МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т J.292

СЕКТОР СТАНДАРТИЗАЦИИ ЭЛЕКТРОСВЯЗИ МСЭ

(11/2006)

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

Кабельные модемы

Архитектура декодера телевизионных каналов следующего поколения, не зависящая от среды передачи

Рекомендация МСЭ-Т J.292

Рекомендация МСЭ-Т J.292

Архитектура декодера телевизионных каналов следующего поколения, не зависящая от среды передачи

Резюме

В настоящей Рекомендации описывается базовая архитектура декодера телевизионных каналов следующего поколения, которая не зависит от транспортной среды передачи и которая позволит поставщикам услуг в будущем предлагать существующие и новые усовершенствованные услуги, независимо от транспортной среды передачи. В настоящей Рекомендации предполагается, что все содержимое передается на IP-пакетах с соответствующим механизмом, управляемым QoS. В настоящей Рекомендации отражаются ключевые функциональные аспекты декодера телевизионных каналов следующего поколения, например возможность адаптации ресурсов сети, безопасный аутентифицированный двусторонний обмен данными и управление ресурсами сеанса связи и механизм управления QoS.

Источник

Рекомендация МСЭ-Т J.292 утверждена 29 ноября 2006 года 9-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

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

ПРИМЕЧАНИЕ

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

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

© ITU 2009

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

Стр.

Рекомендация МСЭ-Т J.292

Архитектура декодера телевизионных каналов следующего поколения, не зависящая от среды передачи

1 Сфера применения

В настоящей Рекомендации описывается базовая архитектура декодера телевизионных каналов следующего поколения, которая не зависит от транспортной среды передачи. Операторы связи и поставщики оборудования МОГУТ самостоятельно выбирать решения по инвестициям в сеть и продукт. В этой архитектуре, в частности, определяются: возможность адаптации ресурсов сети, безопасный аутентифицированный двусторонний обмен данными и механизмы управления сеансом связи и QoS в условиях полномасштабного использования протокола IP. Эта архитектура применима для поддержки развития услуг видео по запросу, цифрового телевидения высокой четкости, домашних сетей, которые соединяются с большим количеством устройств, предоставляемых пользователем, и мультимедийных IP-услуг, включая передачу голоса по IP-протоколу, видеотелефонию и многопользовательские сетевые игры. Целью настоящей Рекомендации является описание базовых функций декодера телевизионных каналов следующего поколения, независимо от среды транспортировки. При реализации функций NG-STB-A настоящая Рекомендация ДОЛЖНА использоваться вместе с [ITU-T J.290]. В настоящей Рекомендации приведено несколько технических решений, которые являются примерами, предназначенными только для облегчения понимания читателем и не являющимися спецификацией декодера телевизионных каналов, независимой от среды передачи. Заметим, что в последующих Рекомендациях будут определены технические решения, относящиеся к независимому от среды передачи декодеру телевизионных каналов.

2 Справочные документы

Нет.

3 Определения

В настоящей Рекомендации используются следующие термины:

3.1 сеть распределения контента (CDN) (content distribution network): CDN включает в себя базовую сеть и сеть доступа, где доставка контента управляется маршрутизацией идентифицированных пакетов и механизмами, связанными с QoS.

3.2 оборудование, устанавливаемое в помещении абонента (CPE) (customer premises equipment): CPE включает в себя видеоустройства абонента (SVD), шлюз на стороне абонента (RGW) и дополнительные устройства домашней сети.

3.3 многоадресная передача по протоколу IP (IP multicast): Используется для вещания по протоколу IP на условиях эффективности использования ширины полосы пропускания центрального блока управления, CDN (сети распределения контента) и сегмента CPE.

3.4 двусторонние аутентифицированные каналы обмена данными (2-way authenticated communication channels): Эти каналы используются для возобновляемого условного управления ключами, дистанционного управления видеоустройствами абонента, загружаемыми обновлениями для встроенных программ и перенастройкой алгоритмов шифрования между головным узлом и видеоустройствами абонента.

3.5 транспортный поток (TS) (transport stream): Описываемый в этой Рекомендации транспортный поток передается с помощью определенного потока многоадресной передачи, который идентифицируется адресом многоадресной группы, номером порта UDP и т. д.

3.6 услуги веб-портала (PS) (portal services): Функциональный элемент, обеспечивающий управление и функции трансляции между HFC и домашней сетью.

3.7 управление сменой программ (zapping control): Механизм управления для многоадресных групп приема и передачи с учетом последовательности протокола IGMP/MLD, которая необходима в устройствах CPE, совместимых с NG-STB.

3.8 шлюз на стороне абонента (residential gateway): Устройство, обеспечивающее функциональные средства для взаимосвязи между сетью доступа и домашней сетью, как это описывается в [b-ITU-T J.190].

ПРИМЕЧАНИЕ. – Способы применения функциональных средств шлюза на стороне пользователя в разных сетях СЛЕДУЕТ рассмотреть в ближайшем будущем.

4 Сокращения и акронимы

Данная Рекомендация использует следующие сокращения:

ARQ	Automatic Repeat ReQuest	Автоматический повтор запроса
BE	Best Effort	Доступное качество
BGP	Border Gateway Protocol	Пограничный межсетевой протокол
CA	Conditional Access	Условный доступ
CAS	Conditional Access System	Система условного доступа
CDN	Content Distribution Network (in terms of the definition in [b-ITU-T J.282])	Сеть распределения контента (на условиях определения в [b-ITU-T J.282])
CoS	Class of Service	Класс обслуживания
CPE	Customer Premises Equipment	Оборудование, устанавливаемое в помещении абонента
DB	Database	База данных
DHCP	Dynamic Host Configuration Protocol	Протокол динамической конфигурации сетевого узла
DiffServ	Differentiated Services Architecture for Network Traffic	Архитектура дифференцированного обслуживания для трафика сети
DOCSIS	Data over Cable Service Interface Specification	Спецификация интерфейса услуги передачи данных по кабелю
DSCP	DiffServ Code Point	Кодовая точка дифференцированного обслуживания
DSLAM	Digital Subscriber Line Access Multiplexer	Мультиплексор цифровой абонентской линии доступа
DTV	Digital Television	Цифровое телевидение
EMM	Entitlement Management Message	Сообщение наименования управления
FEC	Forward Error Correction	Упреждающая коррекция ошибок
GigE	Gigabit Ethernet	Гигабитная сеть Ethernet
HDTV	High-definition Television	Телевидение высокой четкости
HE	Headend	Головной узел
HGW	Home Gateway	Шлюз домашней сети
IGMP	Internet Group Management Protocol	Протокол управления группами в интернете
IP	Internet Protocol	Протокол Интернет
Layer 3	Network layer 3 in OSI stack	3-й уровень сети в комплекте OSI
LDPC	Low-Density Parity Check	Проверка четности с малой плотностью
MAC	Media Access Control	Управление доступом к среде передачи
MLD	Multicast Listener Discovery	Обнаружение многоадресного приемника
MPEG	Motion Picture Experts Group	Группа экспертов по вопросам кинотехники
NAT	Network Address Translation	Трансляция сетевых адресов
NG-STB	Next Generation Set-Top Box	Декодер каналов телевидения последующих поколений

