

**МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ  
УЗБЕКИСТАН**

**ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ**

**Кафедра сетей и систем передачи данных**

**«ИЗУЧЕНИЕ ПРИНЦИПОВ ТЕХНОЛОГИИ IPTV»**

**Методические указания к практическим занятиям**

**по дисциплине:**

**«СЛУЖБЫ МУЛЬТИМЕДИА»**

**Для магистрантов I курса обучающихся по направлению SA350101  
Телекоммуникационный инжиниринг**

**Ташкент 2015**

# ТИЯ

## *Изучение принципов технологии IPTV*

### 1. Цель занятий

- 1.1. Изучение общих принципов пакетной передачи видео данных (сигналов)
- 1.2. Изучение протоколов используемых в сетях IPTV
- 1.3. Изучение структуры построения и стандартизации IPTV
- 1.4. Изучение проблем обеспечения качества обслуживания в сетях IPTV

### 2. Домашние задания

- 2.1. Изучить теоретический материал, приведенный в настоящем пособии и в литературах
- 2.2. Перечислите методы доставки видео данных в сетях IPTV
- 2.3. Описать процессы инкапсуляции при передаче видео данных по сетям с коммутацией пакетов
- 2.4. Перечислите преимущества технологии IPTV относительно традиционных сетей кабельного и спутникового телевидения
- 2.5. Перечислить особенности технологий IntServ, DiffServ, MPLS при обеспечении качества обслуживания в сетях IPTV.

<b>ВВЕДЕНИЕ</b> .....	4
<b>1. ОСНОВЫ МЕЖСЕТЕВОГО ОБМЕНА В ГЛОБАЛЬНЫХ СЕТЯХ</b> .....	9
1.1. Эталонная модель взаимодействия открытых систем OSI.....	9
1.2. Общие принципы пакетной коммутации.....	11
1.3. Структура стека протоколов TCP/IP.....	12
<b>2. ПРИНЦИП ПАКЕТНОЙ ПЕРЕДАЧИ ВИДЕО СИГНАЛОВ.</b>	16
2.1. Принципы инкапсуляции видео данных в пакеты MPEG- TS.....	16
2.2. Кодеки используемые при передаче видео данных поверх IP.....	18
<b>3. ПРОТОКОЛЫ ИСПОЛЬЗУЕМЫЕ В IPTV</b> .....	22
3.1. Транспортные протоколы UDP, RTP.....	23
3.2. Протоколы управления RTSP, RTSP.....	25
3.3. Протоколы IGMP, HTTP.....	27
<b>4. СТРУКТУРА IPTV</b> .....	28
4.1. Услуги IPTV.....	29
4.2. Архитектура IPTV.....	32
4.3. Режимы передачи трафика и протоколы в IP-сетях.....	39
4.4. Достоинства и недостатки IPTV.....	42
<b>5. СТАНДАРТИЗАЦИЯ IPTV</b> .....	43
<b>6. ОБЕСПЕЧЕНИЕ КАЧЕСТВА IPTV</b> .....	46
6.1. Показатели качества передачи видео.....	46
6.2. Методы оценки качества IPTV.....	48
6.2.1. Субъективные методы.....	49
6.2.2. Объективные методы.....	56
6.3. Влияние сети на показатели качества передачи видео данных (сигналов).....	63
6.4. Механизмы обеспечения качества передачи видео данных (сигналов).....	65
<b>ЛИТЕРАТУРА</b> .....	

## ВВЕДЕНИЕ

В условиях современного динамичного развития общества информация становится таким же стратегическим ресурсом, как и традиционные ресурсы: материальные и энергетические. Современные информационные технологии, позволяющие создавать, хранить, перерабатывать и обеспечивать эффективные способы представления информации потребителю, стали неотъемлемой частью жизни общества и средством повышения эффективности управления всеми сферами общественной деятельности.

За годы независимости Узбекистана произошли кардинальные изменения в жизни нашего общества, коренным образом изменились цели и задачи, стоящие сегодня перед нашей экономикой, телекоммуникационной отраслью, информационной индустрией.

В Узбекистане установилась макроэкономическая и финансовая стабильность, осуществляется модернизация и техническое перевооружение в сфере телекоммуникаций, призванной стать эффективным локомотивом нашей экономики. Создаются необходимый фундамент и условия для дальнейшего устойчивого развития данной отрасли, все большей ее интеграции в мировое информационно - телекоммуникационное пространство.

Для обеспечения условий оперативной работы необходимо иметь качественные услуги, основанные на современных средствах телекоммуникаций, использующих новейшие технологии.

Последние десятилетия характеризуются лавинообразным ростом объемов самой различной информации: социально- политической, производственной, научной, культурной и др. Широкое использование средств вычислительной техники, а также создание информационной- вычислительных систем и сетей самых разнообразных конфигураций позволит во многом преодолеть проблемы, связанные с так называемым «информационным взрывом». Как показывает международный опыт

развитых стран, наиболее перспективный путь использования информационно-вычислительной техники основывается на ее интеграции с современными высокоскоростными системами телекоммуникаций. Это видно на примере объединения современных телекоммуникационных и компьютерных технологий, наиболее полно реализованных в глобальной компьютерной сети Интернет. Поэтому построение развитого государства невозможно без создания современной информационной инфраструктуры, которая должна базироваться на мощной транспортной сети телекоммуникаций и распределенных сетях доступа. Кроме того, одной из основных тенденций развития телекоммуникаций является постепенная интеграция самих служб телекоммуникаций на базе широкополосных транспортных сетей, глобализация телекоммуникаций, а также персонализация всех служб телекоммуникаций и интеллектуализация сетей. Взаимопроникновение современных компьютерных и телекоммуникационных технологий обеспечивает создание инфокоммуникационных сетей с широким набором разнообразных услуг пользователям. При этом каждый вид телекоммуникаций, постепенно вбирая в себя самые последние достижения научно-технического прогресса (цифровые принципы обработки сигналов, широкополосные системы коммутации и передачи данных, системы передачи синхронной цифровой иерархии, волоконно-оптические линии и др.), выходит на качественно новый уровень. В этой связи все виды телекоммуникаций становятся в плане реализуемых технических принципов однородными, что обеспечивает техническую возможность и экономическую целесообразность их интеграции в единую систему.

Таким образом, оказывая существенное влияние на различные сферы человеческой деятельности (экономику, науку, культуру, образование, промышленность и т.д.) современные крупномасштабные системы передачи общего пользования станут важнейшим компонентом Глобального информационного общества XXI века.

Основными этапами развития крупномасштабных сетей передачи информации являются: сети передачи данных с коммутацией пакетов на базе технологий IP/MPLS и Gigabit Ethernet; цифровые сети с интеграцией служб (узкополосные и широкополосные); высокоскоростные сети с технологией SDH и DWDM.

Непрерывный рост скоростей и числа локальных вычислительных сетей (ЛВС), растущие потребности в количестве и скорости передаваемой информации, влекут за собой бурное развитие глобальных сетей с коммутацией пакетов. Именно на методах пакетной передачи и коммутации построено функционирование современных сетей. Заложённая в них идея проста: информация любого вида (данные, изображение, речь, звук, служебные и управляющие посылки и т.д.) представляются в виде цифровой последовательности, которая в дальнейшем делится на пакеты, снабжённые всей необходимой информацией для идентификации, маршрутизации, коррекции ошибок и прочее. Подобный подход позволяет в едином информационном русле передавать все виды информации, используя для этого различные пути и средства, применяя универсальные системы коммутации, инвариантные относительно видов информации.

Работа устройств в сети Интернет осуществляется с использованием специального протокола IP (Internet Protocol - протокол межсетевое взаимодействия). В настоящее время IP протокол используется не только в сети Интернет, но и в других сетях передачи данных с пакетной коммутацией (локальных, корпоративных, региональных и др.). И во всех этих сетях, имеется возможность передавать видео данные с использованием пакетов данных. Такой способ передачи видео получил название IP-телевидение. За рубежом обычно употребляется аббревиатура IPTV – IP-television. В широком смысле основная задача обсуждаемого варианта телевидения заключается в обеспечении телевидением нескольких лиц, являющихся абонентами сетей операторов связи с коммутацией пакетов.

Интерес различных субъектов рынка телекоммуникационных услуг (операторов связи, провайдеров Интернет, производителей оборудования и пользователей) к данному виду услуг необычно возрос в последние годы в связи с разработкой новых стандартов и протоколов, когда IP-телевидение вплотную приблизилось по качеству к цифровому телевидению по "классическим" кабельным сетям. Этот интерес объясняется тем, что IP-телевидение позволяет внедрить ряд инновационных, существенно экономить требуемую полосу пропускания каналов, что неизбежно ведет к снижению тарифов, особенно на междугородние и международные телефонные разговоры.

Телекоммуникационный рынок испытывает в настоящее время поистине революционное развитие. Массовое внедрение цифрового телевидения уже произошло в странах Европы и в Республике Узбекистан и этому уделяется особое внимание. В настоящее время согласно постановлению Президента Республики Узбекистан, внедрение в Республике Узбекистан цифрового телевещания является вопросом общегосударственного значения. Наряду со многими странами Европы и СНГ, в рамках проведения Региональной конференции радиосвязи по наземному цифровому вещанию в Женеве 2006 г., Узбекистан подписал договор о постепенном переходе к цифровому телерадиовещанию к 2017 году. Это соглашение предусматривает отказ на территории нашего государства от аналогового телевизионного сигнала и переход на более современный формат вещания – цифровой.

В последние 5-6 лет у цифрового телевидения появился серьезный конкурент – IPTV (Телевидение по протоколу IP). Этот вид телевидения также оперирует с цифровыми сигналами, но при их передаче и распределении использует принципы IP сетей (сетей Интернет). При этом телевизионные операторы и абоненты получают дополнительные преимущества: высокая экономичность при использовании каналов, возможность передачи сигналов по уже существующим сетям передачи

данных, появление большого количества новых видео и аудио услуг и многое другое. Одним из главных достоинств IPTV является естественная интеграция с другими телекоммуникационными сервисами: телефонией и передачей данных, что в совокупности образует сеть Triple Play.

Все это показывает, что IPTV является перспективной, быстро развивающейся услугой телекоммуникаций, которая будет постепенно вытеснять традиционные кабельные сети широковещательного телевидения. Системы IPTV в настоящее время применяются организациями самых разных форм собственности и направлений деятельности. Оборот капитала IPTV увеличивается на 30 %, а по некоторым направлениям и на 50 % в год. Технология IP не только обладает быстрой окупаемостью, но и приносит значительную прибыль организациям, в которых она была внедрена, за счет повышения качества обслуживания абонентов, повышения эффективности работы сотрудников.

Настоящие методические указания рассматривают общие принципы построения, эффективности использования IPTV и предназначены как для бакалавров, так и для магистров и обладают информацией, необходимой для ознакомления с современной услугой телекоммуникаций – IPTV.



# 1. ОСНОВЫ МЕЖСЕТЕВОГО ОБМЕНА В ГЛОБАЛЬНЫХ СЕТЯХ

## 1.1. Эталонная модель взаимодействия открытых систем OSI

При рассмотрении процедур межсетевого взаимодействия всегда опираются на стандарты, разработанные International Standard Organization (ISO). Эти стандарты получили название "Семиуровневой модели сетевого обмена" или в английском варианте "Open System Interconnection Reference Model" (OSI Model). В данной модели обмен информацией может быть представлен в виде стека, представленного на рис. 1.1. Как видно из рисунка, в этой модели определяется все - от стандарта физического соединения сетей до протоколов обмена прикладного программного обеспечения.

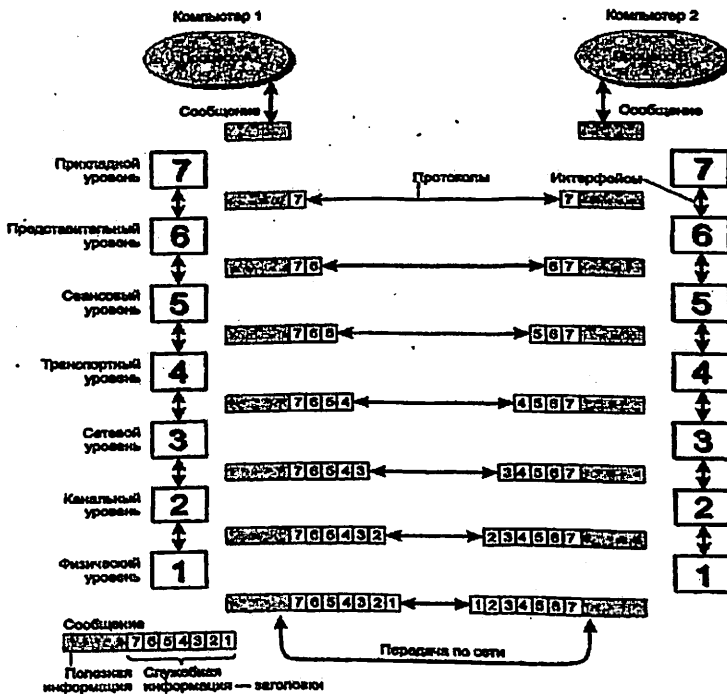


Рис. 1.1. Семиуровневая модель протоколов межсетевого обмена OSI

Физический уровень данной модели определяет характеристики физической сети передачи данных, которая используется для межсетевого обмена. Это такие параметры, как: напряжение в сети, сила тока, число контактов на разъемах и т.п. Типичными стандартами этого уровня являются, например RS232C, V3.5, IEEE 802.3 и т.п.

К канальному уровню отнесены протоколы, определяющие соединение, например, SLIP (Serial Line Internet Protocol), PPP (Point to Point Protocol), NDIS, пакетный протокол, ODI и т.п. В данном случае речь идет о протоколе взаимодействия между драйверами устройств и устройствами, с одной стороны, а с другой стороны, между операционной системой и драйверами устройства. Такое определение основывается на том, что драйвер - это, фактически, конвертор данных из одного формата в другой, но при этом он может иметь и свой внутренний формат данных.

К сетевому (межсетевому) уровню относятся протоколы, которые отвечают за отправку и получение данных, или, другими словами, за соединение отправителя и получателя. Вообще говоря, эта терминология пошла от сетей коммутации каналов, когда отправитель и получатель действительно соединяются на время работы каналом связи. Применительно к сетям TCP/IP, такая терминология не очень приемлема. К этому уровню в TCP/IP относят протокол IP (Internet Protocol). Именно здесь определяется отправитель и получатель, именно здесь находится необходимая информация для доставки пакета по сети.

Транспортный уровень отвечает за надежность доставки данных, и здесь, проверяя контрольные суммы, принимается решение о сборке сообщения в одно целое. В Internet транспортный уровень представлен двумя протоколами TCP (Transport Control Protocol) и UDP (User Datagram Protocol). Если предыдущий уровень (сетевой) определяет только правила доставки информации, то транспортный уровень отвечает за целостность доставляемых данных.

