stratum-3. Устройствам MTA следует использовать скорость передачи данных в "нисходящих" потоках для выведения значения времени для определения периода пакетизации. Устройствам MTA также следует использовать это значение для определения скорости проигрывания из буфера приема.

8.3 Адресация IP

MTA является составным объектом, где первая часть требуется для администрирования CM, а вторая представляет собой собственно MTA.

Требуется, чтобы все MTA IPCablecom имели два адреса IP – один для CM и один для MTA. Требуется, чтобы все встроенные MTA IPCablecom имели два адреса MAC – один для CM и один для MTA. В рамках IPCablecom поддерживаются только адреса IPv4.

Посредством использования конфигурации с двойным адресом IP могут быть выполнены следующие требования:

- Оператор IPCablecom может назначить CM-компоненту индивидуальный адрес IP в случае, если NAT не предоставляется нигде больше в данной сети IPCablecom.
- Наличие двух адресов IP на MTA позволяет оператору IPCablecom маршрутиризировать пакеты голосовых услуг через голосовую магистраль, а все остальные пакеты (данные) – через магистраль данных. В этом случае маршрутиризирующая магистраль должна быть сконфигурирована таким образом, чтобы к каждому из двух адресов IP получателя вели различные пути.
- При помощи использования раздельных адресов IP оператор IPCablecom может упростить функции администрирования на стороне сети. Например, фильтры политик могут быть установлены таким образом, чтобы либо блокировать, либо пропускать трафик от MTA-компонента устройства. Дополнительно поставщики сетевых услуг могут предоставлять

услуги экранирования адреса источника, и сбор статистики по сетевому трафику и диагностика могут осуществляться на основе адреса IP MTA.

В связи с использованием двойного адреса IP возникают дополнительные факторы, оказывающие влияние на:

- реализацию стека протоколов IP для MTA;
- реализацию OSS IPCablecom и протоколов инициализации и подготовки к работе MTA;
- реализацию сетевой маршрутиризации.

8.4 Динамическое назначение адресов IP

В ходе работы требуется динамическое назначение адресов IP MTA как для инициализации и подготовки к работе устройства, так и для различных операций протокола. Модель сигнализации вызовов, описанная в Рекомендации по NCS (Рек. МСЭ-Т J.162), основана на возможности Сервера управления вызовами устанавливать соответствие между услугами оператора и идентификатором конечной точки и Полным доменным именем (FQDN) MTA. Смена адреса IP, назначенного MTA, происходящая в ходе активного вызова (это может иметь место в случае истечения срока аренды адреса IP у DHCP в ходе активного вызова), повлияет на операции обработки вызова. DHCP не допускает смены адреса IP путем обновления; в плане администрирования такое изменение может быть осуществлено только путем принудительной реинициализации MTA (либо в явной форме, либо посредством отказа в обновлении). Рекомендуется поддерживать непрерывность адреса IP MTA посредством обновлений DHCP. Такие операции, как "перенумерация адреса IP", должны учитывать такие воздействия.

8.5 Назначение FQDN

Предполагается, что вспомогательные системы OSS генерируют FQDN для устройств IPCablecom и передают эти данные соответствующим устройствам IPCablecom и другим сетевым элементам. Данные интерфейсы не определены в рамках IPCablecom (фаза 1).

8.6 Маркировка приоритетов для пакетов потоков сигнализации и медиапотоков

Как для медиапотоков, так и для потоков сигнализации услуг на основе IPCablecom требуется наличие методов правильной маркировки и транспортировки пакетов на достаточно высоком уровне Качества обслуживания как в сети доступа DOCSIS, так и в управляемой магистрали IP.

Основным механизмом обеспечения Качества обслуживания с низким значением задержки для медиапотоков в сети доступа является служба классификации потоков DOCSIS. Данная служба классифицирует пакеты по отдельным потокам на основе полей, содержащихся в пакетах, таких, как адрес источника и получателя IP и номер порта UDP. В "восходящих" потоках данных такие классифицированные пакеты транспортируются посредством соответствующих услуг с постоянной битовой скоростью (для кодеков, поддерживаемых в настоящее время) в соответствии с динамическим планированием CMTS. В "нисходящих" потоках данных такие пакеты транспортируются посредством соответствующего механизма постановки пакетов в очередь с высоким приоритетом и планирования. Механизмы сигнализации DQoS (между CMS и CMTS) и DOCSIS (между CMTS и CM) используются для динамического конфигурирования правил классификации потоков медипотоков и параметров QoS трафика потоков услуг.