NG-STB-MI-A	Next Generation Set-Top Box Media-Independent Architecture	Архитектура декодера телевизионных каналов следующего поколения, не зависящая от среды передачи
NIT	Network Information Table	Таблица сетевой информации
OLT	Optical Line Terminal	Терминал оптической линии связи
OSPF	Open Shortest Path First	Открыть кратчайший путь первым
PCR	Program Clock Reference	Метка синхронизации программы
PID	Packet Identifier	Идентификатор пакета
PIMSM	Protocol Independent Multicast Sparse Mode	Разреженный режим работы протокола маршрутизации многоадресных сообщений
QoS	Quality of Service	Качество обслуживания
RGW	Residential Gateway	Шлюз на стороне пользователя
RTP	Real Time Protocol	Протокол реального времени
RTSP	Real-Time Streaming Protocol	Потоковый протокол реального времени
SI	Service Information	Служебная информация
STB	Set-Top Box	Декодер телевизионных каналов
SVD	Subscriber Video Device	Видеоустройство абонента
TCP	Transmission Control Protocol	Протокол управления передачей
TLS	Transport Layer Security	Безопасность на уровне транспортного протокола
ToS	Type of Service	Тип услуги
TS	Transport Stream	Транспортный поток
UPnP	Universal Plug and Play	Универсальное устройство "включи и работай"
ГУН	Voltage-Controlled Oscillator	Генератор, управляемый напряжением
VoD	Video on Demand	Видео по запросу
VoIP	Voice over Internet Protocol	Голосовая связь по IP-протоколу

5 Соглашения по терминологии

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

"ДОЛЖЕН" ("MUST")	Данное слово означает, что то или иное положение является безусловным требованием данной Рекомендации.
"НЕЛЬЗЯ" ("MUST NOT")	Данная фраза означает, что то или иное положение является безусловным запретом, налагаемым настоящей Рекомендацией.
"ДОЛЖЕН" ("SHOULD")	Данное слово означает, что при определенных условиях могут существовать веские причины, для того чтобы не принимать во внимание данное положение, однако следует осознать все последствия и тщательно взвесить ситуацию до выбора иного образа действия.
"НЕ ДОЛЖЕН" ("SHOULD NOT")	Данная фраза означает, что при определенных условиях могут существовать веские причины приемлемости и даже пользы отмеченного поведения, однако следует осознать все последствия и тщательно взвесить ситуацию до реализации любого поведения, описываемого этой фразой.
"МОЖЕТ" ("MAY")	Данное слово означает, что это положение на самом деле факультативно. Один поставщик может решить включить такое положение, поскольку, например, оно требуется на конкретном рынке или поскольку оно улучшает продукт, другой поставщик может пропустить то же самое положение.

6 Архитектура декодера телевизионных каналов следующего поколения в условиях, независимых от среды передачи

В дополнение к разделу 6 [ITU-T J.290] обязательными ключевыми атрибутами архитектуры независимого от среды передачи декодера телевизионных каналов следующего поколения (NGSTB) для условий работы в сети IP являются следующие пункты:

– *Адаптируемость ресурсов сети*. Позволяет оператору сети более эффективно использовать ширину полосы пропускания сети за счет применения схем восстановления потери пакетов; подавления остаточного трафика, обусловленного сменой программ канала; комплексного сквозного управления QoS в направлении от головного узла к видеоустройствам абонента (SVD), совместимого с независимой от среды передачи архитектурой NGSTB (NG-STB-MI-A); совместно с аудио/видеокодеком, описанным в [ITU-T J.290].

– *Передача транспортного потока MPEG-2 через IP*. Позволяет оператору сети распределять транспортные потоки в условиях, не зависящих от среды передачи, посредством использования стандартного кадра протокола Интернет с информацией описания потока, определенной в спецификации для многоадресной передачи по протоколу IP.

– *Гибкая синхронизация TS с головным узлом*. Позволяет всем видеоустройствам абонента (SVD), совместимым с архитектурой NG-STB-MI-A, исключить возможность переполнения буфера воспроизведения и работы с недогрузкой в среде IP-сети.

– О*бщий механизм представления*. Позволяет видеоустройству SVD, совместимому с архитектурой NG-STB-MI-A, поддерживать механизмы представления, определенные в документах [b-ITU-T J.200] и [b-ITU-T J.201].

– *Получение данных о местоположении*. Позволяет оператору сети управлять областью распределения транспортных потоков, исходя из местоположения устройств SVD. Требование знания о местоположении SVD является необязательным.

– *Безопасные двунаправленные аутентифицированные каналы в IP-сети*. Безопасность на уровне транспортного протокола (TLS) 1.0 в устройстве SVD, совместимом с архитектурой NG-STB-MI-A, обеспечивает наличие защищенных двусторонних каналов обмена данными между центральным блоком управления и SVD. Такие каналы используют в управлении ключами возобновляемого условного доступа, дистанционном управлении SVD, загружаемых обновлениях для встроенных программ, в секретных данных интерактивных применений и в перенастройке алгоритмов шифрования.

6.1 Опорная архитектура

На рисунке 1 показана опорная архитектура служебной инфраструктуры распределения IP-контента. Также учтена взаимосвязь между основными сегментами сети, например CPE (оборудованием, устанавливаемым в помещении абонента), включающим в себя видеоустройство абонента (SVD) и устройства домашней сети, например шлюз на стороне абонента (RGW), сеть доставки контента (CDN), которая МОЖЕТ быть определена отдельно как базовая сеть или периферийная сеть, интернет и центральный блок управления (HE). В условиях работы, независимой от среды передачи, все услуги распределения контента предоставляются посредством одноадресной IP-рассылки или в канале многоадресной передачи. Многоадресную IP-передачу СЛЕДУЕТ использовать для IP-радиовещания в целях повышения эффективности использования полосы пропускания центрального блока управления, сети CDN и сегмента CPE.

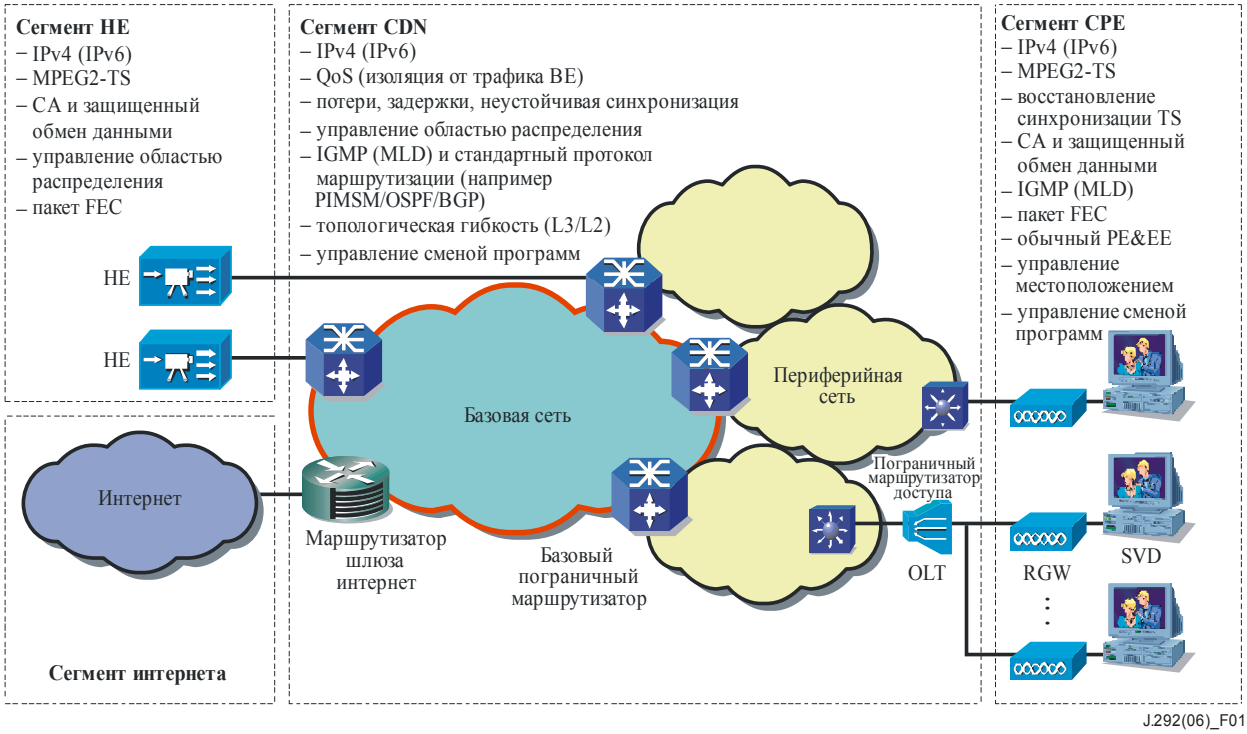


Рисунок 1 – Опорная архитектура служебной инфраструктуры распределения IP-контента

6.2 Атрибуты декодера телевизионных каналов следующего поколения для условий, не зависящих от среды передачи

6.2.1 Архитектура услуг распределения контента

Как минимум, в архитектуру NG-STB-MI-A ДОЛЖНЫ входить следующие атрибуты кроме тех, которые были упомянуты в разделе 6.2.1 Рекомендации [ITU-T J.290].