Уровень сессии определяет стандарты взаимодействия между собой прикладного программного обеспечения. Это может быть некоторый промежуточный стандарт данных или правила обработки информации. Условно к этому уровню можно отнести механизм портов протоколов TCP и UDP и Berkeley Sockets. Однако обычно, рамках архитектуры TCP/IP такого подразделения не делают.

Уровень обмена данными с прикладными программами (Presentation Layer) необходим для преобразования данных из промежуточного формата сессии в формат данных приложения. В Internet это преобразование возложено на прикладные программы.

Уровень прикладных программ или приложений определяет протоколы обмена данными этих прикладных программ. В Internet к этому уровню могут быть отнесены такие протоколы, как: FTP, TELNET, HTTP, GOPHER и т.п.

## 1.2. Общие принципы пакетной коммутации

При коммутации пакетов все передаваемые пользователем данные разбиваются передающим узлом на небольшие (до нескольких килобайт) части — пакеты (packet). Каждый пакет оснащается заголовком, в котором указывается, как минимум, адрес узла-получателя и номер пакета. Передача пакетов по сети происходит независимо друг от друга. Коммутаторы такой сети имеют внутреннюю буферную память для временного хранения пакетов, что позволяет сглаживать пульсации трафика на линиях связи между коммутаторами. Пакеты иногда называют дейтаграммами (datagram), а режим индивидуальной коммутации пакетов — дейтаграммным режимом.

### 1.3. Структура стека протоколов TCP/IP

Главной задачей стека TCP/IP является объединение в сеть пакетных подсетей через шлюзы. Каждая сеть работает по своим собственным законам, однако предполагается, что шлюз может принять пакет из другой сети и доставить его по указанному адресу. Реально, пакет из одной сети передается в другую подсеть через последовательность шлюзов, которые обеспечивают сквозную маршрутизацию пакетов по всей сети. В данном случае, под шлюзом понимается точка соединения сетей. При этом соединяться могут как локальные сети, так и глобальные сети. В качестве шлюза могут выступать как специальные устройства, маршрутизаторы, например, так и компьютеры, которые имеют программное обеспечение, выполняющее функции маршрутизации пакетов. Маршрутизация - это процедура определения пути следования пакета из одной сети в другую.

Такой механизм доставки становится возможным благодаря реализации во всех узлах сети протокола межсетевого обмена IP. Если обратиться к истории создания сети Internet, то с самого начала предполагалось разработать спецификации сети коммутации пакетов. Это значит, что любое сообщение, которое отправляется по сети, должно быть при отправке "нашинковано" на фрагменты. Каждый из фрагментов должен быть снабжен адресами отправителя и получателя, а также номером этого пакета в последовательности пакетов, составляющих все сообщение в целом. Такая система позволяет на каждом шлюзе выбирать маршрут, основываясь на текущей информации о состоянии сети, что повышает надежность системы в целом. При этом каждый пакет может пройти от отправителя к получателю по своему собственному маршруту. Порядок получения пакетов получателем не имеет большого значения, т.к. каждый пакет несет в себе информацию о своем месте в сообщении (рис. 1.2).

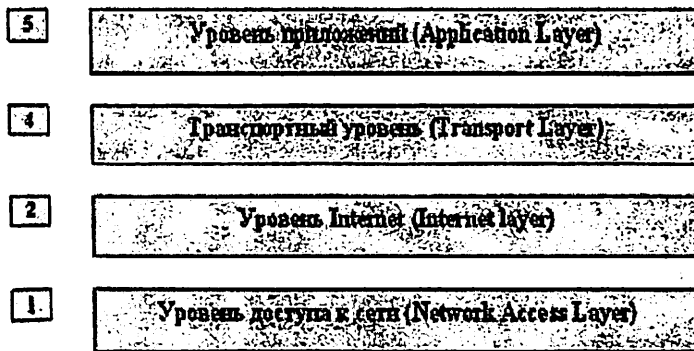


Рис. 1.2. Структура стека протоколов TCP/IP

В этой схеме на уровне доступа к сети располагаются все протоколы доступа к физическим устройствам. Выше располагаются протоколы межсетевого обмена IP, ARP, ICMP. Еще выше основные транспортные протоколы TCP и UDP, которые кроме сбора пакетов в сообщения еще и определяют какому приложению необходимо данные отправить или от какого приложения необходимо данные принять. Над транспортным уровнем располагаются протоколы прикладного уровня, которые используются приложениями для обмена данными.

На прикладном уровне (Application layer) работает большинство сетевых приложений. Эти программы имеют свои собственные протоколы обмена информацией, например, HTTP для WWW, FTP (передача файлов), SMTP (электронная почта), SSH (безопасное соединение с удалённой машиной), DNS (преобразование символьных имён в IP-адреса) и многие другие.

В массе своей эти протоколы работают поверх TCP или UDP и привязаны к определённому порту, например: HTTP на TCP-порт 80 или 8080, FTP на TCP-порт 20 (для передачи данных) и 21 (для управляющих команд), SSH на TCP-порт 22, запросы DNS на порт UDP (реже TCP) 53, обновление маршрутов по протоколу RIP на UDP-порт 520.

Протоколы транспортного уровня (Transport layer) могут решать проблему негарантированной доставки сообщений («дошло ли сообщение до адресата?»), а также гарантировать правильную последовательность прихода данных. В стеке TCP/IP транспортные протоколы определяют, для какого именно приложения предназначены эти данные.

Протоколы автоматической маршрутизации, логически представленные на этом уровне (поскольку работают поверх IP), на самом деле являются частью протоколов сетевого уровня; например OSPF (IP идентификатор 89).

TCP — «гарантированный» транспортный механизм с предварительным установлением соединения, предоставляющий приложению надёжный поток данных, дающий уверенность в безошибочности получаемых данных, перезапрашивающий данные в случае потери и устраняющий дублирование данных. TCP позволяет регулировать нагрузку на сеть, а также уменьшать время ожидания данных при передаче на большие расстояния. Более того, TCP гарантирует, что полученные данные были отправлены точно в такой же последовательности. В этом его главное отличие от UDP.

UDP протокол передачи датаграмм без установления соединения. Также его называют протоколом «ненадёжной» передачи, в смысле невозможности удостовериться в доставке сообщения адресату, а также возможного перемешивания пакетов. В приложениях, требующих гарантированной передачи данных, используется протокол TCP.

UDP обычно используется в таких приложениях, как потоковое видео и компьютерные игры, где допускается потеря пакетов, а повторный запрос затруднён или не оправдан, либо в приложениях вида запрос-ответ (например, запросы к DNS), где создание соединения занимает больше ресурсов, чем повторная отправка.

И TCP, и UDP используют для определения протокола верхнего уровня число, называемое портом.

Сетевой уровень (Internet layer) изначально разработан для передачи данных из одной (под)сети в другую. С развитием концепции глобальной сети в уровень были внесены дополнительные возможности по передаче из любой сети в любую сеть, независимо от протоколов нижнего уровня, а также возможность запрашивать данные от удалённой стороны, например в протоколе ICMP (используется для передачи диагностической информации IP-соединения) и IGMP (используется для управления multicast-потоками).

ICMP и IGMP расположены над IP и должны попасть на следующий — транспортный — уровень, но функционально являются протоколами сетевого уровня, и поэтому их невозможно вписать в модель OSI.

Пакеты сетевого протокола IP могут содержать код, указывающий, какой именно протокол следующего уровня нужно использовать, чтобы извлечь данные из пакета. Это число — уникальный IP-номер протокола. ICMP и IGMP имеют номера, соответственно, 1 и 2.

Канальный уровень (Link layer) описывает, каким образом передаются пакеты данных через физический уровень, включая кодирование (то есть специальные последовательности бит, определяющих начало и конец пакета данных). Ethernet, например, в полях заголовка пакета содержит указание того, какой машине или машинам в сети предназначен этот пакет. Кроме того, канальный уровень описывает среду передачи данных (будь то коаксиальный кабель, витая пара, оптическое волокно или радиоканал), физические характеристики такой среды и принцип передачи данных (разделение каналов, модуляцию, амплитуду сигналов, частоту сигналов, способ синхронизации передачи, время ожидания ответа и максимальное расстояние).

## **2. ПРИНЦИП ПАКЕТНОЙ ПЕРЕДАЧИ ВИДЕО СИГНАЛОВ**

Головное IP-TV оборудование передает, а абонентское оборудование принимает потоковое видео (streaming video). Этот термин обозначает технологии сжатия, сокращения и буферизации видео данных, которые позволяют передавать видео сигналы в реальном времени через сеть с пакетной коммутацией. Главная особенность потокового видео заключается в том, что при его передаче пользователь не должен ждать полной загрузки файла для того, чтобы его просмотреть. Потоковое видео пересылается непрерывным потоком в виде последовательности IP-пакетов и проигрывается по мере того, как передается на абонентское устройство.

Некоторые провайдеры используют шифрование потока, чтобы определённые каналы можно было смотреть только через теле приставку с использованием идентификационной карты или пин -кода, такой поток плеер воспроизвести не сможет. Если провайдер продаёт услугу только вместе с приставкой и шифрует каналы, то плеер для вас также будет бесполезен.

Основная функция головной станции IPTV это формирование видео-контента и последующая трансляция выходного потока видео-данных в формате Video over IP (видео по IP протоколу). Функцию инкапсуляции в головной станции выполняет его составная часть называемая IP-инкапсулятор или IP-стриммер.

### **2.1. Принципы инкапсуляции видео данных в пакеты MPEG-TS**

Инкапсуляция – это главный процесс, выполняемый IPTV станцией. Для передачи транспортных MPEG-потоков через традиционные сети с пакетной передачей данных, головная станция IPTV объединяет множество 188-ми байтовых MPEG транспортных пакетов и формирует из них полезную нагрузку кадра PDU (protocol data unit).



Заголовок (Header) и замыкающая часть кадра (Trailer) определяются используемым сетевым протоколом.

Инкапсуляция MPEG -пакетов в Gigabit Ethernet сетях.

Рисунки 2.1., 2.2 и 2.3 иллюстрируют инкапсуляцию MPEG-пакетов в Gigabit Ethernet сетях.

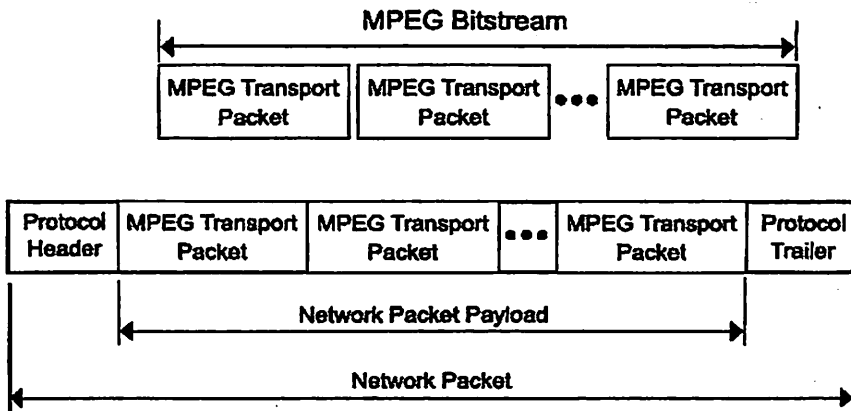


Рис. 2.1. Иллюстрация процесса инкапсуляции.

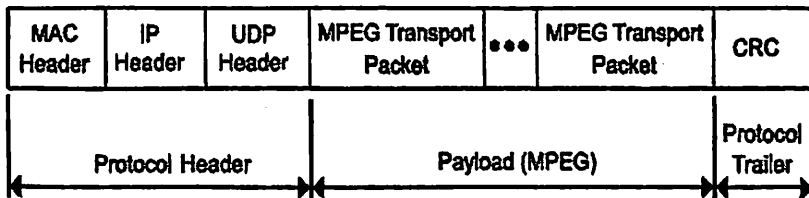


Рис. 2.2. Кадр в формате MPEG over UDP/IP over Gigabit Ethernet.

На рис 2.2 показан кадр в формате MPEG over UDP/IP over Gigabit Ethernet. Замыкающая часть кадра это как обычно CRC (cyclic redundancy code) – контрольный циклический избыточный код.

Рис. 2.3 показывает инкапсуляцию MPEG over Gigabit Ethernet в реальном времени с использованием протокола RTP.

Tashkent axborot  
 texnologiyalari universiteti  
 Axborot-Resurs markazi

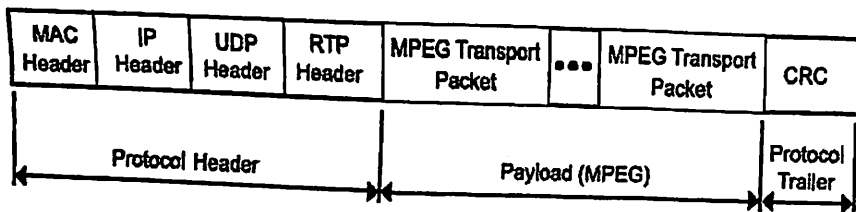


Рис. 2.3. Инкапсуляция MPEG over Gigabit Ethernet в реальном времени с использованием протокола RTP.

Протокол RTP (Real-time transport protocol) определяет и компенсирует потерянные пакеты, обеспечивая безопасность передачи контента и распознавание информации. Протокол RTP функционирует поверх протокола UDP (User Datagram Protocol), расположенного в стеке протоколов TCP/IP над протоколом IP. Разница между двумя рисунками только в добавлении RTP-заголовка в секцию заголовка протокола (Protocol Header).

## 2.2. Кодеки используемые при передаче видео данных поверх IP

Все форматы сжатия семейства MPEG (MPEG 1, MPEG 2, MPEG 4, MPEG 7) используют высокую избыточность информации в изображениях, разделенных малым интервалом времени. Между двумя соседними кадрами обычно изменяется только малая часть сцены – например, происходит плавное смещение небольшого объекта на фоне фиксированного заднего плана. В этом случае полная информация о сцене сохраняется выборочно – только для опорных изображений. Для остальных кадров достаточно передавать разностную информацию: о положении объекта, направлении и величине его смещения, о новых элементах фона, открывающихся за объектом по мере его движения. Причем эти разности можно формировать не только по сравнению с предыдущими изображениями, но и с последующими

(поскольку именно в них по мере движения объекта открывается ранее скрытая часть фона).

Форматы сжатия семейства MPEG сокращают объем информации следующим образом:

- устраняется временная избыточность видео (учитывается только разностная информация);
- устраняется пространственная избыточность изображений путем подавления мелких деталей сцены;
- устраняется часть информации о цветности;
- повышается информационная плотность результирующего цифрового потока путем выбора оптимального математического кода для его описания.