В дополнение к классификации потоков полезно помечать пакеты медиапотоков соответствующим маркером приоритета. Такие маркеры приоритета могут быть использованы в системах выстраивания очереди CMTS/CM, а также внутри магистралей QoS под управлением Diffserv для того, чтобы обеспечить высокий приоритет обслуживания для таких пакетов. В рамках IPCablecom не определяется, как политики QoS применяются в управляемой магистрали, однако предоставляются механизмы протоколов для создания специальных классов услуг.

Для пакетов сигнализации также есть определенные преимущества, связанные с использованием услуг QoS на основе приоритетов. В частности, когда сеть доступа загружается до уровня своей пропускной способности, может оказаться важным перенаправлять пакеты сигнализации с более высоким приоритетом, нежели пакеты данных, с тем чтобы избежать избыточных задержек сигнализации. В случае если используется приоритетная система сигнализации, метод предоставления QoS на основе приоритетов базируется на двух механизмах. Во-первых, все пакеты

сигнализации помечаются маркером высокого приоритета, а во-вторых, предоставляется Классификатор DOCSIS, который классифицирует данные пакеты как подлежащие транспортировке в потоке услуг с более высоким приоритетом. Данный классификатор может либо попросту направлять все пакеты "восходящего" потока данных с данным приоритетом в SID с более высоким приоритетом, либо может функционировать на более сложном уровне и также идентифицировать адрес IP устройства(в) MTA, от которых исходит сигнализация. Поток услуги с более высоким приоритетом может быть либо инициализирован и подготовлен к работе статически, либо создан динамически администратором CMTS. Следует отметить, что, если администратор обеспокоен проблемой "кражи услуги" потока услуги с более высоким приоритетом, он может сконфигурировать поток услуги таким образом, чтобы установить более высокий приоритет (низкий уровень задержки), но ограничить пропускную способность.

В рамках архитектуры IPCablecom имеется возможность использования структуры Дифференцированных услуг (IETF RFC 3260) для установления различия между медиаинформацией и сигнализаций IPCablecom и высокоскоростными пакетами данных. Маркировка пакетов для медиапотоков (RTP и RTCP) и потоков сигнализации (NCS, TGCP) осуществляется MTA/MG и/или CMS/MGC. Маркировка пакетов может осуществляться на уровне IP с использованием Кода точки Diffserv (DSCP). Следует отметить, что в IETF RFC 2474 предпринята попытка переименовать октет TOS заголовка IPv4 и октет Класс трафика (Traffic Class) заголовка IPv6 соответственно в поле DS. Поле DS содержит 6-битовый Код точки Diffserv и два бита, в настоящее время не используемых. IETF RFC 2474 был обновлен IETF RFC 3168, где два не использовавшихся были определены как биты "оповещения о явной перегрузке (ECN)". Настоятельно рекомендуется использовать поле DSCP вместо байта TOS IPv4.

Конфигурирование значений DSCP для медиапотоков и потоков сигнализации осуществляется посредством модулей MIB IPCablecom для MTA. Следует отметить, что в NCS сигнализированные параметры SDP могут содержать значения, замещающие сконфигурированные маркировки приоритета медиапотока для каждого конкретного соединения.

8.7 Поддержка факсимильных сообщений

В IPCablecom поддерживается передача факсимильных сообщений в режиме реального времени. В рамках IPCablecom передача факсимильных сообщений наилучшим образом выполняется при использовании Рек. МСЭ-Т Т.38 для ретрансляции факсимильных сообщений по сетям IP (т. е. при помощи локального завершения передачи факсимильного сообщений и преобразования потока факсимильной информации в поток данных ретрансляции факсимильного сообщения IP). Если вызов установлен при помощи аудиокодека, MTA предписывается искать тоновый сигнал факсимильного сообщения. Если тональный сигнал факсимильного сообщения обнаружен, то уведомляется CMS и MTA предписывается переключить поток широкополосного канала на Т.38. В IPCablecom также поддерживается сквозная передача факсимильных сообщений, когда тоновые сигналы факсимильного сообщения передаются через сеть IP как аудиопоток, закодированный при помощи G.711. Для сквозной передачи факсимильных сообщений также поддерживается устранение эффекта эха.