– *Распределение контента на основе IP*. Протокол IP выбирается в качестве основного уровня канала передачи для всех услуг распределения контента. Все устройства, совместимые с архитектурой All NG-STB-MI-A, должны поддерживать протокол версии IPv4 с возможностью дальнейшей модернизации до версии IPv6. Также может использоваться двойной пакет IPv4/v6. Также для обеспечения возможности IP-подключения без ручной настройки требуются механизмы автоматической настройки, например DHCP.

– *Соединение между многоадресным потоком и транспортным потоком*. Доставка транспортного потока осуществляется при помощи определенного многоадресного потока, который идентифицируется групповым многоадресным адресом, номером порта UDP и пр. Рекомендуется назначать каждому транспортному потоку свой групповой адрес. Для получения информации о транспортном потоке, который должен быть завершен на устройстве SVD, все устройства SVD должны быть совместимыми с архитектурой NG-STB-MI-A.

– *Управление сменой программ*. Механизм управления, необходимый в устройствах CPE, совместимых с архитектурой NG-STB-MI-A, для сценариев смены программ контента, где SVD на высокой скорости последовательно меняет многоадресные группы (т. е. транспортные потоки). В результате остаточный трафик уже пройденных групп МОЖЕТ стать причиной перегрузки в сегменте CPE.

– *Восстановление потерь пакетов*. Для того чтобы улучшить качество передачи в транспортном потоке (TS), для поддержки механизма восстановления потерь пакетов все устройства SVD должны быть совместимыми с архитектурой NG-STB-MI-A.

– *Синхронизация TS*. Для того чтобы синхронизировать воспроизведение звука и изображения с кодером в сегменте центрального узла управления, требуется надежный механизм восстановления синхронизации транспортного потока даже в тех случаях, когда наблюдаются колебания времени прибытия пакетов и/или потери пакетов с информацией временной отметки программ (PCR) в IP-канале передачи.

– *Выходной видеосигнал высокой четкости*. Выходной сигнал высокой четкости является обязательным даже для устройства SVD базового уровня в условиях, независимых от среды передачи.

6.2.2 Сегмент сети: CPE

Сегмент CPE состоит из видеоустройств абонента (SVD), шлюза на стороне абонента (RGW) и дополнительных устройств домашней сети, с которыми связаны SVD и RGW. SVD – это видеоустройство, совместимое с архитектурой NG-STB-MI-A, которое включает в себя тюнер, например декодеры телевизионных каналов, или автономный цифровой ТВ-приемник (DTV). Шлюз RGW находится на границе сегмента CPE и размещается в пограничном устройстве доступа сегмента CDN. Шлюз RGW предоставляет доступ в интернет другим устройствам CPE. Шлюз RGW отделяет и защищает входящий транспортный поток от интернет-трафика доступного качества. Кроме того, шлюз RGW отвечает за разграничение услуг исходящего трафика из домашней сети к сегменту CDN. Также шлюз RGW МОЖЕТ управлять QoS домашней сети. Если говорить о пограничном устройстве сегмента доступа CDN, с которым соединен шлюз RGW, то это устройство МОЖЕТ использоваться, но не служит границей для: OLT (терминала оптической линии связи), DSLAM (мультиплексора линии доступа цифрового абонента) и переключателя уровня 2/3.

6.2.3 Сегмент сети: CDN

Транспортные потоки распределяются через сегмент CDN. Интернет-трафик доступного качества МОЖЕТ распределяться посредством маршрутизаторов шлюзов интернета. Сегмент CDN ДОЛЖЕН получить необходимую ширину полосы пропускания, для того чтобы передавать все транспортные потоки, и использование этой ширины полосы пропускания ДОЛЖНО быть гарантировано, даже если объем интернет-трафика доступного качества растет. Описание механизма обеспечения ширины полосы пропускания содержится в Рекомендации [b-ITU-T J.282]. Кроме того, сегмент CDN ДОЛЖЕН быть эластичен и противостоять возникновению внутри себя любой отдельно взятой ошибки. Описание способа увеличения эластичности сети IP содержится в Рекомендации [b-ITU-T J.283].

Дополнительно к техническим требованиям, приведенным в Рекомендации [ITU-T J.290], устройства сети, совместимые с архитектурой NG-STB-MI-A, в сегменте CDN ДОЛЖНЫ поддерживать механизм QoS, если устройства управляют и интернет-трафиком доступного качества, и трафиком высокоприоритетного транспортного потока от сегмента центрального блока управления. Стандарт IEEE 802.1p определяет идентификатор приоритета, встроенный в структуру сети Ethernet, как пример механизма QoS.

6.2.4 Сегмент сети: Центральный блок управления

Сегмент центрального блока ДОЛЖЕН создаваться на основе IP. В качестве интерфейсов сетей для распределения многоканального содержимого HDTV требуются сеть GigE или сеть с большей шириной полосы пропускания. Пакет FEC ДОЛЖЕН создаваться так же, как пакет FEC в устройстве SVD. Другие свойства сегмента центрального блока управления описаны в Рекомендации [ITU-T J.290].

6.2.5 Сегмент сети: интернет

Трафик из сегмента интернета может попадать в сегмент CDN через маршрутизаторы шлюзов интернет и наоборот. Маршрутизаторы шлюзов интернет нужны для обеспечения возможности изолировать искаженный трафик от трафика интернета, направляемого к устройствам в центральном блоке управления и в сегментах CDN.

7 Помещение клиента

7.1 Функциональные средства устройств CPE

– *Видеоустройства абонента (SVD)*. В таблице 1 приводятся основные функции SVD и примеры расширения его возможностей. В качестве базового устройства (низкого уровня) определяется SVD с минимальными функциональными средствами архитектуры NG-STB-MI-A. Устройства SVD более высокого уровня включают возможности расширения в разделения поставщиков, операторов сети и розничных торговцев.

Таблица 1 – Базовые и расширенные функциональные средства устройств SVD

Основные функциональные средства устройств SVD	Дополнительные функции расширения для устройств SVD (примеры)
– Протокол IPv4; – Возможность модернизации протокола в будущем от версии IPv4 до версии IPv6; – Протокол IGMPv2; – Возможность модернизации протокола в будущем от версии IGMPv2 до версии MLDv2; – Клиент DHCP; – Выходной сигнал высокой четкости; – Многоадресный поток/соединение TS; – Управление сменой программ; – TLS 1.0; – Пакет FEC; – Синхронизация TS; – Получение данных о местоположении.	– Двойной стек IPv4/IPv6, IPv6; – Протокол MLDv2; – Протокол IGMPv3; – Расширенный пакет FEC и/или локальный пакет ARQ/FEC.