Форматы сжатия MPEG сжимают только опорные кадры – I-кадры (Intra frame – внутренний кадр). В промежутки между ними включаются кадры, содержащие только изменения между двумя соседними I-кадрами – P-кадры (Predicted frame – прогнозируемый кадр). Для того чтобы сократить потери информации между I-кадром и P-кадром, вводятся так называемые B-кадры (Bidirectional frame – двунаправленный кадр). В них содержится информация, которая берется из предшествующего и последующего кадров. При кодировании в форматах сжатия MPEG формируется цепочка кадров разных типов. Типичная последовательность кадров выглядит следующим образом: IBVRVBIVRVBIVB... Соответственно, последовательность кадров в соответствии с их номерами будет воспроизводиться в следующем порядке: 1423765...

**Форматы сжатия видео изображения MPEG 1 и MPEG 2.** В качестве начального шага обработки изображения форматы сжатия MPEG 1 и MPEG 2 разбивают опорные кадры на несколько равных блоков, над которыми затем производится дискретное косинусное преобразование (DCT). По сравнению с MPEG 1, формат сжатия MPEG 2 обеспечивает лучшее разрешение изображения при более высокой скорости передачи видео данных за счет

использования новых алгоритмов сжатия и удаления избыточной информации, а также кодирования выходного потока данных. Также формат сжатия MPEG 2 дает возможность выбора уровня сжатия за счет точности квантования. Для видео с разрешением 352x288 пикселей формат сжатия MPEG 1 обеспечивает скорость передачи 1,2 – 3 Мбит/с, а MPEG 2 – до 4 Мбит/с.

По сравнению с MPEG 1, формат сжатия MPEG 2 обладает следующими преимуществами:

- как и JPEG2000, формат сжатия MPEG 2 обеспечивает масштабируемость различных уровней качества изображения в одном видеопотоке;

- формате сжатия MPEG 2 точность векторов движения увеличена до 1/2 пикселя;

- пользователь может выбрать произвольную точность дискретного косинусного преобразования;

- в формат сжатия MPEG 2 включены дополнительные режимы прогнозирования.

Формат сжатия MPEG 2 использовал снятый сейчас с производства видеосервер AXIS 250S компании AXIS Communications, 16-канальный видеонакопитель VR-716 компании JVC Professional, видеорегистраторы компании FAST Video Security и многие другие устройства системы видеонаблюдения.

**Формат сжатия MPEG 4.** MPEG4 использует технологию так называемого фрактального сжатия изображений. Фрактальное (контурно-основанное) сжатие подразумевает выделение из изображения контуров и текстур объектов. Контурные представляются в виде сплайнов (полиномиальных функций) и кодируются опорными точками. Текстуры могут быть представлены в качестве коэффициентов пространственного частотного преобразования (например, дискретного косинусного или вейвлет-преобразования).

Диапазон скоростей передачи данных, который поддерживает формат сжатия видео изображений MPEG 4, гораздо шире, чем в MPEG 1 и MPEG 2. Дальнейшие разработки специалистов направлены на полную замену методов обработки, используемых форматом MPEG 2. Формат сжатия видео изображений MPEG 4 поддерживает широкий набор стандартов и значений скорости передачи данных (табл.2.1).

Таблица 2.1. Сравнительные характеристики стандартов сжатия видео

Свойства	MPEG-1	MPEG-2	MPEG-4 / ASP	MPEG-4 / AVC (H.264)
Максимальный размер блока	16x16	16x16 (режим фрейма), 16x8 (режим поля)	16x16	16x16
Размер блоков	8x8	8x8	16x16, 8x8, 16x8	8x8, 8x16, 16x8, 16x16, 4x8, 8x4, 4x4
Преобразования	DCT	DCT	DCT / преобразование Вейвлета	Точное целочисленное преобразование пространственных блоков 4x4
Размер блока преобразования	8x8	8x8	8x8	4x4
Профили	Нет	5 профилей с несколькими уровнями в каждом из профилей	8 профилей с несколькими уровнями в каждом из профилей	3 профиля с несколькими уровнями в каждом из профилей
Типы кадров	I, P, B, D	I, P, B	I, P, B	I, P, B, SI, SP
Скорость передачи	До 1,5 Мбит/с	2 – 15 Мбит/с	64 Кбит/с – 2 Мбит/с	64 Кбит/с – 150 Мбит/с
Сложность шифрования	Низкая	Средняя	Средняя	Высокая
Совместимость с предыдущими стандартами	Да	Да	Да	Нет

MPEG 4 включает в себя методы прогрессивного и чересстрочного сканирования и поддерживает произвольные значения пространственного разрешения и скорости передачи данных в диапазоне от 5 кбит/с до 10 Мбит/с. В MPEG 4 усовершенствован алгоритм сжатия, качество и эффективность которого повышены при всех поддерживаемых значениях скорости передачи данных. Разработка компании JVC Professional – веб-камера VN-V25U, входящая в линию сетевых устройств V.Networks, использует для обработки видео изображений формат сжатия MPEG 4.

### 3. ПРОТОКОЛЫ, ИСПОЛЬЗУЕМЫЕ В IPTV

Поддержка разнообразных данных и мультимедиа приложений через общую инфраструктуру, вероятно, является основным достижением конвергированных сетей. Только верхние уровни (третий или четвертый) протоколов предназначены для определенных приложений. Таким протоколом является IGMP, который предназначен для поддержки переключения каналов и управления мультикаст-потоками, или RTSP, обеспечивающий функции VCR (также как: воспроизведение / пауза / перемотка-вперед/назад), который специально предназначен для приложений VoD. Эти протоколы используются для предоставления услуг IPTV. Кроме этих, также используются:

- UDP – для передачи потокового видео;
- HTTP – для организации интерактивных сервисов (таких как пользовательские меню, электронная программа передач и пр.);
- RTP – для передачи потокового видео;
- RTCP – отвечает за проверку идентичности отправленных и полученных пакетов, идентифицирует отправителя и контролирует загруженность сети.

### 3.1. Транспортные протоколы UDP, RTP

UDP (англ. *Use rDatagram Protocol* — протокол пользовательских датаграмм, описан в RFC-768) является одним из основных протоколов, расположенных непосредственно над IP. Он предоставляет прикладным процессам транспортные услуги, немногим отличающиеся от услуг протокола IP. Протокол UDP обеспечивает доставку дейтограмм, но не требует подтверждения их получения. Протокол UDP не требует соединения с удаленным модулем UDP ("бессвязный" протокол). К заголовку IP-пакета UDP добавляет поля порт отправителя и порт получателя, которые обеспечивают мультиплексирование информации между различными прикладными процессами, а также поля длина UDP-дейтограммы и контрольная сумма, позволяющие поддерживать целостность данных. Таким образом, если на уровне IP для определения места доставки пакета используется адрес, на уровне UDP - номер порта.

Хотя протокол UDP не гарантирует доставки, по умолчанию предполагается, что вероятность потери пакета достаточно мала.

Прикладные процессы и модули UDP взаимодействуют через UDP-порты. Эти порты нумеруются, начиная с нуля. Прикладной процесс, предоставляющий некоторые услуги (сервер), ожидает сообщений, направленных в порт, специально выделенный для этих услуг. Программа-сервер ждет, когда какая-нибудь программа-клиент запросит услугу.

Протокол RTP. В Интернет, также как и в некоторых других сетях, возможна потеря пакетов изменение их порядка в процессе транспортировки, а также вариация времени доставки в достаточно широких пределах. Мультимедийные приложения накладывают достаточно жесткие требования на транспортную среду. Для согласования таких требований с возможностями Интернет был разработан протокол RTP (англ. *Real-time Transport Protocol* - транспортный протокол реального времени). При этом определяется тип поля данных, производится нумерация посылок,

присвоение временных меток и мониторинг доставки. Приложения обычно используют RTP поверх протокола UDP для того, чтобы использовать его возможности мультиплексирования и контрольного суммирования. Но RTP может использоваться и поверх любой другой сетевой транспортной среды. RTP поддерживает одновременную доставку по многим адресам, если мультикастинг поддерживается нижележащим сетевым уровнем.

Следует иметь в виду, что сам по себе RTP не обеспечивает своевременной доставки и не предоставляет каких-либо гарантий уровня сервиса (QoS). Этот протокол не может гарантировать также корректного порядка доставки данных.

Правильный порядок выкладки информации может быть обеспечен принимающей стороной с помощью порядковых номеров пакетов. Такая возможность крайне важна практически всегда, но особое внимание этому уделяется при восстановлении передаваемого изображения.

На практике протокол RTP не отделим от протокола RTCP (RTP control protocol). Последний служит для мониторинга QoS и для передачи информации об участниках обмена в ходе сессии.

RTP гибкий протокол, который может доставить приложению нужную информацию, его функциональные модули не образуют отдельный слой, а чаще встраиваются в прикладную программу. Протокол RTP не является жестко регламентирующим.

RTP не имеет стандартного зарезервированного номера порта. Единственное ограничение состоит в том, что соединение проходит с использованием чётного номера, а следующий нечётный номер используется для связи по протоколу RTCP. Установление и разрыв соединения не входит в список возможностей RTP, такие действия выполняются сигнальным протоколом (например, RTSP).



## 3.2. Протоколы управления RTCP, RTSP

**RTSP** (англ. *Real Time Streaming Protocol* — потоковый протокол реального времени, описан в RFC-2326) предназначенным для использования в системах, работающих с мультимедиа данными, и позволяющим клиенту удалённо управлять потоком данных с сервера, предоставляя возможность выполнения команд, таких как «Старт», «Стоп», а также доступа по времени к файлам, расположенным на сервере.

RTSP не выполняет сжатие, а также не определяет метод инкапсуляции мультимедийных данных и транспортные протоколы. Передача потоковых данных сама по себе не является частью протокола RTSP. Большинство серверов RTSP используют для этого стандартный транспортный протокол реального времени (RTP), осуществляющий передачу аудио- и видеоданных.

Управляющий протокол RTCP (RTP control protocol) базируется на периодической передаче управляющих пакетов всем участникам сессии, используя тот же механизм рассылки, что и для пакетов данных. Этот протокол не имеет самостоятельного значения и используется лишь совместно с RTP. Нижележащий протокол должен обеспечивать мультиплексирование пакетов данных и управления, используя разные номера портов. RTCP выполняет четыре функции:

1. Главной задачей данного протокола является обеспечение обратной связи для контроля качества при рассылке данных. Обратная связь может быть непосредственно полезна при адаптивном кодировании, но эксперименты с IP мультикастингом показали, что для получателей крайне важно диагностировать ошибки при рассылке пакетов. Посылка сообщений-отчетов о приеме данных всем участникам позволяет тому, кто обнаружил какие-то проблемы, разобраться в том, являются ли эти трудности локальными или глобальными. При механизме рассылки типа IP-мультикастинга, сервис провайдер, который непосредственно не вовлечен

в сессию, получив обратную связь, может независимо мониторить ситуацию в сети.

2. RTCP имеет постоянный идентификатор транспортного уровня для RTP источника, который называется каноническим именем или спаме. Так как SSRC-идентификатор может быть изменен, если будет зафиксировано столкновение или источник будет вынужден рестартовать, получатели нуждаются в спаме, для того чтобы отслеживать каждого из участников. Получателям также нужно спаме, чтобы установить соответствие между многими потоками данных от одного участника при реализации нескольких сессий одновременно, например, чтобы синхронизовать аудио- и видео-каналы.

3. Первые две функции требуют, чтобы все участники посылали RTCP-пакеты, следовательно скорость передачи должна контролироваться для того, чтобы RTP мог работать с большим числом участников. При отправке каждым участником своих управляющих пакетов всем остальным любой партнер может независимо определить полное число участников сессии. Это число используется при вычислении частоты отправки пакетов.

4. Четвертая опционная функция служит для передачи минимальной управляющей информации, например идентификаторов участников, для графического интерфейса пользователя. Это полезно для "слабо управляемых" сессий, когда участники входят и выходят без должного контроля и без согласования параметров. RTCP выполняет функции удобного канала для контакта со всеми участниками, но он необязательно поддерживает все коммуникационные требования приложения.

Функции 1-3 являются обязательными, когда RTP используется в среде с IP мультикастингом, и рекомендательными для всех остальных сред. Разработчикам приложений RTP рекомендуется избегать механизмов, которые могут работать только в уникальном режиме.

### 3.3. Протоколы IGMP, HTTP

**IGMP** (англ. *Internet Group Management Protocol* — протокол управления группами Интернета) - протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP. IGMP используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы.

Этот протокол является частью спецификации групповой передачи пакетов в IP-сетях. IGMP расположен выше сетевого уровня, хотя, по сути, действует не как транспортный протокол. IGMP может использоваться для поддержки потокового видео и онлайн-игр, для этих типов приложений он позволяет использовать сетевые ресурсы более эффективно.

IGMP используется только в сетях IPv4, так как в IPv6 групповая передача пакетов реализована по-другому.

Сеть, предоставляющая услуги групповой передачи данных (например, видео) с использованием IGMP, может иметь следующую базовую архитектуру (рис. 3.1):

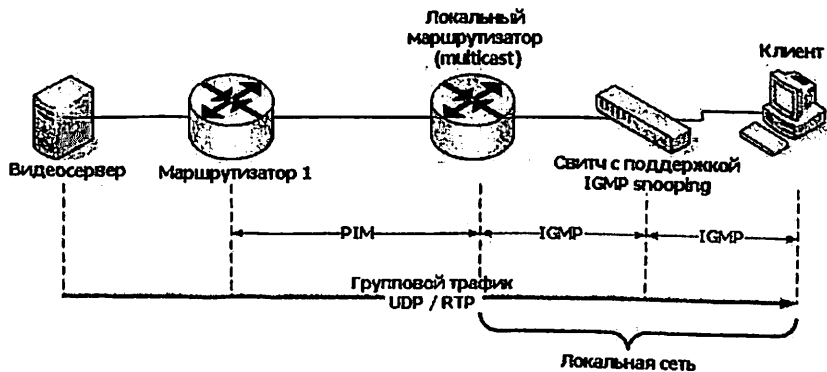


Рис. 3.1. Базовая архитектура сети, с использованием IGMP

IGMP используется клиентским компьютером и соседними коммутаторами для соединения клиента и локального маршрутизатора, осуществляющего групповую передачу. Далее между локальным и удаленным маршрутизаторами используется протокол PIM (Protocol Independent Multicast), с его помощью групповой трафик направляется от видеосервера к многочисленным клиентам групповой передачи.

HTTP (англ. *Hyper Text Transfer Protocol* — протокол передачи гипертекста) — протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов). Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом. HTTP в настоящее время повсеместно используется сети Internet для получения информации с веб-сайтов.

#### 4. СТРУКТУРА IPTV

IPTV (Internet Protocol Television) - цифровое интерактивное телевидение в сетях передачи данных по протоколу IP. Не следует путать IPTV с Internet-TV.