Требуется поддержка переключения в режим факса из голосового вызова. В случае ретрансляции факсимильного сообщения также поддерживается обратное переключение в голосовой режим из режима факса.

8.8 Поддержка аналогового модема

Аналоговые модемы поддерживаются способом, аналогичным способу поддержки сквозной передачи факсимильных сообщений. MTA запрашивается на предмет обнаружения тональных сигналов модема, и, когда такие сигналы обнаружены, CMS предписывает MTA переключиться на кодек G.711, если он уже не используется. Для сквозной передачи данных аналогового модема также поддерживается устранение эффекта эха.

Для голосового вызова поддерживается переключение с кодека с низкой шириной полосы пропускания на G.711 для поддержки сигнализации аналогового модема. Также поддерживается возврат к кодеку с низкой шириной полосы пропускания по окончании сигнализации модема.

Локальное завершение модемов и трансляции потока модема в поток данных IP ретрансляции модема не требуется.

Приложение I

Словарь терминов

В настоящем Приложении содержится полный список терминов, определений, акронимов и аббревиатур, используемых в данном наборе Рекомендаций IPCablecom.

I.1 Определения

I.1.1 контроль доступа: Ограничение потока информации от ресурсов системы для использования только авторизованными людьми, программами, процессами или другими системными ресурсами сети.

I.1.2 активный: Поток J.112 называется "активным", если ему разрешено перенаправлять пакеты данных. Поток J.112 должен быть допущен прежде, чем стать активным.

I.1.3 аутентификация: Процесс проверки заявленной одним объектом другому идентификационной информации.

I.1.4 аутентичность: Возможность удостовериться в том, что данная информация не содержит изменений или подлога и что она действительно была создана тем объектом, который заявляет, что выдал данную информацию.

I.1.5 авторизация: Акт предоставления услуге или устройству доступа в случае, если у него есть право на получение этого доступа.

I.1.6 кабельный модем: Кабельный модем представляет собой оконечное устройство второго уровня, которое завершает соединение J.112 со стороны клиента.

I.1.7 вызов: Вызов является примером инициированных пользователем возможностей голосовой связи. В традиционной телефонии под вызовом подразумевается установление прямого соединения между двумя точками: вызывающей и завершающей стороной. В контексте системы IPCablecom, как было указано выше, связь между сторонами устанавливается без установки "соединения" в традиционном смысле.

I.1.8 шифр: Алгоритм преобразования обычного текста в зашифрованный текст.

I.1.9 набор шифрования: Набор, который должен содержать как алгоритм шифрования, так и алгоритм аутентификации сообщений (например, MAC или HMAC). В общем случае он также может содержать алгоритм управления ключами, который не применяется в контексте IPCablecom.

I.1.10 конфиденциальность: Способ удостовериться в том, что информация не раскрывается кому-либо, кроме тех сторон, для которых она предназначается. Информация шифруется для обеспечения конфиденциальности. Также известна как "секретность".

I.1.11 нисходящий поток: Направление от головного узла к местоположению абонента.

I.1.12 шифрование: Метод, используемый для преобразования обычного текста в зашифрованный текст.

I.1.13 конечная точка: Оконечное оборудование, шлюз или MCU.

I.1.14 сообщение о событии: Сообщение о событии – это набор данных, представляющий событие в структуре IPCablecom, которое может свидетельствовать об использовании одной или более платных возможностей IPCablecom. Само по себе Сообщение о событии может не являться стопроцентным свидетельством использования клиентом платных возможностей, однако Сообщение о событии, находящееся во взаимосвязи с другими Сообщениями о событиях, формирует базу для формирования Детального отчета о пользовании услугами, на основании которого выставляются счета на оплату.

I.1.15 атрибут сообщения о событии: Атрибут Сообщения о событии представляет собой заранее заданный элемент данных, описывающийся определением атрибута и типом атрибута.