– *Шлюз на стороне абонента (RGW)*. Для обеспечения работы RGW МОГУТ использоваться либо подход маршрутизации уровня 3, либо метод соединения уровня 2. С точки зрения предоставления доступа в интернет для других устройств CPE, метод уровня 3 с транслятором сетевых адресов (NAT) применяется чаще, так как другие устройства CPE нуждаются в защите от злонамеренного доступа с узлов, находящихся за пределами сегмента CPE. Тем не менее, функции, обозначенные в таблице 2, используются в качестве RGW уровня 3.

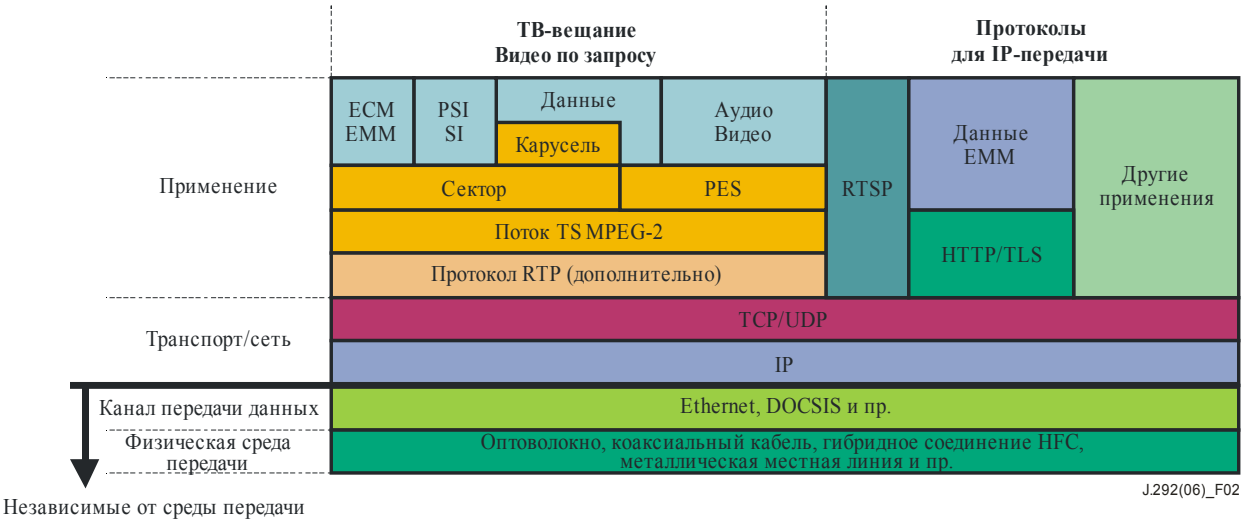
Таблица 2 – Базовые и расширенные функциональные средства шлюза RGW (Уровень 3)

Основные средства шлюза RGW	Дополнительные функции расширения для шлюза RGW (примеры)
– Протокол IPv4; – Возможность модернизации протокола в будущем от версии IPv4 до версии IPv6; – Прокси-протокол IGMPv2; – Возможность модернизации протокола в будущем от прокси-протокола IGMPv2 к прокси-функции MLDv2; – Протокол DHCP клиент/сервер; – Возможность подключения к интернету; – Прохождение NAT к протоколу IPv4; – Получение данных о местоположении.	– Двойной стек IPv4/IPv6, IPv6; – Прокси-протокол MLDv2; – Прокси-протокол IGMPv3; – Локальный пакет ARQ/FEC по направлению к устройствам SVD.

– *Дополнительные устройства домашней сети*. Домашняя сеть МОЖЕТ создаваться внутри сегмента, используя другие устройства, которые выполняют функции коммутации, например коммутатор Ethernet. Дополнительная информация о домашних сетях, например управление QoS, содержится в Рекомендации [ITU-T J.290].

7.2 Архитектура протокола для применений передачи видеосигнала и данных

На рисунке 2 показана архитектура протокола для применений передачи видеосигнала и данных. Для обеспечения независимости от среды передачи все устройства, совместимые с архитектурой NG-STB-MI-A, используют во всех сегментах сети протокол IP в качестве основного канала передачи. Приложения передачи видеосигнала, например ТВ-вещание и видео по запросу, основаны на транспортном потоке (TS) MPEG-2, и один или несколько пакетов передаются как сообщения RTP/UDP. Следует заметить, что протокол TCP может использоваться вместо протокола UDP для IP-услуг одноадресной передачи, например VoD. Однако в услугах ТВ-вещания по протоколу IP, рекомендуется многоадресная IP-передача протоколов RTP/UDP из-за эффективности использования полосы пропускания в центральном блоке управления, сети CDN, CPE, где для передачи между соседними устройствами сети требуется только одна копия пакета.



ПРИМЕЧАНИЕ. – Протокол TCP требуется для передачи протоколов RTSP и HTTP/TLS.

Рисунок 2 – Архитектура протокола для применений передачи видеосигнала и данных

Существует две версии протокола IP, IPv4 и IPv6, которые различаются в основном длиной адреса. Для каждого протокола были определены процедуры многоадресного распределения, сигнализации и управления адресом. Для поддержки протокола IPv4 и обеспечения возможности его модернизации в будущем, как минимум, до версии IPv6 требуется, чтобы все устройства были совместимыми с архитектурой NG-STB-MI-A. Также можно использовать двойной стек IPv4/v6. Рекомендуется осуществлять реконфигурацию версии протокола IP в он-лайн режиме, например загрузка встроенных программ через сегмент CDN.

Если требуется более надежная защита контента, чем существующая система CAS, группа пакетов TS MPEG-2 шифруется в полезной нагрузке RTP/UDP. На рисунке 3 показан пример сообщения RTP/UDP с зашифрованными пакетами TS MPEG-2. Этот пример содержит зашифрованные пакеты TS MPEG-2, идентификатор ключа шифрования и информация по модернизации ключа.

Заголовок RTP	Идентификатор ключа	Зашифрованная группа пакетов MPEG-2 TS	Информация по модернизации ключа

Рисунок 3 – Пример сообщения RTP/UDP с зашифрованными пакетами TS MPEG-2

7.3 Протокол сигнализации между сегментами CPE и CDN

Протокол IGMP и/или MLD используются в качестве механизмов выбора программ устройств SVD. С точки зрения равноправного узла IGMP/MLD, может использоваться шлюз RGW или маршрутизатор на границе доступа сегмента CDN. При использовании шлюза RGW уровня 3 он ДОЛЖЕН работать как прокси-протокол IGMP/MLD, действующий как маршрутизатор IGMP/MLD для устройств SVD и как хост IGMP/MLD для маршрутизатора на границе доступа.

Протокол IGMPv2 или дополнительно IGMPv3 рекомендуется для работы в условиях IPv4, а MLDv2 для работы в условиях IPv6. При использовании протокола IGMPv3 ДОЛЖНО гарантироваться взаимодействие протокола IGMPv2, как это показано в документе RFC 3376.

7.4 Соединение между многоадресным потоком и транспортным потоком (TS)

Необходимая для получения определенного транспортного потока информация по соединению приведена ниже:

1) идентификатор услуги;
2) идентификатор транспортного потока;
3) идентификатор сети;
4) версия протокола IP (4 или 6);
5) транспортный протокол (TCP или UDP);
6) многоадресная группа или адрес назначения;
7) номер порта назначения;
8) использование заголовка протокола RTP;
9) тип FEC;
10) формат кадра.

Пункты, приведенные ниже, не являются обязательными, но их наличие желательно с точки зрения безопасности, универсальности и облегчения действий устройств SVD:

11) IP-адрес источника;
12) номер порта источника;
13) размер пакета IP;
14) размер пакета TS;
15) скорость TS;
16) информация о потоке FEC, включая IP-адреса источника/назначения и номеров порта, если для пакетов FEC используется информация потока, отличного от транспортного потока.