IPTV не означает телевидение, вещающее в Интернете. IPTV - это закрытая или полужакрытая сеть, полностью принадлежащая оператору связи, со своей топологией и инфраструктурой. Таким образом IPTV это всего лишь один из способов доставки видео до пользователя на основе IP-сети.

Разработка сетевого и терминального оборудования IPTV определена в утвержденной рекомендации ITU-T Y.1910

"Функциональная архитектура IPTV". Данная рекомендация позволит поставщикам услуг предлагать весь спектр услуг IPTV на базе сетей NGN.

#### 4.1. Услуги IPTV

Интерактивное телевидение IPTV является наиболее сложным и интересным из всех новых видах вещания. Оно предоставляет телезрителю самые невероятные возможности активного участия в телепередачах — от ответов на вопросы в режиме онлайн до участия в шоу с помощью своего виртуального образа. Характерной особенностью цифрового IPTV является, наряду с предоставлением абоненту интерактивного видеоконтента, высокое качество изображения (т. е. телевидение высокой четкости - HDTV) и дополнительные услуги для зрителя, позволяющие ему через обратный канал связи активно взаимодействовать с системой IPTV и оказывать влияние на то, что происходит на экране. Функции интерактивности реализуются с помощью пульта дистанционного управления или интерактивной клавиатуры через клиентский терминал STB.

Особенность интерактивного телевидения состоит в возможности его персонализации: из всего обширного спектра телепрограмм и телеуслуг пользователь может сформировать собственный пакет в соответствии со своими предпочтениями.

В систему IPTV могут входить как обычные каналы, так и каналы расширенного телевидения с интерактивным контентом и различные вариации услуг «видео по запросу» VOD (Video-on-Demand). VOD предоставляет возможность просмотра заказанных программ в определенное время, позволяет заказать фильмы с пульта управления и включает основные функции видеоманитюфона: пуск, паузу и перемотку.

Известные услуги IPTV можно разделить на 3 большие группы:

1. Телевизионные сервисы и PVR сервисы;

2. Услуги VOD;

3. Интерактивные сервисы.

К первой группе относятся такие услуги как: BTV, EPG, SO, NPVR, PLTV, Instant PVR, TSTV. Они включают в себя как классическую услугу вещания телевизионных каналов, так и реализуемые только в IPTV услуги записи и повторного просмотра понравившейся телепередачи. Рассмотрим данные услуги подробнее.

**BTV** - Broadcast Television – вещание телевизионных каналов по IP сети. Как правило, способом оплаты является абонентская плата за пакет телеканалов или в более широкой версии за канал. Пользователь имеет возможность переподписки на пакеты каналов.

**EPG** – Electronic Program Guide – электронная программа передач. Предоставляется без оплаты, т.к. является основным инструментом информирования пользователя о будущих программах и для использования PVR сервисов.

**NPVR** – Network Personal Video Recorder – сетевой видеомэгнитофон – заказ «записи» будущих программ через EPG. Заказ каждой программы оплачивается отдельно. Пользователь может просматривать «записанную» программу в течение определенного времени (например, 24 или 72 часа) неограниченное количество раз.

**SO** – Start Over – перезапуск программ – возможность просмотра текущей телепередачи сначала. Отсутствие возможности прокрутки.

**PLTV** – Pause Live TV - пауза прямого эфира. Абонент в любое время прямой трансляции может нажать кнопку — pause на ПДУ. После паузы, нажав кнопку —play, можно продолжить просмотр с места остановки.

**Instant PVR** – реализация записи не через заказ по EPG, а по нажатию абонентом кнопки —record на ПДУ в режиме полноэкранного просмотра. В результате осуществляется запись временного интервала между нажатиями кнопок —record и —stop.

*TSTV* – Time-shift TV – телевидение со сдвигом во времени. Это наиболее широкая реализация всех —PVR-based сервисов. *TSTV* позволяет в любой момент времени нажать на «прямой трансляции» кнопку —rewind и перемотать телеканал на любое время назад (10 минут, час, день, и т.д.).

К услугам «Видео по требованию» можно отнести: VoD, SVoD, NVoD.

Базовой услугой является VOD – Video on Demand – Видео по запросу. Пользователь может выбрать любой фильм, имеющийся в видеотеке и купить его на определенный период времени. Возможна вариация цены в зависимости от срока аренды (например, 6/12/24 часа), также на стоимость фильма влияет категория, в которой он находится. Например, новинки стоят дороже, чем фильмы из раздела «классика». Пользователь перед покупкой может бесплатно просмотреть трейлер к понравившемуся фильму.

*SVoD* – Subscription Video on Demand – видео по запросу по подписке. Позволяет оплатить абоненту неограниченный доступ к определенной категории VoD контента. При покупке фильма из этой категории будут обходиться дешевле. Форма оплаты также как и для VOD осуществляется за заказ с вариацией цены в зависимости от срока аренды (например, 6/12/24 часа). Бесплатный просмотр трейлеров.

*NVoD* – Near Video on Demand – виртуальный кинозал, трансляция видеоконтента по расписанию в широкоэвещательном режиме (multicast). Эта услуга больше интересна оператору, нежели пользователю, т.к. позволяет экономить ресурс сети, за счет использования режима multicast. Как и в двух предыдущих случаях оплата происходит за заказ. Стоимость назначается в зависимости от категории фильма и периода аренды. Возможен бесплатный просмотр трейлеров.

К третьей группе услуг относятся те сервисы, которые интегрируются извне и могут являться частной разработкой оператора связи, например, игры на базе технологии Java (морской бой, крестики-нолики), интеграция с сервисом IP-телефонии, работа с электронной почтой на экране ТВ, интеграция с интернет-пейджером ICQ, информационно-справочные и

коммерческие сервисы: погода, курс валют, новости. Таким образом, используя, IPTV пользователи могут заключать виртуальные пари, посещать телемагазины, голосовать на местных референдумах, участвовать в форумах и чатах, отправлять SMS-сообщения, хранить персональную информацию в электронных адресных книгах и календарях, создавать семейные фотоальбомы и т. п.

Важнейшую роль в системах IPTV играет свойство интерактивности, которое позволяет зрителю при просмотре телевизионных программ запрашивать с помощью пульта управления через STB и получать на экране дополнительные сведения: информацию о программе, ее авторах и участниках, анонсы будущих передач, материалы по той же теме, не вошедшие в основную телепрограмму. Пользователь имеет доступ к архиву прошлых выпусков программы и т. п.

## 4.2. Архитектура IPTV

На сегодняшний день на рынке телекоммуникаций ведущими компаниями производителями и разработчиками оборудования и ПО представлен ряд решений IPTV, отвечающий всем заявленным требованиям со стороны операторов телекоммуникации.

Несмотря на многообразие предлагаемых решений можно однозначно выделить ряд компонентов, составляющих типовой комплекс IPTV.

Основными компонентами комплекса IPTV являются:

- головная станция (Head End) и узел кодирования;
- подсистема Видео по требованию (Video on Demand);
- сервисная платформа (Middleware);
- абонентское оборудование (Set-Top-Box);
- подсистема условного доступа (Conditional Assess System).

Сеть телекоммуникации можно построить разными способами, базовые требования можно сформулировать следующим образом:



- достаточная полоса пропускания — это от 4 Mbps для MPEG2 и от 2,5 Mbps для MPEG4, для получения приемлемого качества изображения на среднестатистическом телевизоре;

- поддержка Multicast во всей сети, обязательное условие для реализации услуг IPTV;

- сквозная поддержка механизмов QoS. Для расчета ресурсов полосы пропускания. Если используется достаточная полоса пропускания, услуга работает, но необходимо учитывать приоритетный трафик.

**Головная станция и узел кодирования.** Для удобства головная станция и узел кодирования территориально находятся на одной площадке и осуществляют прием, преобразование сигналов от различных источников и формирование потоков IP-multicast / IP-unicast.

Оборудование захвата контента в реальном времени получает аудиовизуальные потоки от различных источников при помощи спутниковых антенн, частотных и т.д. При необходимости шифрует, декодирует, оцифровывает и направляет их в оборудование упаковки в пакеты IP - IP Streamer.

**Компоненты Головной станции:**

- антенный пост – обеспечивает прием сигналов от эфирных станций и спутников;

- цифровые спутниковые приемники – дескрипторы – обеспечивают раскодирование цифровых сигналов, полученных с Антенного поста и передачу материалов стримеру / мультиплексу;

- узел цифрового кодирования – обеспечивает MPEG-кодирование аналоговых и цифровых сигналов и передачу материалов стримеру / мультиплексу;

- стример / мультиплексор - ключевой элемент Головной станции, обеспечивает мультиплексирование материалов и IP-вещание таким образом, что каждый канал имеет свой уникальный адрес и порт IP вещания.

Для качественного приема сигнала во всем частотном диапазоне 47-826 МГц в точке приема устанавливается несколько эфирных антенн (каждая для своего диапазона). Далее сигналы с этих антенн суммируются, и затем групповой аналоговый сигнал через систему активных сплиттеров поступает на входы профессиональных эфирных приемников. С выходов приемников аналоговый видеосигнал в формате цветового кодирования SECAM подается на транскодер для преобразования его в SDI.

Таким образом, на кодеры сжатия подается сигнал в формате SDI и аналоговые аудио сигналы (отдельно каналы левый и правый). Кодеры служат для компрессии сигналов по стандарту MPEG-2 и MPEG-4. С выхода каждого кодера транспортные видео потоки поступают на коммутаторы, целью которых является суммирование трафика от кодеров и перенаправление его в сеть оператора. На данном рисунке представлена конкретная техническая реализация узла кодирования. В зависимости от требований оператора и возможностей сети, сигнал может сразу приниматься в цифровом виде или, например, в формате PAL, а не SECAM.

Подсистема видео по требованию. В задачу подсистемы VOD входит запись и проигрывание по запросу пользователя видеоматериалов.

Основными компонентами системы VOD являются:

- центральный узел – аппаратно-программный комплекс, расположенный, как правило, в «центре» сети в непосредственной логической близости к системе условного доступа и головной станции;
- система управления контентом – программное обеспечение, управляющее видеосерверами и распределением контента;
- видеосервер – аппаратно-программный комплекс, устанавливаемый для обслуживания групп пользователей на определенной территории, например, в пределах одного узла агрегации.

Зашифрованный системой предварительного кодирования VOD контент и метаданные поступают на узел и хранятся в системе хранения.

*Метаданные* — одна из существенных составляющих цифрового телевидения. В системах IPTV по требованию абонента ему может быть предоставлено развернутое описание программы или фильма, трейлер, постер причем в любой момент, в том числе и задолго до ее "выхода в эфир".

С помощью системы управления контентом осуществляется распределение контента на видеосерверы в соответствии с заданными правилами. При поступлении пользовательского запроса на вещание контента, после процедур аутентификации CAS, middleware получает от системы управления контентом ссылку на ближайшие свободные видеосерверы, имеющие в своей базе необходимый пользователю контент. Таким образом, в ядре сети минимизируется unicast трафик, т.к. большая часть вещания «видео-по-запросу» осуществляется с ближайшего к пользователю локального видеосервера. В ядре сети циркулирует служебный трафик и трафик распределения видеоконтента между центральным узлом и видеосерверами, который пренебрежимо мал и не предъявляет существенных требований к сети.

Центральный узел служит, в основном, для получения контента и распределения его по периферийным серверам, а также обработки запросов пользователей в случае недостаточности функционала периферийных видеосерверов. На первом этапе развития услуг «Видео-по-запросу» возможно использовать центральный узел для предоставления услуг пользователям. В дальнейшем, при росте абонентской базы, необходимо устанавливать видеосерверы на узлах агрегации.

На рис. 4.1 представлена система видеосерверов VOD.

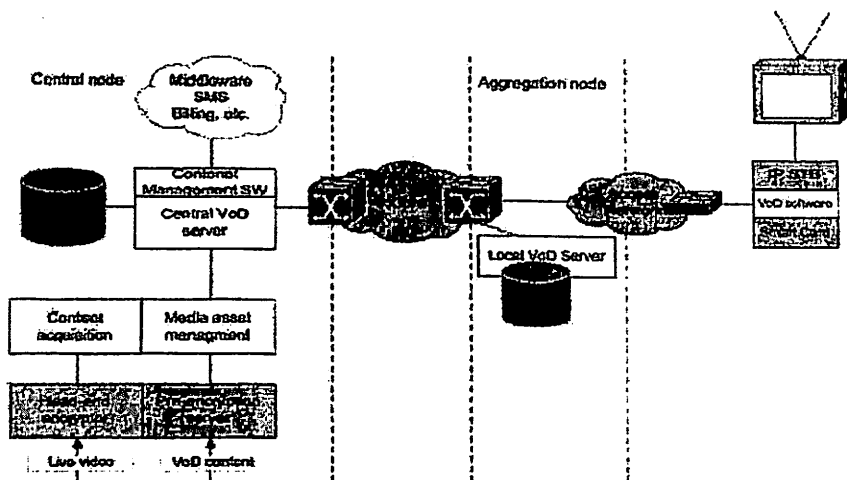


Рис. 4.1 – Система видеосерверов VOD.

**Сервисная платформа Middleware.** Middleware – программно-аппаратный комплекс, который обеспечивает управление всеми компонентами решения IPTV, а также служит для упрощения задач администрирования и управления предоставляемыми услугами. Middleware позволяет осуществлять:

- авторизацию абонента;
- формирование программы передач EPG;
- формирование интерфейса и инструментов управления решением IPTV;
- взаимодействие с системами CAS, VoD, головной станцией, STB-устройствами;
- взаимодействие с биллинговыми системами и системами поддержки бизнеса оператора связи.

Middleware имеет открытую архитектуру, что позволяет оперативно

масштабировать компоненты решения и расширять спектр услуг. На рис. 4.2 представлена аппаратная архитектура Middleware для инсталляции без резервирования.

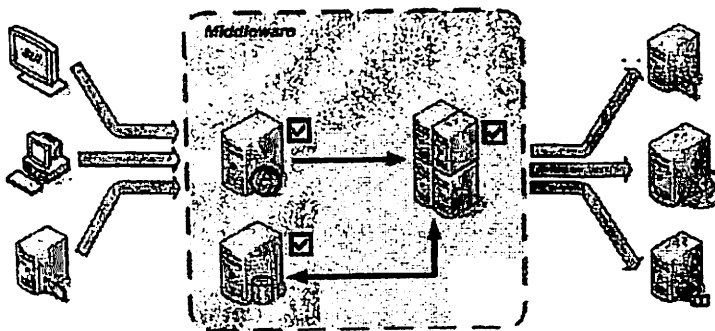


Рис. 4.2. Аппаратная архитектура Middleware

В данной конфигурации для работы необходимо три сервера. Все сервера устанавливаются в одном серверном шасси. Middleware является единственной входной точкой в систему IPTV, через него осуществляется взаимодействия как со всеми компонентами системы (VoD, CAS и т.д.), так, и, с внешними компонентами и системами (биллинговые системы, рабочая станция администратора и т.д.).