I.1.16 шлюз: Устройства-мосты между средой Голосовой связи IP IPCablecom и КТСОП. Примерами могут служить Медиашлюз, который предоставляет интерфейсы линий широкополосного

канала в КТСОП и преобразует медиапоток, а также Шлюз сигнализации, который отправляет и принимает сигнализацию коммутируемой телефонной сети на границе сети IPCablecom.

I.1.17 заголовок: Контрольная информация протокола, содержащаяся в начале блока данных протокола.

I.1.18 целостность: Способ удостовериться в том, что информация не изменялась никем, кроме тех, кто авторизован производить такие изменения.

I.1.19 IPcablecom: Проект МСЭ-Т, включающий архитектуру и серию Рекомендаций, делающий возможной поставку услуг в режиме реального времени по сетям кабельного телевидения с использованием кабельных модемов.

I.1.20 Транзакция IPCablecom: Транзакция IPCablecom – это ряд событий, происходящих в сети IPCablecom в ходе предоставления услуги абоненту. Сообщения о событиях, относящиеся к одной и той же транзакции, идентифицируются по уникальному Идентификатору расчетной взаимосвязи (Billing Correlation ID). Для получения информации, необходимой для установления полного объема использования некоторых услуг, может потребоваться несколько транзакций. Несколько Сообщений о событиях может потребоваться также в случае необходимости отследить ресурсы, потребленные в ходе предоставления каждой отдельной услуги. Транзакция может продолжаться в течение длительного времени.

I.1.21 поток J.112: Однонаправленный или двунаправленный поток пакетов данных, который является предметом сигнализации уровня MAC и присвоения QoS, соответствующих Рекомендации МСЭ-Т J.112.

I.1.22 Kerberos: Протокол сетевой аутентификации на основе секретного ключа, который использует набор криптографических алгоритмов и централизованную базу ключей для аутентификации.

I.1.23 ключ: Математическое значение, являющееся входной информацией для криптографических алгоритмов.

I.1.24 обмен ключами: Взаимообмен открытыми ключами между объектами, которые впоследствии будут использоваться для шифрования связи между этими объектами.

I.1.25 управление ключами: Процесс распределения симметричных ключей совместного использования, необходимых для работы протокола безопасности.

I.1.26 база управляющей информации (MIB): Изложение информации способом, который делает возможным стандартный доступ при использовании протокола управления сетью.

I.1.27 неоказуемость: Возможность предотвращения отказа отправителя от того, что он или она ранее отправил(а) определенное сообщение или осуществил(а) определенные действия.

I.1.28 секретность: Способ удостовериться в том, что информация не раскрывается кому-либо, кроме тех сторон, для которых она предназначается. Информация шифруется для обеспечения конфиденциальности. Также известна как "конфиденциальность".

I.1.29 секретный ключ: Ключ, используемый в криптографии открытого ключа, который принадлежит индивидуальному объекту и должен держаться в секрете.

I.1.30 прокси(proxy): Оборудование, которое косвенно предоставляет какую-либо услугу или выступает представителем при доставке информации, тем самым освобождая узел от необходимости самостоятельно поддерживать данные услуги.

I.1.31 открытый ключ: ключ, используемый в криптографии открытого ключа, который принадлежит индивидуальному объекту и распространяется открыто. Другие объекты используют данный ключ для шифрования данных, отправляемых объекту-владельцу ключа.

I.1.32 сертификат открытого ключа: Связка между открытым ключом объекта и одним или более атрибутами, относящимися к данному объекту. Также известен как "цифровой сертификат".

I.1.33 криптография открытого ключа: Процедура, использующая пару ключей, открытый ключ и секретный ключ для шифрования и дешифрования; также известна как асимметричный алгоритм. Открытый ключ пользователя доступен для других объектов для передачи сообщений владельцу

ключа. Секретный ключ пользователя хранится в секрете и является единственным ключом, при помощи которого можно расшифровать направленные данному пользователю зашифрованные при помощи открытого ключа этого пользователя сообщения.

I.1.34 корневой секретный ключ: Секретный ключ подписи Центра сертификации высшего уровня. Обычно он используется для подписи сертификатов открытых ключей для Центров сертификации более низкого уровня или других объектов.

I.1.35 корневой открытый ключ: Открытый ключ подписи Центра сертификации высшего уровня, обычно используемый для проверки цифровых подписей, которые он создал при помощи соответствующего корневого секретного ключа.