Существует несколько способов распределения информации о соединении, приведенной выше, делящихся по типам извлечения и помещения. В типе жесткого определения возможна ситуация, когда информация всегда распределяется в виде таблицы с информацией о сети (NIT), используя внутренний многоадресный поток транспортного потока или определенный хорошо известный и внешний многоадресный поток, которому должны подчиняться все устройства SVD. С другой стороны, в гибком типе МОЖЕТ использоваться сервер информации о соединении, когда всем устройствам SVD необходимо воспользоваться этим сервером.

7.5 Восстановление потерь пакетов

Метод исправления ошибок полезно использовать при восстановлении потерь пакетов. Учитывая сценарии потерь импульсных пакетов, могут оказаться эффективными некоторые способы перемежения, когда калькуляция FEC осуществляется среди пакетов, чей порядок передачи отличается друг от друга. На рисунке 4 показан пример FEC, когда может быть восстановлено до 25 последовательных потерянных пакетов.

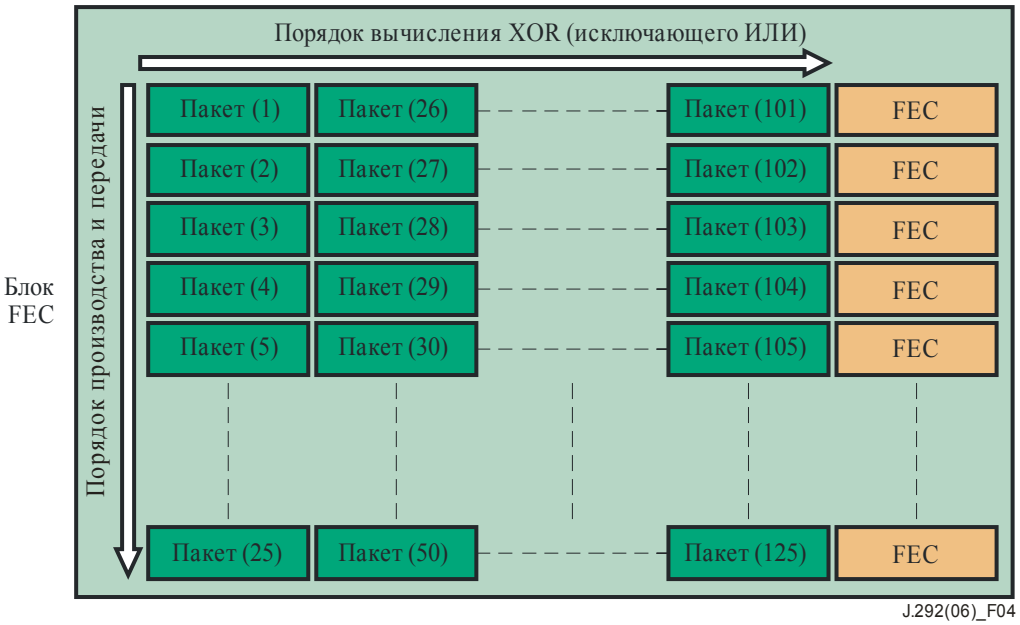


Рисунок 4 – Пример FEC

Некоторые отработанные способы FEC, например проверка четности с малой плотностью (LDPC), МОГУТ обеспечить лучшее качество восстановления пакетов. Также заслуживает внимания локальная повторная передача между шлюзом RGW и устройством SVD.

7.6 Синхронизация TS

Синхрогенератор декодера управляется и синхронизируется синхрогенератором кодера в сегменте центрального блока управления механизмом системы фазовой автоматической подстройки частоты (ФАПЧ) между передаваемыми пакетами PCR и регулируемым генератором, управляемым напряжением (ГУН) внутри декодера. Тем не менее, декодеру внутри устройства SVD НЕ СЛЕДУЕТ напрямую использовать пакеты PCR, передаваемые через сегмент CDN, из-за величины флуктуации обычных IP-сетей, которая выше терпимой флуктуации PCR, равной 500 нс, назначенной в системе MPEG-2. Следовательно, необходим механизм борьбы с флуктуацией, для удовлетворения требованиям системы MPEG-2. Метод борьбы с флуктуацией зависит от реализации и не рассматривается в данной Рекомендации.

7.7 Контроль смены программ

Смена программ, т. е. частое изменение многоадресных групп, увеличивает транзитный трафик и приводит к непроизводительному расходу ширины полосы пропускания. Для наиболее эффективного использования ширины полосы пропускания механизм контроля сменой программ СЛЕДУЕТ помещать в устройства, совместимые с архитектурой NG-STB-MI-A, управляющие протоколом многоадресного управления хост-маршрутизатора, т. е. IGMP и/или MLD.

Есть два способа осуществления контроля над сменой программ. Первый – это запретить запросы каналов от устройств SVD на определенный период времени, что означает, что устройство SVD не будет запрашивать ненужные каналы. Этот способ относится к управлению стороной получателя в многоадресном трафике.

Другой способ состоит в ограничении регистрируемого числа адресов многоадресных групп в таблице многоадресной передачи в промежуточных устройствах сети, управляющих сообщениями контроля IGMP и/или MLD, исходящих от устройств SVD. Такими устройствами могут быть: устройства на границе доступа RGW и CDN, например коммутатор 2/3 с возможностью IGMP/MLD (отслеживания). В таких устройствах многоадресная передача управляется таблицей многоадресной передачи, которая работает с адресами многоадресных групп и набором портов назначения. Смена программ может контролироваться ограничением регистрируемого числа адресов многоадресной группы портом назначения или MAC-адресом устройства SVD. Этот метод существенно ограничивает доступную максимальную полосу вещания многоадресного трафика портом назначения или MAC-адресом устройства SVD; следовательно, он относится к управлению стороной передатчика в многоадресном трафике.

7.8 Получение данных о местоположении

Так как IP-сеть CDN МОЖЕТ обслуживать достаточно большую область, например в пределах страны или даже по всему миру, требуется, чтобы устройство SVD в любой области имело возможность доступа к транспортным потокам, направляемым в другие географические регионы. Поэтому для управления областью распределения транспортных потоков, на базе сведений о местоположении устройств SVD МОЖЕТ понадобиться механизм получения данных о местоположении.

Местоположение устройств доступа на стороне клиента в сегменте сети CDN может координироваться оператором сети CDN; а местоположения шлюза RGW и устройств SVD должны быть связаны с местоположениями устройств доступа. Некоторые механизмы аутентификации на основе порта, например IEEE 802.1X, МОГУТ устанавливаться между каждой парой соседних устройств, например между шлюзом RGW и устройством доступа на стороне клиента, между шлюзом RGW и устройствами SVD и т. п.

8 Многоадресная передача по протоколу IP

8.1 Многоадресная передача по протоколу IP

Многоадресная передача по протоколу IP определяется как передача датаграммы IP в "группу узлов" (множество из нуля или большего числа узлов, идентифицируемых одним IP-адресом места назначения). Многоадресная датаграмма доставляется каждому члену своей группы узлов назначения в виде одноадресной IP-датаграммы. Членство в группе узлов является динамичным; т. е. узел в любое время МОЖЕТ войти и выйти из групп. В группе узлов не существует ограничения по расположению или числу участников, но некоторым узлам членство в группе МОЖЕТ быть запрещено. Группа узлов МОЖЕТ быть постоянной или временной. Постоянная группа имеет хорошо известный, административно присвоенный IP-адрес. А временная группа имеет динамический адрес, присваиваемый при создании группы по запросу узла.

Полная поддержка многоадресной передачи по протоколу IP позволяет хосту создавать, присоединяться и покидать группы узлов так же, как и посылать IP-датаграммы группам узлов. Она требует использования протокола Интернет управления группами (IGMP) и расширения IP-протокола и интерфейсов услуг локальной сети в пределах узла.