Middleware состоит из шлюза доступа, который организует доступ к серверам приложений из публичной сети в частную сеть, где и находится Middleware. Сервера приложений обрабатывают все запросы, производят расчеты, запрашивают другие информационные системы. Вся информация о пользователях, истории их запросов хранятся в базе данных.

**Абонентские устройства.** *STB* (Set-top-Box) - абонентское устройство, является связующим звеном между системами формирования, доставки аудио - и видеоматериалов, и телевизором абонента. *STB* – это миникомпьютер с операционной системой, web-браузером, MPEG

декодером. Устройство должно быть интегрировано под конкретный проект, для взаимодействия со всеми компонентами системы.

**Подсистема условного доступа (Conditional Access System).** Система условного доступа - техническое средство защиты аудиовизуальных и других сообщений и материалов, распространяемых в составе ТВ программы по эфирным, кабельным и спутниковым сетям связи. Также CAS позволяет разграничивать доступ пользователя к мультимедийным услугам, соблюдать авторские права, обеспечивать защиту контента от несанкционированного доступа/копирования.

Вещательный контент (телевизионные каналы) с головной станции в режиме multicast доступен в открытом виде в служебном VLAN. Серверы шифрования вещательных каналов подписываются на мультикастовые группы открытых каналов и шифруют их на уровне MPEG.

Результатом шифрования канала является новая мультикастовая группа в публичной сети. Абонентские STB получают ключи на каналы, на которые они подписаны при загрузке и периодически обновляются. При переключении каналов обращения за ключами не происходит, что ускоряет данный процесс.

Шифрование контента Видео по запросу (VOD) отличается от шифрования вещательного контента. Каждый видеофайл предварительно шифруется системой условного доступа и через систему дистрибуции попадает на видеосерверы. В дальнейшем, при просмотре контента, происходит обращение STB к CAS за получением ключа, которым был закодирован данный контент.

#### 4.3. Режимы передачи трафика и протоколы в IP-сетях:

Для предоставления услуг IPTV используют следующие режимы передачи трафика: multicast – при трансляции телевизионных каналов, и unicast – при предоставлении услуги VOD.

Рассмотрим указанные режимы более подробно.

Unicast трафик (одноцелевая передача пакетов) используется прежде всего для сервисов «персонального» характера. Каждый абонент может запросить персональный видео-контент в произвольное, удобное ему время. Unicast трафик направляется из одного источника к одному IP-адресу назначения (рис.4.3).

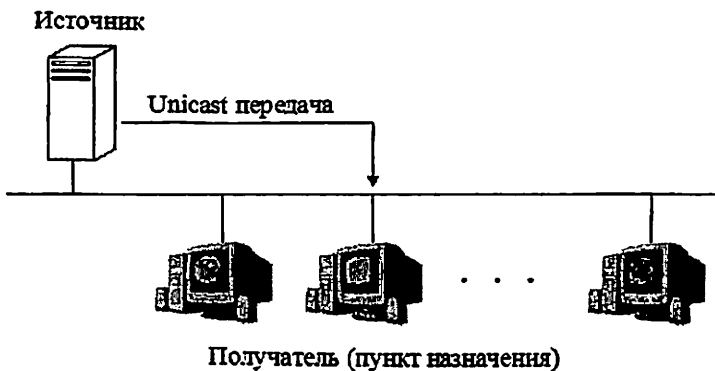


Рис. 4.3. Unicast доставка видео

Этот адрес принадлежит в сети только одному единственному компьютеру или абонентскому терминальному устройству Set-Top-Box (STB). Число абонентов, которые могут получать unicast трафик одновременно, ограничено доступной в магистральной части сети шириной потока (скоростью потока). Для случая сетевой технологии Gigabit Ethernet теоретическая максимальная ширина потока данных может приближаться к 1 Гб/сек за вычетом полосы, необходимой для передачи служебной

информации и технологических запасов оборудования. Предположим, что в магистральной части сети мы можем для примера выделить не более половины полосы для сервисов, которым требуется unicast трафик. Легко подсчитать для случая 5Мб/сек на телевизионный канал MPEG2, что число одновременно получающих unicast трафик абонентов не может превышать 100.

**Multicast** трафик (групповая передача пакетов) используется для передачи потокового видео, когда необходимо доставить видео-контент неограниченному числу абонентов, не перегружая сеть (рис. 4.4). Это наиболее часто используемый тип передачи данных в IP-TV сетях, когда одну и ту же программу смотрят большое число абонентов. Multicast трафик использует специальный класс IP-адресов назначения, например адреса в диапазоне 224.0.0.0 ... 239.255.255.255.

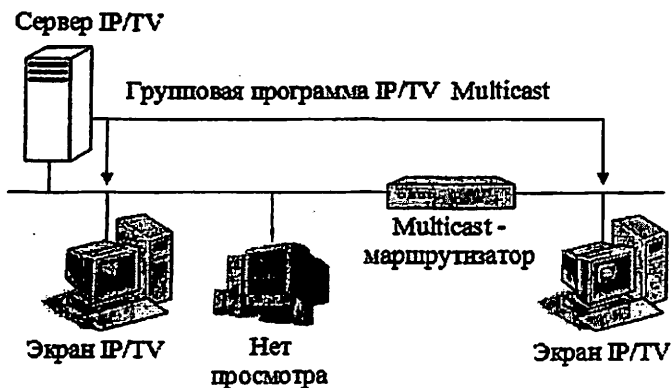


Рис. 4.4. Multicast доставка видео

В отличие от unicast трафика, multicast адреса не могут быть назначены индивидуальным компьютерам (или STB). Когда данные посылаются по одному из multicast IP-адресов, потенциальный приемник данных может принять решение принимать или не принимать их, то есть будет абонент



смотреть этот канал или нет. Такой способ передачи означает, что головное оборудование IP-TV оператора будет передавать один единственный поток данных по многим адресам назначения. В отличие от случая broadcast передачи, за абонентом остается выбор - принимать данные или нет.

Broadcast трафик (широковещательная передача пакетов) использует специальный IP-адрес, чтобы посылать один и тот же поток данных ко всем абонентам данной IP-сети (рис. 4.5). Например, такой IP-адрес может оканчиваться на 255, например 192.0.2.255, или иметь 255 во всех четырех полях (255.255.255.255). Важно знать, что broadcast трафик принимается всеми включенными компьютерами (или STB) в сети независимо от желания пользователя. По этой причине этот вид передачи используется в основном для служебной информации сетевого уровня или для передачи другой исключительно узкополосной информации. Разумеется, для передачи видеоданных broadcast трафик не используется.

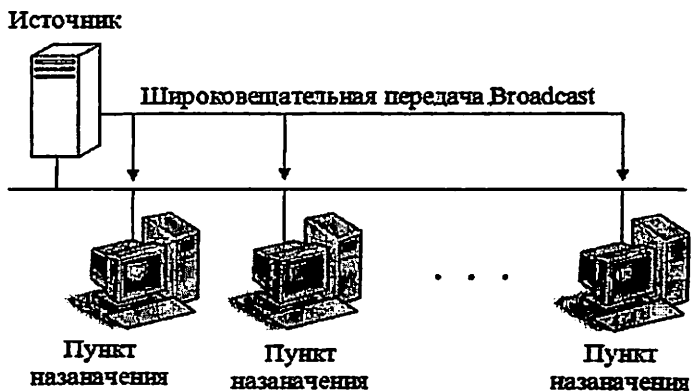


Рис 4.5. Broadcast доставка видео

#### 4.4. Достоинства и недостатки IPTV

Главное преимущество IPTV - это дополнительные услуги, новые и зачастую уникальные возможности, предоставляемые операторами наряду с телевещанием. Если до определенного времени, помимо ТВ, на экран по большей части выводился только телетекст, то технология IPTV позволила кардинально изменить ситуацию с предложением дополнительных интерактивных возможностей, используемые только в пакетных сетях. Кроме того, передача теле и видеoinформации по IP-каналам обладает и рядом явных технологических преимуществ перед кабельным телевещанием. Во-первых, за счет того, что решение IPTV имеет двунаправленную архитектуру, становится возможной не только передача контента абонентскому устройству, но и получение потоков информации от него. Это дает возможность оператору создавать различные интерактивные услуги, например, поддерживать двустороннее интерактивное соединение удаленных видео и аудиостудий. Также, абонентские устройства могут обеспечивать передачу и получение фактически любого контента, от Web-страниц и электронных сообщений до видеоконференций и чата. Наконец, IPTV в отличие от кабельного телевидения можно использовать в существующих IP-сетях, что обеспечивает возможность введения дополнительных сервисов без организации новой инфраструктуры. Использование существующих сетей позволяет снизить срок их окупаемости и не требует крупных издержек на организацию новых сетей для предоставления сервиса IPTV.

Однако видеосигнал, передаваемый по сети IP, весьма чувствителен к потерям пакетов данных, так как чаще всего передается в сильно сжатом виде с использованием механизмов кодирования MPEG-2 и MPEG-4. По причине того, что эти видеокодеки не восстанавливаются при пакетных потерях на сетевом уровне, потеря даже единственного пакета IP-инкапсулированного видео может привести к заметному ухудшению качества видеонизображения. По этой причине на данный момент уделяется

очень большое внимание вопросам обеспечения качества обслуживания в сетях IPTV.

## 5. СТАНДАРТИЗАЦИЯ IPTV

Процесс стандартизации IPTV крайне сложен. Технология IPTV — это комплекс, охватывающий целый ряд областей и использующий среду, изначально не предназначенную для передачи аудио и видео. Тем не менее, некоторые особенности этой среды позволяют предоставлять на ее базе более современные варианты услуг, нежели в сетях вещания.

Комплексных стандартизированных решений для доставки мультимедийных потоков информации на данный момент не существует. Некоторые аспекты работы таких систем были изучены и стандартизированы, но со многими вопросами ни вещатели, поставляющие контент, ни операторы связи, доставляющие его конечному пользователю, еще не сталкивались, и они требуют решения. В этом материале рассмотрен комплекс работ по стандартизации технологии, необходимый для успешного развития рынка IPTV.

В стандартизации IPTV участвуют следующие организации:

- Alliance for Telecommunications Industry Solutions IPTV Interoperability Forum (ATIS IIF)
- International Telecommunication Union (ITU);
- Internet Streaming Media Alliance (ISMA);
- Open IPTV Forum (OIPF);
- European Telecommunication Standards Institute (ETSI);
- Internet Engineering Task Force (IETF);
- DSL Forum (DSLForum);
- MPEG Industry Forum;
- Consumer Electronics Association (CEA);
- Digital Living Network Alliance (DLNA);

- TeleManagement Forum (TMF);

- DVB.

В таблице 5.1 представлена деятельность организаций по стандартизации IPTV:

Таблица 5.1. Деятельность организаций по стандартизации IPTV

Организа ция	Деятельность
ATIS IIF	<p>Создан 23 июня 2005 года;</p> <p>Комитеты: Architecture, IPTV Security Solutions, Metadata, QoS Metrics, Testing and Interoperability;</p> <p>Участники (около 50): IneoQuest Technologies, Sony Electronics, Verimatrix, Alcatel-Lucent, Thomson, Microsoft, Trandberg TV и др.</p>
ITU FG	<p>Была основана в апреле 2006 года.</p> <p>В апреле 2008 года выпустил документ: IPTV Focus Group Proceedings (более 700 страниц).</p> <p>Группы:</p> <ul style="list-style-type: none"><li>- WG-1: Архитектура и требования;</li><li>- WG-2: Качество обслуживания и вопросы производительности;</li><li>- WG-3: Безопасность услуг и защита контента;</li><li>- WG-4: Управление сетью IPTV;</li><li>- WG-5: Конечные системы и аспекты повторного использования;</li><li>- WG-6: Middleware, приложения и платформы контента.</li></ul> <p>Участники: около 140 компаний.</p>

<p>- ISMA</p>	<p>Создан в 2001 г.</p> <p>Последние документы датируются 2007 г.</p> <p>Направления:</p> <ul style="list-style-type: none"> <li>- кодеки (аудио, видео, медиа);</li> <li>- IP сети (протоколы, настройка и другие моменты);</li> <li>- оборудование и ПО;</li> <li>- полупроводниковые технологии и интегральные схемы;</li> <li>- контент (создание, выпуск, распространение и прочие аспекты);</li> <li>- системы вещания;</li> <li>- оборудование пользователя;</li> <li>- видео по запросу и врезка рекламы;</li> <li>- middleware и защита контента.</li> </ul>
<p>OIPF</p>	<p>Создан 20 марта 2007 года.</p> <p>В марте 2011 года выпустили документ: Open IPTV Forum – Functional Architecture v 2.14</p> <p>Основатели: AT&amp;T, Ericsson, France Telecom, Panasonic, Philips, Samsung; Siemens, Sony и Telecom Italia;</p> <p>Основная задача: агрегировать уже существующие стандарты.</p>
<p>DSL Forum</p>	<p>Создан в 1998 г.</p> <p>Стандартизует:</p> <ul style="list-style-type: none"> <li>- широкополосный доступ – технологии ADSL2+ / VDSL2, объединение нескольких технологий DSL, решения PON;</li> <li>- управление многоадресной передачей данных и сетями VLAN – протокол IGMP и поддержка различных сетей VLAN;</li> <li>- управлением доступом к IPTV-услугам и управление качеством обслуживания – получение сведений в режиме реального времени о топологии сети, о доступной ширине полосы пропускания (ШПП), возможность динамического</li> </ul>

	<p>перераспределения ресурсов для обеспечения предоставления запрошенной IPTV-услуги, обеспечения требуемых ШПП и показателей QoS;</p> <ul style="list-style-type: none"> <li>- домашняя сеть – автоматическое распознавание и первичная настройка абонентского оборудования, удаленное управление и самодиагностика;</li> <li>- качество восприятия QoE – мониторинг и измерение показателей, определяющих качество восприятия IPTV-услуг пользователем.</li> </ul>
--	--

## **6. ОБЕСПЕЧЕНИЕ КАЧЕСТВА IPTV**

### **6.1. Показатели качества передачи видео**

Одна из самых больших технических проблем при переходе к передаче видео по сетям с пакетной коммутацией, заключается в обеспечении гарантированного качества обслуживания (Quality of Service, далее QoS), позволяющие получить звук и изображение без искажений и помех. Большинство существующих сетей с пакетной коммутацией построено для выполнения задач и приложений не особо чувствительных к задержке сигнала. Видео напротив очень требовательно к скорости передачи информации, и задержка пакета больше, чем на 200 мс, означает, что этот пакет уже не нужен, поскольку данные успели устареть. Следовательно, сети для передачи голоса и видео должны быть разработаны, построены и эксплуатироваться так, чтобы максимально увеличить эффективность прохождения пакетов в реальном времени.