I.1.36 услуга: Услуга – это отдельная функция связи или пакет функций связи, которые может выбрать абонент. Услуга представляет собой набор из одного или нескольких "вызовов" или транзакций, при помощи которых абонент пользуется необходимыми функциями. Примерами услуг являются: сеанс голосовой связи между двумя местными абонентами IPCablecom, трехсторонняя связь, просмотр платного фильма и сеанс доступа в Интернет. Услуга может оказываться немедленно и единовременно или в течение определенного времени.

I.1.37 Шлюз сигнализации (SG): SG является агентом сигнализации, который принимает и передает "родную" сигнализацию SCN на границе сети IP. В частности, функция SG SS7 преобразует варианты ISUP и TCAP в Шлюзе интернета SS7 в обычные версии ISUP и TCAP.

I.1.38 сертификат X.509: Спецификация сертификата открытого ключа, разработанная как часть каталога стандартов Рек. МСЭ-Т серии X.500.

I.2 Сокращения

AH	Authentication Header	Заголовок аутентификации
AMA	Automated Message Accounting	Автоматический учет сообщений
AN	Access Node	Узел доступа
ANC	Announcement Controller	Контроллер сообщений автоинформатора
ANP	Announcement Player	Проигрыватель сообщений автоинформатора
ANS	Announcement Server	Сервер сообщений автоинформатора
API	Application Programming Interface	Программный интерфейс приложений
BPI+	Baseline Privacy Interface Plus	Базовый интерфейс секретности +
CA	Call Agent	Агент вызова
CBC	Cipher Block Chaining (mode)	Режим сцепления шифрованных блоков
CDR	Call Detail Record	Детальная информация о вызове
CIC	Circuit Identification Code	Идентификационный код линии связи
CID	Circuit ID	Идентификатор линии связи
CM	Cable Modem	Кабельный модем
CMS	Call Management Server	Сервер управления вызовами
CMS	Cryptographic Message Syntax	Синтаксис криптографических сообщений
CMTS	Cable Modem Termination System	Система завершения кабельных модемов
COPS	Common Open Policy Service	Обычная служба открытой политики
CPE	Customer Premises Equipment	Оборудование в помещении потребителя
DCS	Distributed Call Signalling	Распределенная сигнализация вызовов
DHCP	Dynamic Host Configuration Protocol	Протокол динамического конфигурирования узла
DNS	Domain Name System	Доменная система имен
DPC	Destination Point Code	Код точки назначения

DQoS	Dynamic Quality of Service	Динамическое Качество обслуживания
DTMF	Dual Tone Multi-Frequency	Двухтональный многочастотный сигнал
ESP	IPsec Encapsulation Security	Безопасность инкапсуляции IPsec
FID	Flow Identifier	Идентификатор потока
FQDN	Fully Qualified Domain Name	Полное доменное имя узла
GC	Gate Controller	Контроллер шлюза
HFC	Hybrid Fibre/Coaxial (cable)	Гибридный волоконно-коаксиальный (кабель)
HMAC	Hashed Message Authentication Code	Хешированный код аутентификации сообщения
HTTP	HyperText Transfer Protocol	Протокол передачи гипертекста
IANA	Internet Assigned Numbers Authority	Центр по присвоению номеров Internet
IEEE	Institute of Electrical and Electronics Engineers	Институт инженеров по электротехнике и радиоэлектронике
IETF	Internet Engineering Task Force	Рабочая группа по стандартам Интернет
IKE	Internet Key Exchange	Обмен ключами Интернет
IKE–	IKE with pre-shared keys for authentication	IKE с использованием предварительных общих ключей для аутентификации
IKE+	A notation defined to refer to the use of IKE, which requires digital certificates for authentication	Нотация, разработанная для обозначения использования IKE, которое требует цифровых сертификатов для аутентификации
INA	Interactive Network Adapter	Интерактивный сетевой адаптер
IP	Internet Protocol	Протокол Интернет
IPsec	IP security	Протокол IPsec
ISTP	Internet Signalling Transport Protocol	Транспортный протокол сигнализации Интернет
ISUP	Integrated Services Digital Network User Part	Пользовательская часть цифровой сети с интегрированными службами
LNP	Local Number Portability	Переносимость местного номера
MAC	Message Authentication Code	Код аутентификации сообщения
MAC	Media Access Control	Управление доступом к среде передачи
MD5	Message Digest 5	Односторонняя хеш-функция MD5
MF	Multi-Frequency	Многочастотный
MG	Media Gateway	Медиашлюз
MGC	Media Gateway Controller	Контроллер медиашлюза
MGCI	Media Gateway Controller Interface	Интерфейс контроллера медиашлюза
MGCP	Media Gateway Control Protocol	Протокол контроля медиашлюза
MIB	Management Information Base	База управляющей информации
MMH	Multilinear Modular Hash	Полилинейный модульный хеш
MTA	Media Terminal Adapter	Адаптер медиатерминала
MTP	Message Transfer Part	Подсистема передачи сообщений
MWD	Maximum Waiting Delay	Максимальная задержка ожидания
NCS	Network Call Signalling	Сигнализация вызовов сети
NTP	Network Time Protocol	Протокол сетевого времени
OSS	Operations Support System	Система операционной поддержки
PHS	Payload Header Suppression	Сокращение заголовка полезной нагрузки