8.2 IGMP

IGMP (протокол Интернет управления группами) – это протокол, который используется между узлами и многоадресными маршрутизаторами в отдельной физической сети для установления членства в отдельных многоадресных группах. Многоадресные маршрутизаторы используют эту информацию при соединении с многоадресным протоколом маршрутизации в целях поддержки многоадресной передачи по протоколу IP, осуществляемой по сети интернет. Часть протокола IGMP, выполняющую многоадресную маршрутизацию, СЛЕДУЕТ реализовывать на маршрутизаторе.

Вхождение и выход из многоадресной группы осуществляется с помощью протокола IGMP. В момент запуска прикладной программы и присоединении к многоадресной группе протокол IGMP отправляет маршрутизаторам в подсети сообщение-отчет протокола IGMP об участии в группе с целью проинформировать их об узлах, входящих в многоадресную группу. Этот отчет называется сообщением присоединения протокола IGMP. Маршрутизатор отправляет сообщение-запрос протокола IGMP один раз в минуту для подтверждения присутствия устройств SVD в многоадресной группе. В ответ на это сообщение запроса каждое устройство SVD возвращает сообщение-отчет протокола IGMP об участии в группе. Таким образом, маршрутизатор обнаруживает, с каким из устройств SVD у него есть интерфейс, и отправляет многоадресный пакет только на нужный интерфейс.

Если используется протокол IGMPv2, то когда устройство SVD покидает многоадресную группу, оно отправляет явное сообщение выхода. Однако оно не сможет избежать получения многоадресных пакетов из определенных источников в сети, где нет заинтересованных устройств SVD.

Протокол IGMPv3 добавляет возможность "фильтрации источника", т. е. способность системы показывать свой интерес в получении пакетов только с адресов определенных источников, отправленных на определенный многоадресный адрес. Эта информация МОЖЕТ использоваться многоадресными протоколами маршрутизации во избежание отправки многоадресных пакетов от определенных источников в сети, где нет заинтересованных устройств SVD.

8.3 Отслеживание IGMP

Отслеживание IGMP является полезным протоколом управления многоадресной лавинной рассылкой. Когда устройство SVD отправляет сообщение протокола IGMP о присоединении к группе, коммутатор передает его маршрутизаторам. В этот момент коммутатор анализирует сообщение и регистрирует MAC-адрес многоадресной группы, к которой присоединяется устройство SVD. Коммутатор может ретранслировать многоадресный блок данных только на тот интерфейс, где имеется устройство SVD, исключая таким образом возможность лавинной рассылки многоадресных пакетов.

8.4 Протокол маршрутизации многоадресной передачи

Маршрутизаторы или коммутаторы не всегда находятся в той же самой подсети, где имеется устройство SVD. Протокол маршрутизации многоадресной передачи используется для определения местоположения устройства SVD. Первый транзитный маршрутизатор помещается в точку интерфейса между источником многоадресной передачи и сетью передачи пакетов, а последний транзитный маршрутизатор находится в точке интерфейса между многоадресной группой и сегментом сети CDN (см. рисунок 1). Протокол маршрутизации многоадресной передачи обычно используется на участке между первым и последним транзитными маршрутизаторами.

Имеется два режима работы протокола маршрутизации многоадресной передачи: уплотненный режим и разреженный режим. Уплотненный режим создает разветвленную конфигурацию распределения для одного источника и, основываясь на этой конфигурации, доставляет пакеты в режиме лавинной рассылки. Если доставка пакетов не требуется, она прекращается. Уплотненный режим не отправляет запрос о доставке пакета от устройства SVD к исходящему потоку маршрутизаторов. Разреженный режим осуществляет рассылку пакетов, основываясь на комбинации разветвленных конфигураций рассылки для одного многоадресного источника и для нескольких источников. В разреженном режиме определяются маршрутизатор центральной сети и маршрутизаторы, которые называются точками встречи (RP). В каждой многоадресной группе должна быть обязательно одна точка RP. На участке между многоадресным источником и точкой RP применяется разветвленная конфигурация распределения сообщений источника; на участке между точкой RP и устройством SVD многоадресной группы применяется другая конфигурация. В отличие от уплотненного режима, в разреженном режиме имеется функция запроса доставки многоадресных пакетов только на маршрутизаторы исходящего трафика. Она называется сообщением явного присоединения. В этом режиме, когда к группе присоединяется новое устройство, маршрутизатор может отправлять на маршрутизаторы исходящего трафика запрос доставки пакетов, расширить разветвленные конфигурации доставки, при этом становится доступной доставка многоадресных пакетов новым членам группы. Уплотненный режим МОЖЕТ оказать серьезное влияние на сети с лавинной рассылкой пакетов. Для работы большой сети многоадресного распределения рекомендуется разреженный режим.

9 Приоритет QoS и сопоставление правил

9.1 Приоритет QoS

Любое устройство SVD, принадлежащее к архитектуре, описанной в Рекомендации [ITU-T J.292], ДОЛЖНО иметь возможность обеспечения QoS под управлением шлюза на стороне пользователя (RGW).

Информативное ПРИМЕЧАНИЕ 1. – В этой Рекомендации предполагается, что оконечное устройство CPE ДОЛЖНО отвечать соответствующим спецификациям домашней сети, например UPnP.

Описание, приведенное в этом разделе, являет собой пример соединения QoS. Действующий протокол будет описан в будущих Рекомендациях. Метод управления QoS, включая управление доступом, от шлюза RGW к устройству SVD ДОЛЖЕН соответствовать спецификациям домашней сети.

Информативное ПРИМЕЧАНИЕ 2. – В случае использования архитектуры UPnP управляющие сообщения создаются элементами точки управления UPnP, и ответы на них передаются служебными элементами UPnP.

Данная архитектура также определяется как распределенная архитектура, в которой МОЖЕТ существовать несколько экземпляров определенной услуги в домашней сети (HN), которые МОГУТ использоваться взаимозаменяемо.

Информативное ПРИМЕЧАНИЕ 3. – Настоящая Рекомендация описывает определенные услуги QoS UPnP, которые ДОЛЖНЫ присутствовать в функции PS шлюза RGW.

Настоящая Рекомендация определяет три категории приоритетов QoS для передачи пакетов между шлюзом RGW и устройством SVD:

– номер значимости трафика;

– приоритет очередности;

– приоритет доступа к среде передачи.

9.1.1 Номер значимости трафика

Информативное ПРИМЕЧАНИЕ. – В этой Рекомендации трафик устройства UPnP представляет собой двустороннюю передачу пакетов между шлюзом RGW и устройством SVD. В таблице 3 показан номер значимости трафика (TIN) устройства UPnP. Заметим, что устройство UPnP назначает номер TIN от 0 до 7; номера TIN 1 и 2 – это номера более низкого приоритета, чем номер TIN 0, который назначается для трафика услуги доступного качества. Устройство UPnP управления QoS присваивает номер TIN функции управления трафиком, одной из функций услуг веб-портала (PS) на шлюзе RGW, основываясь на требованиях качества обслуживания (QoS) каждого оконечного устройства.

Список номеров TIN СЛЕДУЕТ зарегистрировать в базе данных PS шлюза RGW.

Таблица 3 – Номер значимости трафика

Номера значимости трафика
7 (Самая высокая)
6
5
4
3
0 (Доступное качество/системы прошлых поколений)
2
1 (Самая низкая)

9.1.2 Приоритет организации очереди

Предполагается, что пакеты от многих интерфейсов попадут функциям PS шлюза RGW, который принадлежит сети, описанной в Рекомендации [ITU-T J.292]. Однако пакеты ДОЛЖНЫ отправляться только на один интерфейс с устройством SVD. Для того чтобы гарантировать QoS для всех услуг в этом интерфейсе, ДОЛЖНА быть организована очередь пакетов. Эта Рекомендация описывает несколько процессов организации приоритетной очереди для пакетов QoS. Все описанные далее методы организации очереди широко используются, и выбор метода остается на усмотрение оператора.