Один канал телевизионной трансляции и видео по запросу (VOD) требует скорости передачи порядка 4 Мбит/с. Ситуация заметно улучшится, когда будет осуществлен полный переход на стандарт MPEG-4, но в любом

случае для получения качественного изображения для видео трафика нужно будет резервировать порядка 2 Мбит/с. Проблемы многократно возрастают, когда необходимо поддерживать качество передаваемого видео через глобальную сеть (WAN). Обычные скорости для локальных сетей (10, 100 Мбит/с и даже 1 Гбит/с) не используются при доступе к WAN ввиду высокой стоимости и потому, типичная скорость обращения к глобальной сети составляет около 1.45 Мбит/с и ниже создавая узкое место на границе LAN/WAN. Для электронной почты и других видов обмена данными это хоть и вызывает определенные задержки, но не является критичным. Для передачи голоса и видео необходимо резервировать часть полосы пропускания, иначе смысл получения услуг будет полностью утерян.

Качество обслуживания (QoS) является основным критерием для реализации услуг IPTV. Задача состоит в том, как гарантировать передачу пакетов при различном виде трафика при возможности без задержки или без выброса пакета благодаря вмешательству трафика с низким приоритетом. Основные параметры QoS через которые определяется качество услуг в IPTV:

- задержка доставки пакета. Этот параметр играет роль в основном при передаче голосовых и видео-сообщений;

- джиттер (разброс) – изменения в задержках при доставке пакета.

Оценка джиттера определена в следующих рекомендациях:

- IETF RFC 3550 RTP: A Transport Protocol for Real-Time Applications;

- IETF RFC 3611 RTP: Control Protocol Extended Reports (RTCP XR);

- потеря пакета - при перегрузке сеть вынуждена выбросить отдельные пакеты. Это один из тех параметров, который при передаче видео пакетов играет ощутимую роль.

Требования предъявляемые к качеству услуг IPTV определены в таблице 6.1.

Таблица 6.1. Требования к параметрам QoS при предоставлении услуг IPTV

Услуга	Кастинг	Макс. величина задержки	Макс. величина джиттера	Чувствительность к потерям
Потоковое видео	Multicast	-	50 мс	Да
Видео по запросу	Unicast	-	50 мс	Да
Доступа к ресурсам Интернета	Unicast	-	-	Нет
Аудио/видеотелефонная связь	Unicast	60 мс	20мс	Да

Из вышеприведенной таблицы видно что основными параметрами, к которым чувствительны услуги IPTV являются джиттер, потери пакетов и их задержка.

## 6.2. Методы оценки качества IPTV

В этой главе рассматриваются несколько субъективных методов оценки качества передачи видео, однако использование данных методов в процессе эксплуатации услуг IPTV не представляется возможным, в виду сложности проведения тестов (необходимость постоянно содержать группу экспертов).

Поэтому большую популярность в последнее время получили методы объективной оценки, которые основываются на сборе и анализе сетевых характеристик. В пособии дается краткая характеристика объективных и субъективных методов оценки, получивших в последнее время наибольшую популярность у операторов, предоставляющих услуги IPTV. Качество передачи видео зависит от различных факторов. Потери пакетов, сетевые задержки и джиттер определяются характеристиками сети



передачи. Тип кодека, техника маскировки ошибок, скорость кодирования, схема пакетизации и другие факторы, влияющие на качество передачи видео, зависят от типа приложения. Существующие методы оценки качества передачи видео принято разделять на субъективные и объективные методы.

### 6.2.1. Субъективные методы

До недавнего времени для видео приложений существовали только субъективные методы оценки качества услуг, которые в большей степени учитывают специфические факторы видео приложений, чем характеристики сети.

Субъективные методы позволяют в целом оценить услугу IPTV на этапе внедрения. В основе широко используемых методов субъективной оценки качества передачи видео лежит метод, основанный на субъективной оценке качества группой экспертов, известный как «Mean Opinion Score», MOS. Данный метод описан в Рекомендации ITU-T P.800, используемой для субъективной оценки качества передачи речи. Часть методов субъективной оценки видео описаны в Рекомендации ITU-R BT.500-11. Для методов субъективной оценки можно выделить три основных этапа тестирования:

- выбор или сочетание способов демонстрации видеопоследовательностей;
- определение методики сбора мнений экспертов;
- выбор методики обработки результатов.

Комбинации возможных методик в перечисленных этапах позволяют реализовывать различные методы субъективной оценки.

*MOS.* В соответствии с MOS качество передачи видео, получаемое при прохождении сигнала от источника через сеть связи к приемнику, оценивается как среднее арифметическое от всех оценок, выставяемых

экспертами после просмотра видео, переданного по тестируемому тракту передачи. Экспертные оценки определяются в соответствии со следующей пятибалльной шкалой: 5 – отлично; 4 – хорошо; 3 – приемлемо; 2 – плохо; 1 – неприемлемо. Очевидно, что данный метод не учитывает ряд явлений, типичных для сетей передачи данных и влияющих на качество передачи видео в системах IPTV. В методе, основанном на MOS, отсутствует возможность количественно учесть факторы, влияющие на качество видео, а именно не учитываются сквозная (end-to-end) задержка между источником видео и приемником, влияние вариации задержки и потери пакетов.

Также метод MOS не позволяет осуществлять контроль качества в реальном режиме времени, и, соответственно, своевременно реагировать на возможные проблемы в сети и предотвращать ухудшение качества услуг. Поэтому данный метод в основном применяют для первичной оценки сети при тестировании нового оборудования или новой услуги. Также этот метод является затратным, поскольку для получения достоверной оценки, необходимо пригласить группу экспертов, а это, как правило, 15-50 специалистов. С другой стороны на сегодня это один из наиболее точных методов оценки качества видео.

**PQR.** В рамках Рекомендации BT.500-11 вводятся дополнительные метрики для повышения точности оценки качества передачи видео группой экспертов.

Метрика PQR (Picture Quality Rating) позволяет определить способность пользователя «замечать» разницу между эталонным видео и тестируемым, в то время как MOS определяет шкалу экспертных оценок и позволяет выставлять их любому видео.

Методика PQR основывается на алгоритме JND [9] («just noticeable difference»), который стремится оценить восприятие зрительной системы человека. В ходе эксперимента, основанного на методе JND, сравниваются две видео последовательности: эталонное видео и тестируемое видео,

которое формируется искусственным добавлением ухудшающего воздействия на эталонное видео. Тестируемое видео можно представить следующим образом:

*видео тестируемое* = *видео эталонное* +  $k \cdot (\text{видео после ухудшения} - \text{видео эталонное})$ ,

где: видео эталонное - исходная видео последовательность;

видео после ухудшения - исходная видео последовательность, искаженная ухудшающим воздействием;

$k$  - коэффициент, который устанавливается в ходе эксперимента,  $0 < k < 1$ .

В ходе эксперимента зрителям показывают тестируемое и эталонное видео несколько раз при различных значениях  $k$  и просят определить, какое из просмотренных видео было подвержено ухудшающему воздействию. При низких значениях  $k$ , когда разница между тестируемым и эталонным видео небольшая, зрители в основном предполагают какая видео последовательность была показана. Правильные ответы составляют порядка 50 %. При увеличении  $k$  процент правильных ответов возрастает. Исследования реакции экспертов показали, когда зрители правильно идентифицируют тестируемую видеопоследовательность в 75 % случаев, разница между тестируемым и эталонным видео составляет 1 в оценках JND, если правильных ответов порядка 87 %, то разница между тестируемым и эталонным видео составляет 2 в оценках JND.

Поскольку человеческий глаз до определенного момента не воспринимает ухудшения качества видео, в ряде случаев эталонное видео оценивалось экспертами хуже, нежели тестируемое. Методика PQR преобразует воспринимаемую разницу между эталонным и тестируемым видео в значение, которое представляет способность зрителя «замечать» различия между видео последовательностями. Эксперименты, направленные на оценку чувствительности восприятия, измеряют способность зрителя замечать разницу в оценках JND. Данная методика

подходит для оценки услуги передачи видео на этапе её внедрения, когда реализуется выбор формата, стандарта кодирования, технологии передачи, осуществляется подбор экспертов для проведения тестов оценки качества видео. В то же время эта методика не приемлема для оценки качества передачи видео в процессе предоставления услуг IPTV, поскольку не позволяет в реальном масштабе времени контролировать качество передачи видео, доставляемого каждому пользователю услуги.

**DMOS.** Метрика DMOS (Difference Mean Opinion Score) вычисляет разницу между оценками MOS тестируемого и эталонного видео. В методике DMOS сравнивается пара видеопоследовательностей: эталонное и тестируемое видео (та же последовательность, подвергшаяся ухудшающему воздействию). Зрители сначала оценивают эталонную последовательность по пятибалльной шкале, а затем тестируемую в соответствии с методом MOS. Оценки MOS тестируемых 20 видео последовательностей вычитаются из оценок эталонных последовательностей MOS, что и определяет оценку DMOS.

Значения DMOS являются субъективными оценками качества изображения тестируемого видео относительно эталонного видео. Перед началом эксперимента группе экспертов показывают видео («тренировочная» последовательность) и предлагают оценить его качество. Последующие оценки экспертов будут ориентироваться на качество этой видео последовательности. Например, если в эксперименте участвуют две группы экспертов. Одной группе экспертов показывают тренировочное видео с хорошим качеством, другой группе - с худшим. Соответственно, оценки тестируемой последовательности также будут разными, таким образом, значения DMOS зависят от диапазона, в котором расположены оценки «лучшего случая» и «худшего случая» передачи тренировочной видеопоследовательности и носят относительный характер.

Метрика DMOS используется, когда разница между видео последовательностями не ожидаема, т.е. невозможно предсказать в какой момент и по какой причине произойдет ухудшение видео, или необходимо определить количественно эту разницу, в то время как PQR больше подходит для оценки способности зрителя заметить хоть какую-то разницу между исследуемыми видео последовательностями. Метрика DMOS носит относительный характер и не отражает процессы, происходящие в сети.

*SAMVIQ*. Метод SAMVIQ (Subjective Assessment Method for Video Quality evaluation) создан в EBU (European Broadcasting Union), реализация MSU Perceptual Video Quality tool и недавно был отправлен на стандартизацию. Этот метод используется для субъективного сравнения современных видеокодеков. Экспертам показывают сначала исходную видеопоследовательность, на качество которой они будут ориентироваться, для того, чтобы создать общую шкалу оценок, т.е. чтобы оценка «отлично» значила примерно одно и тоже у разных экспертов. В дальнейшем в ходе проведения теста экспертам показывают видео как с самым высоким качеством, так и с самым низким. Во время теста экспертам показывают видеопоследовательности, сжатые разными кодеками, причем человек не знает каким, именно, кодеком закодирована последовательность, для этого их обозначают буквами. Основная задача эксперта оценить демонстрируемое видео по шкале от 1 до 100. Эти оценки потом обрабатываются и усредняются. Оценка видео производится не автоматически, а человеком, на которого могут влиять внешние факторы, один из них это очередность показа видеопоследовательности, которую еще называют «эффектом памяти». При просмотре большого количества видео у эксперта стирается грань между качеством разных видеопоследовательностях. Эта проблема решается по разному, в некоторых методиках с каждым тестируемым видео показывают исходное. В методе SAMVIQ, во-первых, периодически в ходе проведения теста

демонстрируют исходную видеопоследовательность и, во-вторых, эксперту разрешено повторно просматривать видео и менять свои оценки. Как и все субъективные методы SAMVIQ не используется для оценки качества в реальном режиме времени, в основном применяется для решения задачи сравнения видеокодеков.

*QoE*. В последнее время большую популярность получил показатель QoE (Quality of Experience) или качество восприятия услуги пользователем. QoE является более широким показателем, чем QoS, потому что определяется не только параметрами сети или качеством предоставляемого контента как QoS, а также учитывает удобство использования системы, содержание контента и ожидания пользователя. Определение качества восприятия QoE определено как общий показатель качества приложения или сервиса, воспринимаемый субъективно конечным пользователем. QoE складывается из объективных (параметры качества QoS) и субъективных показателей (человеческий фактор). К субъективным показателям можно отнести компоненты восприятия человеком, такие как, культурный фон, мотивация, эмоциональное состояние, внимание и т.д.

Также к субъективным показателям относятся функции управления сервисом и тарифы. Функции управления сервисом учитывают опыт работы с конкретной системой и ее уровнем качества, удобство навигации при выборе услуг IPTV, при поиске контента, интуитивно понятный интерфейс. Стоимость услуг может быть выражена в предоставлении особых преимуществ для пользователя, например изображение с низким разрешением будет иметь более низкие QoE и стоимость услуги, но быть вполне приемлемым для пользователя в зависимости от конечного устройства, физического размера дисплея.

Объективные показателя включают в себя факторы передачи информации, факторы функционирования приложений и факторы услуг. Под факторами передачи информации понимают минимальную скорость

передачи данных, максимальный уровень потерь пакетов, задержки и другие сетевые характеристики. Факторы функционирования приложений учитывают параметры кодека, разрешение видеоданных источника, скорость кодирования, схему маскировки ошибок и т.д. Факторы услуг оценивают уровень предоставления услуги, например, время переключения между каналами (Zapping time), возможность выбора контента, электронную программу передач (Electronic Program Guide, EPG), время отклика.

На сегодняшний день нет модели, позволяющей учитывать все показатели QoE. Некоторые из этих показателей, такие как эмоциональное состояние и культурный фон оператор сознательно исключает при оценке, т.к. они не могут контролироваться оператором и не влияют на требования к оборудованию и сети.

Для оценки других факторов используется целый ряд объективных методов, в основном они нацелены на контроль факторов передачи информации, а факторы услуг и управления сервисом отслеживаются в меньшей степени и как правило на начальном этапе при внедрении услуги. Так, например, для уменьшения времени переключения каналов, в некоторых пользовательских приставках происходит сначала подключение в режиме «unicast» и, если пользователь остается на выбранном канале, идет подключение к группе в режиме «multicast». Также с этой целью при включении приставки от Системы условного доступа пользователь получает набор ключей для дешифрования тех каналов, на которые он подписан.

Далее при предоставлении услуг IPTV этот параметр не отслеживается. Тем не менее, качество восприятия является важным фактором при оценке широкополосных услуг и имеет все основания стать ключевым параметром для сравнения различных сервисов, т.к. пользователю наиболее важно насколько сервис удовлетворяет его требованиям. Поскольку в QoE входит большое число объективных

показателей оценки качества IPTV, то он может использоваться на этапе реализации услуг для контроля сетевых характеристик с целью оптимизации существующей сети и показателей систем различных производителей.

Субъективные методы не учитывают особенности пакетных сетей и не позволяют оценивать качество видео в реальном режиме времени, поэтому требуется разработка новых моделей и методов оценки качества передачи видео.