PKI	Public Key Infrastructure	Инфраструктура открытого ключа
PKINIT	Public Key Cryptography Initial Authentication	Первоначальная аутентификация криптографии открытого ключа
КТСОП	Public Switched Telephone Network	Коммутируемая телефонная сеть общего пользования, КТСОП
QoS	Quality of Service	Качество обслуживания, КО
RADIUS	Remote Access Dial-In User Service	Служба удаленной аутентификации пользователей по коммутируемым линиям
RAP	Resource Allocation Protocol	Протокол выделения ресурсов
RC4	A variable key length stream cipher offered in the ciphersuite, used to encrypt the media traffic in IPCablecom	Шифр с переменной длиной ключа для потоков, содержащийся в наборе шифрования, используемый для шифрования медиатрафика в IPCablecom
RFC	Request for Comments	Запрос на пояснение
RFI	Radio Frequency Interface	Радиочастотный интерфейс
RKS	Record Keeping Server	Сервер учетной информации
RSVP	Resource reSerVation Protocol	Протокол резервирования ресурсов
RTCP	Real-Time Control Protocol	Протокол контроля режима реального времени
RTO	Retransmission Timeout	Период ожидания повторной передачи
RTP	Real-Time Transfer Protocol	Протокол передачи в режиме реального времени
SA	Source Address	Адрес источника
SA	Security Association	Безопасное соединение
SCCP	Signalling Connection Control Part	Подсистема управления соединением сигнализации
SCP	Service Control Point	Контрольная точка обслуживания
SCTP	Stream Control Transmission Protocol	Протокол передачи контроля потоков
SDP	Session Description Protocol	Протокол описания сеанса
SG	Signalling Gateway	Шлюз сигнализации
SHA-1	Secure Hash Algorithm 1	Алгоритм аутентификации и проверки целостности информации версии 1, алгоритм SHA-1
SID	System IDentification number	Идентификационный номер системы
SIP	Session Initiation Protocol	Протокол инициации сеанса
SIP+	Session Initiation Protocol Plus	Протокол инициации сеанса плюс
SNMP	Simple Network Management Protocol	Простой протокол управления сетью
SPI	Security Parameter Index	Индекс параметра безопасности
SS7	Signalling System No. 7	Система сигнализации №7
SSP	Signal Switching Point	Точка переключения сигнала
TCAP	Transaction Capabilities Application Part	Прикладная подсистема возможностей транзакции
TCP	Transmission Control Protocol	Протокол контроля передачи
TGS	Ticket Granting Server	Сервер предоставления мандата
TLV	Type-Length-Value	Тип-Длина-Значение
ToS	Type of Service	Тип услуги
UDP	User Datagram Protocol	Протокол дейтаграмм пользователя
VAD	Voice Activity Detection	Обнаружение голосовой активности
VoIP	Voice Over IP	Голосовая IP телефония (передача голоса по сети IP)

БИБЛИОГРАФИЯ

– IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.

– IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions*.

– IETF RFC 2274 (1998), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

– IETF RFC 2575 (1999), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).* (Obsoletes RFC 2275).

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, 2006 г.