Информативное ПРИМЕЧАНИЕ. – Выбор методов организации очереди СЛЕДУЕТ предоставить услуге или приложению (т. е. номер значимости трафика UPnP).

Эта комбинация методов организации очереди ДОЛЖНА быть зарегистрирована в базе данных PS шлюза RGW.

– *WFQ (организация очереди на основании весовых коэффициентов)*

  Метод WFQ динамически назначает приоритеты очередности для потока каждого применения. Он составляет расписание равномерного распределения полосы пропускания, на основании очередности передачи каждого пакета по протоколу IP. Этот метод помогает не допустить ситуации, когда пакеты большого размера препятствуют доставке пакетов малого размера.

– *CBWFQ (организация очереди на основании классов)*

  Метод CBFWQ разделяет пакеты по классам, которые назначает оператор, назначая им приоритет постановки в очередь. Этот метод составляет расписание распределения необходимой полосы пропускания для каждого явно назначенного класса. В то время как метод WFQ автоматически назначает очередь в потоке, метод CBWFQ может распределять полосу пропускания в соответствии с классом, явно назначенным оператором: этот метод позволяет осуществлять более гибкое управление организацией очереди.

– *PQ (Организация очереди по приоритету)*

Метод PQ создает четыре уровня очереди, т. е. высокая, средняя, нормальная и низкая, в соответствии с требуемым приоритетом. В этом методе пакеты в очереди с "высоким" уровнем приоритета получают первый приоритет. Пакеты другой очереди не отправляются, до тех пор пока полностью не переданы пакеты с "высокой" степенью приоритета. Метод PQ позволяет присваивать "высокий" приоритет пакетам, для которых критично время передачи, например пакетам VoIP или пакетам центрального процессора.

– *LLQ (Организация очереди с малой задержкой)*

Метод LLQ, как и метод CBWFQ, присваивает пакетам классы очередности, назначенные оператором, и может установить пакету высокий приоритет доставки. Полоса пропускания распределяется между пакетами с высоким приоритетом и всеми остальными. Метод LLQ позволяет доставлять приоритетные пакеты VoIP и пакеты других приложений, а также обеспечивать гарантированную полосу пропускания.

– *WRR (Циклическая очередь на основании весовых коэффициентов)*

У метода WRR есть четыре очереди для выходного интерфейса, и он формирует очередь в соответствии с указанным приоритетом пакета. Приоритет пакета и очередность его передачи определены предварительно и четко связаны, и каждая очередь имеет весовой коэффициент. Метод WRR осуществляет организацию очереди в соответствии с весовыми коэффициентами и управляет доставкой пакетов. Только одна очередь из четырех может получить высокий приоритет. Передача начинается с первого приоритета, а пакеты с другими приоритетами доставляются после завершения передачи пакетов с более высоким приоритетом. Пакет VoIP обычно получает первый приоритет.

9.1.3 Приоритет доступа к среде передачи

В данной Рекомендации описывается механизм очередности QoS с помощью приоритетных потоков пакетов в совместно используемой среде передачи. На рисунке 5 в качестве примера показана многоадресная радиовещательная передача с заранее определенной полосой пропускания и приоритетные QoS.

Информативное ПРИМЕЧАНИЕ. – Участок между шлюзом RGW и устройством SVD является участком QoS устройства UPnP; каждый пакет имеет свой приоритет, и на этом участке регулируется организация очереди.

С другой стороны полоса пропускания назначена заранее на участке доступа, а пакет в QoS основе DiffServ управляется с помощью поля ToS, содержащего данные об IP-приоритете, DSCP или CoS.

До тех пор пока участок сети CDN имеет достаточный объем ресурсов, а выделенная ему полоса пропускания больше суммарной полосы пропускания всех пакетов с определенными приоритетами, качество пакетов с определенными приоритетами гарантируется тем, что первыми доставляются пакеты с приоритетным QoS. Например, если общая полоса пропускания всех пакетов в очереди составляет 100 Мбит/с, а полоса пропускания, выделенная участку сети CDN, превышает 100 Мбит/с, то пакеты в очереди должны доставляться без потерь при указанных приоритетах QoS. Исходя из качества, приоритетное QoS с заранее предоставленной полосой пропускания считается эквивалентным параметрическому QoS.

Преобразование QoS ДОЛЖНО выполняться в шлюзе RGW для обеспечения сигнализации QoS на каждом участке сети.

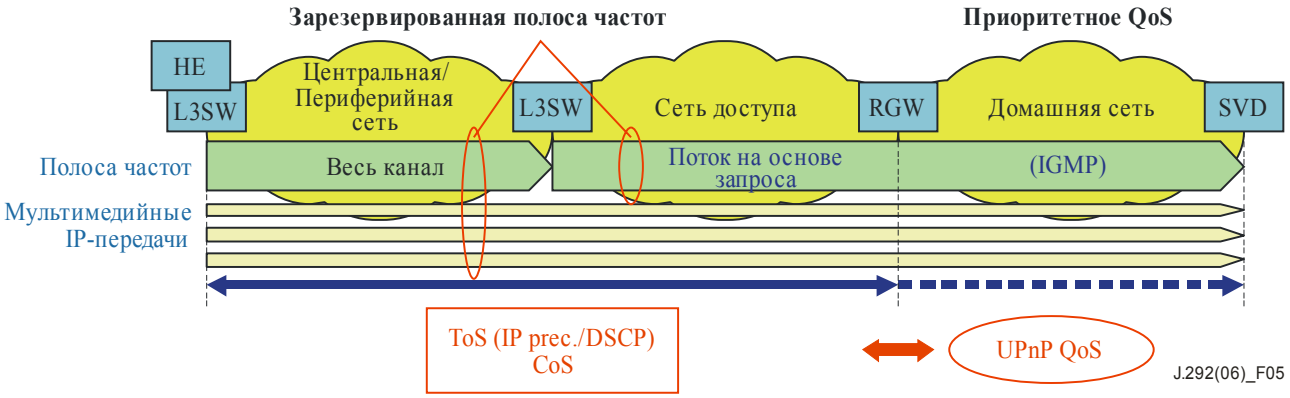


Рисунок 5 – Полоса пропускания в виде многоадресной передачи

Подробное описание сопоставления правил QoS находится вне сферы рассмотрения настоящей Рекомендации, но общие указания содержатся в параграфе 9.2.

9.2 Преобразование правил QoS

Поток пакетов ДОЛЖЕН управляться при помощи приоритетного пакета QoS и приоритетной организации очереди между шлюзом RGW и устройством SVD.

Информативное ПРИМЕЧАНИЕ. – Хранитель правил QoS и Менеджер QoS играют основную роль в схеме управления QoS устройства UPnP.

Хранитель правил QoS ДОЛЖЕН регистрировать правила QoS и ДОЛЖЕН обеспечивать интерфейс для правил доступа; однако ему НЕ СЛЕДУЕТ управлять ресурсами QoS. Менеджер QoS работает совместно с Хранителем правил QoS и управляет ресурсами QoS на участке локальной сети (LAN). Устройство SVD ДОЛЖНО обеспечивать поддержку QoS с помощью информации о ресурсах и предоставлять интерфейс для управления ресурсами. На рисунке 6 показана взаимосвязь между механизмами преобразования правил QoS.