### 6.2.2. Объективные методы

Применяемые на сегодняшний день методы оценки качества передачи видео, основанные на анализе характеристик сети, являются фактически теми же средствами, что используются для контроля качества передачи голосовой информации, т.е. они измеряют параметры транспортной сети. В отличие от субъективных методов объективные методы не дают представления о том, что же на самом деле видит пользователь на экране своего телевизора, т.к. они, по сути, не делают различия между пакетами, переносящими видео и пакетами, переносящими другую информацию. В настоящее время не разработаны рекомендации, специфицирующих введение какой-либо метрики, поэтому существует ряд методов и ещё больше метрик, которые имеют существенные различия между собой и базируются на разных подходах.

Поставщики предоставляют видео в различных форматах. Существует иерархия цифровых форматов сигналов изображения, отличающихся от базового величиной частот дискретизации компонент сигнала, и применяемых в различных областях, связанных с производством и распространением телевизионных программ и фильмов. В настоящее время для работы с различными видео приложениями в сетях связи особую популярность получили форматы «Common Intermediate Format», CIF



(разрешение 352x288 пикселей) и «Quarter CIF» QCIF (разрешение 176x144 пикселя). Также, широко используются форматы 4:2:2 и 4:2:0 (разрешение 720x576 пикселей «основной уровень» стандарта MPEG-2. Однако, передача изображения без преобразований не сулит никаких преимуществ и используется только при студийной работе, так как требует огромной пропускной способности каналов связи. Поэтому на этапе цифровой обработки изображения осуществляется сжатие видео сигнала различными кодеками. Результатом сжатия является сигнал, закодированный в определенном видео формате, в котором устранены различные формы избыточности изображения. Видео формат определяет структуру видео файла, способ хранения файла на носителе информации (CD, DVD, жестком диске или канале связи). Форматы, в свою очередь, по-разному восприимчивы к потерям и задержкам на сети.

Разные видимые искажения, такие как мерцание, блочность, застывшие видеокadres вызваны различным уровнем потерь. Таким образом, сложно разработать методику объективной оценки качества передачи видео, основанную на одном или нескольких сетевых показателях. В таблице 6.2 представлена зависимость различных видов искажений видео от сетевых характеристик.

Таблица 6.2. Зависимость искажений видео от сетевых показателей

№ п/п	Искажение видео	Сетевые показатели	Метод измерения
1	Блочность видео (пикселизация, распадание картинки на квадраты)	Потери пакетов	VQM, PSNR, MDI, MPQM
2	Случайные полосы в изображении	Джиттер	MDI

3	Искаженное видео, рассыпание изображения	Прибытие пакетов в неправильном порядке	
4	Несинхронный звук по отношению к изображению	Ошибки в настройке буфера на приеме, джиттер	
5	Смазанность	Уровень потерь 5%	VQM, PSNR, MDI, MPQM
6	Мерцание	Переполнение буфера абонентского устройства и потери пакетов	
7	Застывшие видеок cadры	Эти искажения вызваны разным уровнем потерь	VQM, PSNR, MDI, MPQM
8	Провалы в видеоизображении		
9	Отсутствие видео		
10	Потеря звука в видео	Задержки, джиттер	MDI

**MDI.** Большую популярность получил параметр доставки информации Media Delivery Index, MDI, описанный в IETF RFC 4445. Параметр MDI применяется для контроля сети, предназначенной для доставки потоковой информации, видео в формате MPEG, VoIP, и другой информации, чувствительной к задержкам и потерям пакетов. Параметр MDI определяет критический размер буфера приемника, обусловленный джиттером и потерей пакетов. Время измерений может варьироваться от достаточно большого промежутка, чтобы уловить аномальную ситуацию на сети, до бесконечно большого для постоянного контроля.

Параметр MDI состоит из двух компонент: фактора задержки (DF, delay Factor), измеряемого в мс, и параметра потерь пакетов (MLR, Media Loss Rate), измеряемого в пакетах за секунду. Фактор задержки представляет собой максимальную разницу между реальным временем прибытия пакета и ожидаемым, наблюдаемую при приеме каждого пакета транспортного потока. Фактор задержки определяет время, на которое поток данных должен помещаться в буфер приемника для достижения постоянной скорости передачи и предотвращения потерь данных. Таким образом, он учитывает джиттер и позволяет получить значение размера буфера, что помогает избежать потерь пакетов из-за опустошения буферов, например в случае большого значения задержки и недостаточного размера буфера. Значение DF может быть в диапазоне от 0 до 50 мс (согласно ITU G.1050, в котором описана хорошо контролируемая сеть для передачи звука и видео).

Параметр потери пакетов определяет количество потерянных или неправильно принятых пакетов данных за исследуемый период времени. Очевидно, что основной задачей для MLR является достижение 0, поскольку потеря нескольких MPEG-2 TS пакетов приводит к видимому ухудшению качества изображения. Однако на практике все сети имеют некоторый уровень потерь IP пакетов, так при потере менее 0,5% пакетов считается, что сеть обеспечивает хорошее качество видео для конечного пользователя. При 5% потерь появляются видимые пользователю проблемы с видео, например, распад изображения на квадраты, смазанность и т.д. Длина каждого пакета транспортного потока MPEG-2 составляет 188 байт. Как правило, если для передачи используется технология Ethernet, для которой размер поля данных не может превышать 1500 байт, то в одном пакете IP передаются семь пакетов транспортного потока MPEG-2. Потеря одного такого кадра Ethernet означает потерю 7 пакетов данных MPEG-2.

Одним из основных достоинств параметра MDI можно назвать локализацию проблем, возникающих на сети, т.к. MDI позволяет проводить

измерения в разных точках сети, что позволяет получить данные, указывающие на наличие проблемы в сети, до того как она приведет к ухудшению качества видео. Ещё одним преимуществом MDI является то, что не нужно проводить подробный разбор или декодирование транспортного потока MPEG-2, поэтому для измерения не требуется мощного процессора для обработки данных в реальном времени. Для измерения параметра MDI используется информация транспортного заголовка, при этом MDI не зависит от типа видеокodeка, что позволяет производить измерения одновременно на большом количестве каналов и для зашифрованных видеопотоков. Поскольку параметр MDI основывается на сетевых характеристиках, то он может быть использован для установки пороговых значений в сети, достижение которых сигнализирует о приближении проблемы, влияющей на качество видео. Также он может применяться для контроля сетевого оборудования, например, маршрутизатора, на котором зачастую происходят задержки и потери пакетов.

Несмотря на ряд достоинств, параметр MDI не дает четкого понимания, что за картинку видит пользователь на экране своего телевизора. По своей сути параметр линейно отображает характеристики сети, в то время как, видео данные в зависимости от алгоритмов сжатия отличаются нелинейностью и, как результат, значения сетевых параметров, удовлетворительные в одном случае, могут оказаться критичными для качества видео в другом. Например, при потере одного I-кадра MPEG-2, происходит потеря целой группы P- и B-кадров, предсказанных на основе этого I-кадра. В то время как, при потере даже группы P- и B-кадров, они могут быть скорректированы на основе I-кадра или заменены I-кадром (в зависимости от реализации кодека). I-кадр представляет собой изображение с внутрикадровым кодированием, в котором сокращается только пространственная избыточность. P-кадры - изображения с однонаправленным предсказанием на основе предыдущего I-изображения, в

котором сокращается и пространственная и временная избыточность. В-кадры – изображения с двунаправленным предсказанием на основе предыдущего и последующего изображений. В них сокращается и временная и пространственная избыточность и достигается наибольшая степень компрессии.

*VQM.* Метод VQM (Video Quality Measurement) описан в Рекомендации ITU- R BT.1683. VQM основывается на идее о том, что в большинстве случаев наблюдатель при оценке качества изображения менее внимателен к мелким деталям, в то время как его основное внимание концентрируется на крупных объектах. Для получения видео, пригодного для передачи по сети, оно подвергается кодированию и сжатию. В основном методы сжатия информации, используемые сегодня, являются методами с необратимыми потерями, которые возникают в ходе сокращения пространственной, временной и спектральной избыточности. Следовательно, возможно представить высокочастотную временную и пространственную информацию с меньшей точностью, а потерей качества в таком случае можно пренебречь, поскольку человеческий глаз малочувствителен к искажениям на подобном уровне. Метод VQM оценивает видимый результат ухудшения видео, включая смазанность, дрожание, блочность, шум, искажение цвета. Далее все эти параметры комбинируются в одну метрику.

Результаты тестирования показывают, что VQM имеет высокую корреляцию с субъективными методами оценки качества видео и претендует на то, чтобы стать стандартом в области объективной оценки качества видео. Поскольку в методе VQM для расчета качества передачи происходит сравнение исходного видео и видео, полученного в конечной точке, то для его реализации требуется высоко производительное оборудование, что делает этот метод не пригодным для оценки качества видео в реальном масштабе времени, когда необходимо анализировать одновременно большое количество потоков.

**MPQM**. Метрика MPQM (Moving Picture Quality Metric) или в практической реализации «V-фактор» осуществляет контроль в реальном режиме времени и основывается на модели «human vision system», т.е. оценивает параметры видео, видимые человеком. Сначала MPQM анализирует исходную последовательность, которая берется в начальной точке измерений и искаженную версию этой последовательности, взятую в исследуемых каналах. Далее измерения, основанные на искажениях в каналах, подсчитываются, учитывается чувствительность к контрасту и маскируются. Наконец, информация об измерениях со всех исследуемых каналов, которая включает в себя оценку 34 параметров, объединяется для подсчета рейтинга качества передачи видео, который варьируется от 1 до 6 (от «плохого» до «превосходного»). Несмотря на то, что данная метрика позволяет достаточно полно и точно оценить качество изображения видимое пользователем, она является затратной с точки зрения использования ресурсов и не подходит для применения в реальном масштабе времени.

**NQM**. Метрика NQM (Noise Quality Measure) подсчитывает влияние аддитивного шума на исходный сигнал. Воспринимаемые человеческим глазом эффекты от частотного искажения и влияния шума являются независимыми, при эксперименте разделяют эти два источника ухудшения видео и измеряют насколько производимый ими эффект видим для человеческой системы восприятия. NQM принимает во внимание следующее: разброс контраста в зависимости от расстояния элементов, разрешения изображения и пространственной частоты; разброс значений яркости соседних элементов; зависимость контраста от пространственных частот; эффекты, маскирующие контраст. Подобный подход позволяет исследовать фундаментальное соотношение между искажением и шумом для того, чтобы улучшить алгоритмы восстановления получаемых видео последовательностей, но не дает полного видения ситуации, т.к. не учитывает большинство сетевых характеристик и специфических особенностей видео приложений.

*PSNR*. Метрика PSNR (Peak Signal to Noise Ratio) является наиболее традиционным методом измерения качества системы обработки и передачи цифрового видео, измеряется в дБ. PSNR измеряет отношение сигнала к шуму или пиковое отношение сигнала к шуму между исходным сигналом и сигналом на выходе системы. PSNR не позволяет измерить все параметры компрессированного цифрового видео, поскольку точность представления изображения постоянно изменяется в зависимости от визуальной сложности изображения, доступной скорости передачи и даже метода компрессии. Таким образом, PSNR не может определить насколько заметными эти искажения будут для пользователя. Одним из основных преимуществ PSNR можно назвать невысокую вычислительную сложность. Поэтому часто именно эту метрику берут за основу для создания различных моделей оценки качества передачи видео и дополняют её необходимыми показателями.

### 6.3. Влияние сети на показатели качества передачи видео данных (сигналов)

Определение качества услуг возможно лишь в сравнении исходного качества услуг, передаваемого поставщиком услуг, с качеством услуг, получаемого на оборудовании пользователя (рис. 6.1).

На качество видео изображения влияет не только функционирование сети связи на нижних уровнях модели взаимодействия открытых систем, поэтому необходимо осуществлять прямой мониторинг услуги для обеспечения гарантированной доставки видео услуги. Тем не менее, для оценки качества полученного видеонаизображения с точки зрения функционирования сети можно воспользоваться следующими метриками:

- доля потерянных пакетов (Packet Loss Ratio, PLR);
- задержка при доставке пакетов;
- вариация задержки;
- количество пакетов, полученных с ошибкой;

- количество поврежденных пакетов;
- коэффициент ошибок (Bit-Error Ratio, BER);
- потеря фреймов синхронизации (Loss Of Frame, LOF);
- потеря сигнала (Loss Of Signal, LOS);
- доля времени без ошибок (Error-Free Seconds, EFS).



Рис. 6.1. Параметры влияющие на качество услуг IPTV

В дополнение к приведенным метрикам функционирования транспортной сети на сети IPTV должен осуществляться мониторинг и обеспечиваться определение взаимосвязей множества единичных индикаторов функционирования. Ключевыми индикаторами при этом являются:



- количество ошибок, связанных с остановившимся видео изображением (застывших видео моментов), при предоставлении услуг телевизионного вещания и VOD;
- количество ошибок, связанных с пропущенными видео изображениями, при предоставлении услуг телевизионного вещания и VOD;
- задержка при присоединении и отключении от группы многоадресной рассылки;
- задержка при переключении между телевизионными каналами;
- задержка после выбора функции «Воспроизведение»;
- задержка при выборе функции «Быстрая перемотка вперед», «Пауза», «Обратная перемотка»;
- индекс качества при предоставлении услуг телевизионного вещания и VOD.

#### 6.4. Механизмы обеспечения качества передачи видео данных (сигналов)

В настоящее время существует целый ряд методов и механизмов, способных обеспечить качество обслуживания в сетях. Некоторые из них появились совсем недавно, а другие были разработаны и используются достаточно давно. Начнем с механизмов обработки очередей, которые являются одним из основных способов обеспечения QoS.

##### Механизмы обслуживания очередей

Механизм FIFO (“FirstIn — FirstOut”, “первым пришел — первым ушел”) представляет собой механизм обслуживания очередей, в соответствии с которым порядок постановки пакетов в очередь совпадает с порядком их извлечения из очереди для обработки (передачи). Очередь механизма FIFO схематически представлена на рис. 6.2.