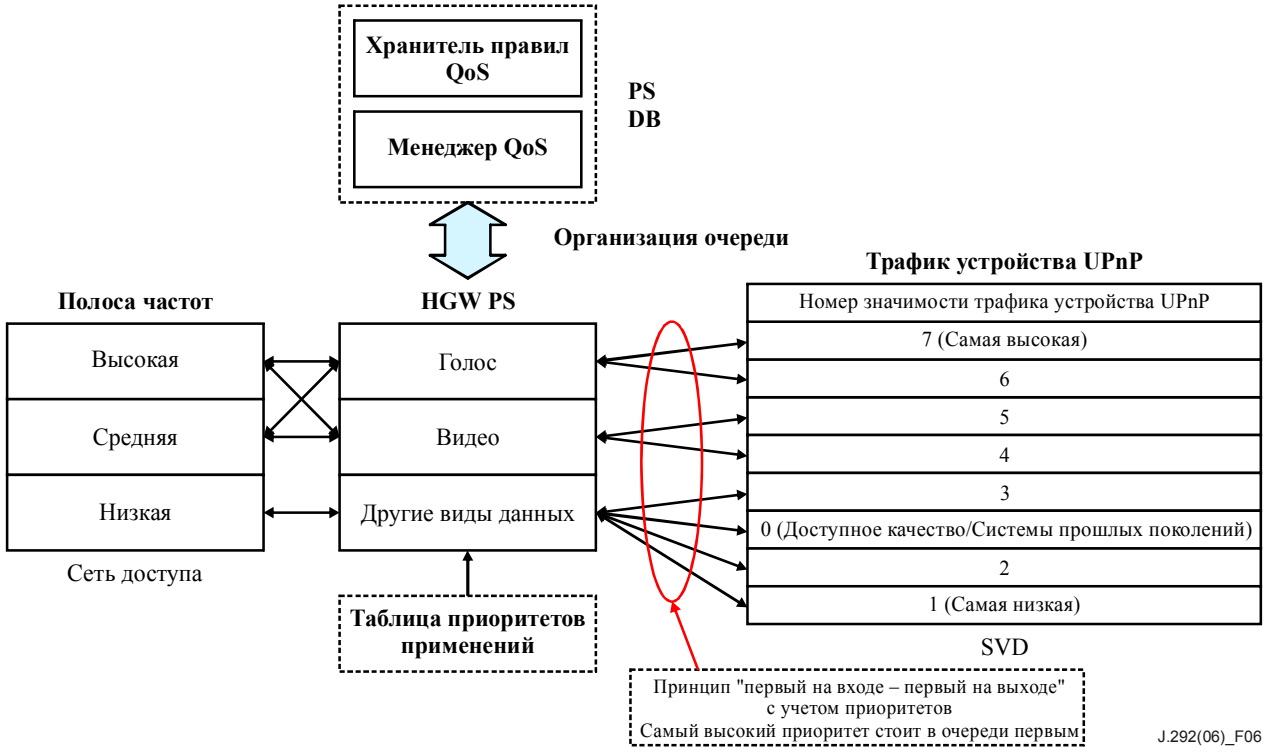


Рисунок 6 – Взаимосвязь между механизмами преобразования правил QoS

Для разных услуг могут понадобиться многочисленные таблицы преобразования. Эти таблицы преобразования СЛЕДУЕТ контролировать с помощью правил QoS, а управлять ими должен Менеджер QoS. На рисунке 6 показаны механизмы преобразования QoS, приоритет которых определяется услугами; могут применяться другие методы присвоения приоритетов, использующие номер порта. Базы данных услуг PS ДОЛЖНЫ содержать таблицы преобразования.

10 Вещание по протоколу IP и коммутатор каналов

Вещание требует того, чтобы все программы доставлялись на оконечное устройство; однако тенденции развития технологии допускают, чтобы в процессе радиовещания для доставки всех программ на ближайшую станцию использовались линии связи. Это означает, что многоадресная доставка на последний транзитный маршрутизатор связи является одним из видов вещания, т. е. вещанием по протоколу IP. Услуга VoD является одним из применений вещания по протоколу IP, и для ее предоставления занимается полоса частот, требуемая для передачи программы абоненту. На рисунке 7 показана взаимосвязь между вещанием по протоколу IP и коммутатором каналов. Весь контент вещания по протоколу IP, т. е. IP-поток (IPS), доставляется на коммутатор каналов от центрального блока управления. Выбранный контент доставляется на оборудование пользователя (CPE) от коммутатора канала связи.

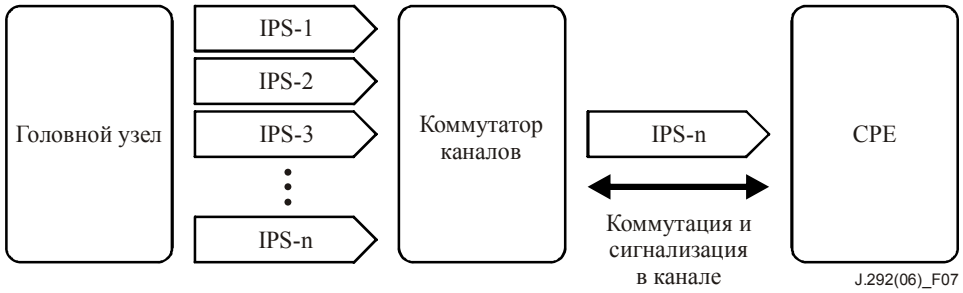


Рисунок 7 – Взаимосвязь между вещанием по протоколу IP и коммутатором каналов

Поток IPS – это поток IP-пакетов, для которого известны адрес и номер порта. Предполагается, что коммутатор каналов, не определенный при физической реализации, включает в себя коммутатор станции с устройствами OLT/DSLAM, терминал сети со шлюзом RGW и программное обеспечение, используемое в устройствах CPE. Сигнал выбора канала – это поступающая от CPE информация сигнализации управления коммутатором каналов, в настоящее время он использует IP-протоколы многоадресного управления, например IGMP/MLD. Он необходим для того, чтобы в расширенных функциональных возможностях учитывались требования для анонимных запросов.

Обнаружение многоадресного приемника (MLD) – это протокол, который используется маршрутизатором в стеке протокола IPv6 для поисков приемников определенной многоадресной группы, почти точно так же, как используется протокол IGMP в стеке протокола IPv4. Вместо того чтобы использовать отдельный протокол, он включается в состав протокола управляющих сообщений в интернет (ICMP) версии 6. Этот протокол описан в документе IETF RFC 2710.

Протоколы MLD и MLDv2 эквивалентны протоколам IGMPv2 и IGMPv3, соответственно.

Библиография

[b-ITU-T J.200] ITU-T Recommendation J.200 (2001), *Worldwide common core – Application environment for digital interactive television services*.

[b-ITU-T J.201] Рекомендация МСЭ-Т J.201 (2004 г.), *Согласование формата декларативного контента для приложений по интерактивному телевидению*.

[b-ITU-T J.202] Рекомендация МСЭ-Т J.202 (2005 г.), *Согласование форматов процедурного контента для приложений интерактивного ТВ*.

[b-ITU-T J.282] ITU-T Recommendation J.282 (2006), *Architecture of multi-channel video signal distribution over IP-based networks*.

[b-ITU-T J.283] Рекомендация МСЭ-Т J.283 (2006 г.), *Архитектура IP-сетей с разнесением маршрутов сетевого уровня, обеспечивающих устойчивое распределение видеосигналов при многоадресной передаче по IP*.

[b-IETF RFC 768] IETF RFC 768 (1980), *User Datagram Protocol*.

[b-IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.

[b-IETF RFC 793] IETF RFC 793 (1981), *Transmission Control Protocol*.

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

[b-IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.

[b-IETF RFC 2236] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*.

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[b-IETF RFC 2733] IETF RFC 2733 (1999), *An RTP Payload Format for Generic Forward Error Correction*.

[b-IETF RFC 3022] IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT)*.

[b-IETF RFC 3376] IETF RFC 3376 (2002), *Internet Group Management Protocol, Version 3*.

[b-IETF RFC 3810] IETF RFC 3810 (2004), *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*.

[b-IEEE 802.1] IEEE 802.1: 802.1X – *Port Based Network Access Control*.

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

Отпечатано в Швейцарии
Женева, 2009 г.