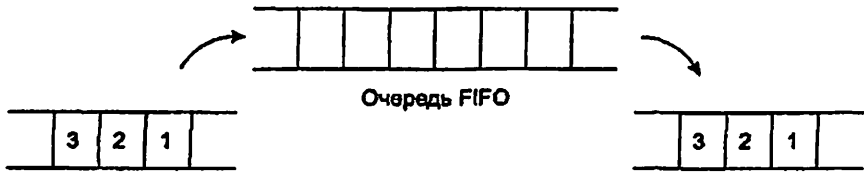


Рис. 6.2. Очередь FIFO

Как уже говорилось ранее, в соответствии с механизмом обслуживания FIFO порядок постановки пакетов в очередь совпадает с порядком их извлечения из очереди. На сегодняшний день механизм FIFO является наиболее распространенным механизмом обслуживания очередей, применяющимся в маршрутизаторах. Его реализация отличается своей простотой. К сожалению, механизм FIFO не имеет средств дифференцирования потоков трафика и, следовательно, не может выделить приоритетные потоки. Более того, механизм FIFO не способен обеспечить равномерное обслуживание потоков трафика с одинаковым приоритетом и защитить их от подавления потоками с неравномерной интенсивностью. Последние могут отобрать часть ресурсов у потоков, имеющих постоянную интенсивность и обслуживаемых сквозными адаптивными схемами управления потоком, такими, как схема управления динамическим окном протокола TCP. Выясняется, что в соответствии с механизмом FIFO потоки трафика обслуживаются почти пропорционально их интенсивности. Подобная схема обслуживания очередей не является равномерной, поскольку она допускает преобладание потоков высокой интенсивности над всеми остальными потоками трафика. Любой же равномерный алгоритм обслуживания очередей обеспечивает защиту от потоков с высокой интенсивностью по своей природе.

*Random Early Detection* (случайное раннее обнаружение) предоставляет собой альтернативу очередям FIFO. Этот метод позволяет смягчить эффект

от потери пакетов даже при очень больших нагрузках. Такая очередь по-прежнему использует принцип FIFO, но пакеты отбрасываются случайным образом (вместо того, чтобы отбрасывать хвост очереди), когда средняя длина очереди за данный промежуток времени превосходит установленное значение. Этим достигается оптимизация заполнения очереди. Данный алгоритм был изначально придуман для протокола TCP, но он может быть применим к трафику любого протокола, когда сеть не гарантирует доставки.

*Generalized Processor Sharing* (обобщенная схема разделения процессорного времени). При обработке потоков трафика, передаваемого по методу негарантированной доставки (а также всех других равновесных классов трафика), должна применяться схема, обеспечивающая справедливое обслуживание по типу максимальной схемы равномерного распределения ресурсов. Именно такой схемой и является обобщенная схема разделения процессорного времени.

В соответствии со схемой GPS каждый поток трафика помещается в собственную логическую очередь, после чего бесконечно малый объем данных из каждой непустой очереди обслуживается по круговому принципу. Необходимость обработки бесконечно малого объема данных на каждом круге обусловлена требованием обслуживания всех непустых очередей на любом конечном временном интервале. Таким образом, схема GPS является справедливой в любой момент времени.

Если же всем потокам трафика назначить вес, то объем данных потока, обрабатываемый на каждом круге, будет пропорционален его весу. Подобное расширение схемы GPS фактически представляет собой взвешенную максимальную схему равномерного обслуживания.

*Priority Queuing* (приоритетное обслуживание) основан на разделении всего сетевого трафика на небольшое количество классов, а затем назначении каждому классу некоторого числового признака — приоритета (рис. 6.3).

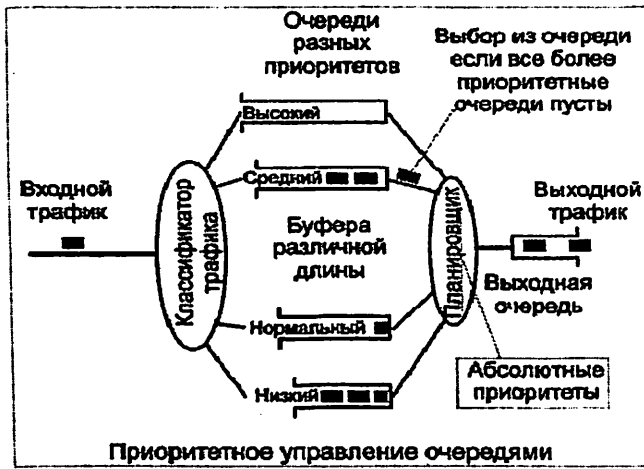


Рис. 6.3. Приоритетное обслуживание

Классификация трафика представляет собой отдельную задачу. Пакеты могут разбиваться на приоритетные классы в соответствии с типом сетевого протокола— например, IP, IPX или DECnet (заметим, что такой способ подходит только для устройств, работающих на втором уровне), на основании адресов назначения и источника, номера TCP/UDP порта, поля IP-пакета имеет под названием “тип сервиса и любых других комбинаций признаков, которые содержатся в пакетах. Правила классификации пакетов на приоритетные классы представляют собой часть политики управления сетью.

*Weighted Queuing* (взвешенные очереди) разработан для того, чтобы можно было предоставить всем классам графика определенный минимум пропускной способности или гарантировать некоторые требования к задержкам. Под весом данного класса понимается процент предоставляемой классу трафика пропускной способности от полной пропускной способности выходного интерфейса. Алгоритм, в котором вес классов трафика может назначаться администратором, называется “настраиваемой очередью”

(*Custom Queuing*). В случае, когда веса назначаются автоматически, на основании некоторой адаптивной стратегии, реализуется так называемый алгоритм “взвешенного справедливого обслуживания” (*Weighted Fair Queuing, WFQ*).

Как при взвешенном (рис. 6.4.), так и при приоритетном обслуживании, трафик делится на несколько классов для каждого из которых ведется отдельная очередь пакетов.

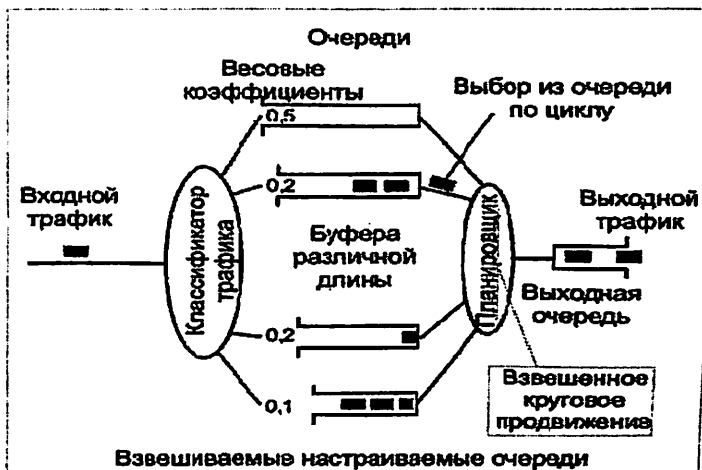


Рис. 6.4. Взвешенные очереди

*Weighted Random Early Detection* – WRED (взвешенный алгоритм произвольного раннего обнаружения) предоставляет различные уровни обслуживания пакетов в зависимости от вероятности их отбрасывания и обеспечивает избирательную установку параметров механизма RED на основании значения поля IP-приоритета. Другими словами, алгоритм WRED предусматривает возможность более интенсивного отбрасывания пакетов, принадлежащих определенным типам трафика, и менее интенсивного отбрасывания всех остальных пакетов.

*Class Based Weighted Fair Queuing* (CBWFQ) соответствует механизму обслуживания очередей на основе классов. Весь трафик разбивается на 64 класса на основании следующих параметров: входной интерфейс, лист доступа (accesslist), протокол, значение DSCP, метка MPLS QoS.

Общая пропускная способность выходного интерфейса распределяется по классам. Выделяемую каждому классу полосу пропускания можно определять как в абсолютном значении (bandwidth в kbit/s) или в процентах (bandwidthpercent) относительно установленного значения на интерфейсе.

Пакеты, не попадающие в сконфигурированные классы, попадают в класс по умолчанию, который можно дополнительно настроить и который получает оставшуюся свободной полосу пропускания канала. При переполнении очереди любого класса пакеты данного класса игнорируются.

**Интегрированное обслуживание.** Модель интегрированного обслуживания обеспечивает сквозное (End-to-End) качество обслуживания, гарантируя необходимую пропускную способность. IntServ использует протокол сигнализации RSVP (протокол резервирования сетевых ресурсов – Resource Reservation Protocol), который обеспечивает выполнение требований ко всем промежуточным узлам.

В основу протокола резервирования ресурсов RSVP заложены три понятия:

- сеанс;
- спецификация потока;
- спецификация фильтра.

*Сеанс* - это период обработки потока данных. Сеанс начинается с выделения ресурсов, необходимых для пропуска потока, и заканчивается после прохождения потока. Запрос на резервирование ресурсов от получателя состоит из спецификации потока и фильтра.

*Спецификацию потока* определяют параметры услуг, которые необходимо зарезервировать, чтобы поток мог пройти через данный узел без потери качества.

*Спецификация фильтра* определяет набор пакетов, под которые запрашиваются ресурсы. Любые другие пакеты обрабатываются по остаточному принципу с предоставлением минимальных услуг, которые сеть может обеспечить в это время. Спецификация фильтра описывает произвольное подмножество пакетов одного сеанса. Фильтр может быть настроен на различные параметры: конкретных отправителей, конкретные протоколы, поля заголовков и т.д.

Протокол резервирования ресурсов имеет следующие атрибуты:

- RSVP выполняет резервирование для уникастных и мультикастных приложений, динамически адаптируясь к изменениям членства в группе вдоль маршрута;
- RSVP является симплексным протоколом, т.е., он выполняет резервирование для однонаправленного потока данных;
- RSVP ориентирован на получателя, т.е., получатель данных инициирует и поддерживает резервирование ресурсов для потока;
- RSVP поддерживает динамическое членство в группе и автоматически адаптируется к изменениям маршрутов;
- RSVP не является маршрутным протоколом, но зависит от существующих и будущих маршрутных протоколов;
- RSVP транспортирует и поддерживает параметры управления трафиком и политикой, которые остаются непрозрачными для RSVP;
- RSVP обеспечивает несколько моделей резервирования или стилей, для того чтобы удовлетворить требованиям различных приложений;
- RSVP обеспечивает прозрачность операций для маршрутизаторов, которые его не поддерживают;
- RSVP может работать с IPv4 и IPv6.

Основная сложность протокола RSVP связана с групповой рассылкой, так как запросы на выделение ресурсов распространяются в обратном направлении по дереву маршрутизации. Протокол RSVP использует два основных типа сообщений (рис. 6.5): RESV и PATH.

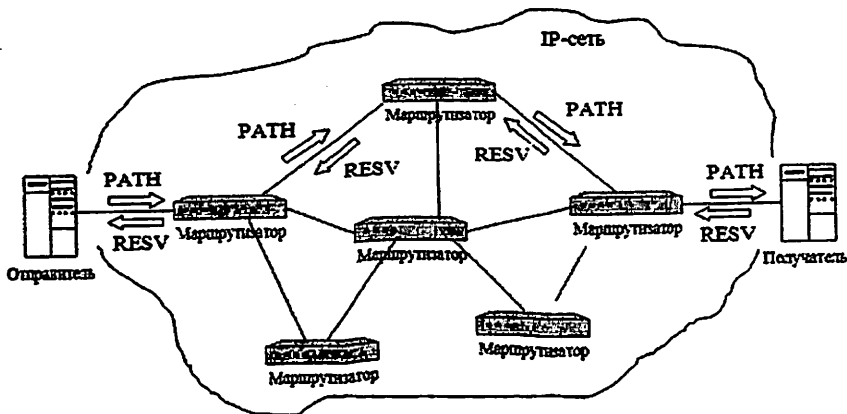


Рис. 6.5. Передача сообщений протокола RSVP в IP-сети для резервирования сети

Первое сообщение генерируется получателем и распространяется вверх по дереву маршрутизации. Данное сообщение передается каждому маршрутизатору на пути потока. Если маршрутизатор не может обеспечить требуемую полосу пропускания, он отвергает этот запрос. Если может, это сообщение передается следующему маршрутизатору. Сообщение RESV приводит к переходу маршрутизатора в состояние резервирования ресурсов для сеанса. Объединенные сообщения RESV достигают отправителя, и на основании полученной информации о зарезервированных ресурсах отправитель задает необходимые параметры потоку до первого маршрутизатора.

Сообщение PATH используется для распространения информации об обратном маршруте. Используемый протоколом RSVP протокол маршрутизации не может определить обратный маршрут, а сообщение RESV должно передаваться именно по обратному маршруту. Информация об обратном маршруте получается следующим образом: любое устройство, желающее стать отправителем, посылает сообщение PATH членам своей



группы. При получении этого сообщения маршрутизаторы и члены группы переходят в состояние PATH. В этом состоянии пакеты для данного отправителя должны пересылаться на маршрутизатор, от которого они были получены. Каждый маршрутизатор, получивший сообщение PATH, запоминает идентификатор потока и канал связи, по которому пришло это сообщение. Если потенциальный адресат, принявший команду PATH, хочет получить указанные данные, он посылает команду RESV. Эта команда следует по пути PATH, но в обратном направлении.

Можно упрощенно описать данный алгоритм на следующем примере. Предположим, что отправитель, зная всех получателей, хочет показать им видеоклип. Так как адреса известны, он посылает им сообщение PATH. Это сообщение несет информацию о том, что отправитель собирается показать видеоклип членам своей группы. По пути следования к адресатам, сообщение выставляет на маршрутизаторах необходимые для передачи потока параметры. Если какой-либо маршрутизатор не может обеспечить данные параметры, он отвергает сообщение. Это означает, что получатель на таком маршруте не сможет посмотреть видеоклип. После достижения сообщением PATH всех получателей, они анализируют полученную с этим сообщением информацию и отвечают сообщением RESV. Сообщение RESV проходит по маршруту сообщения PATH, но в обратном направлении. Получатели закладывают в сообщения RESV информацию о том, хотят ли они посмотреть клип. Они могут попросить показать другой клип. Некоторые попросят уменьшить качество видео, так как имеют плохие каналы связи и т.д. После того как отправитель получил все сообщения RESV, он начинает сеанс с учетом пожеланий каждого получателя.

Сообщения RESV/PATH могут использоваться для определения вышедшего из строя узла или канала связи. Обмен этими сообщениями подтверждает, что сеанс ещё не окончен, то есть выделенные ресурсы должны поддерживаться.

Можно привести другой пример работы протокола RSVP. Если рабочей станции необходимо зарезервировать полосу пропускания для какого-либо трафика, она посылает ближайшему маршрутизатору запрос протокола RSVP, который определяет, что необходим канал с пропускной способностью 1 Мбит/с до определенного получателя. Данный запрос просматривается всеми маршрутизаторами на пути. Если маршрутизатор может поддержать содержащиеся в запросе требования, он передает запрос следующему маршрутизатору и т.д. Запрос считается выполненным, если все маршрутизаторы ответили утвердительно. Если один из маршрутизаторов не поддерживает требований, он ответит конечной станции сообщением о том, что запрос отклонен.

Основной недостаток протокола RSVP заключается в том, что имеющиеся протоколы маршрутизации не принимают во внимание вопросы качества обслуживания, а запросы RSVP выполняются только после того, как был выбран маршрут передачи. Из некоторого количества альтернативных маршрутов протокол маршрутизации может выбрать маршрут, который не оптимален с точки зрения протокола RSVP. Это приводит к тому, что выбранный маршрут зачастую не может соответствовать запросу RSVP, по причине, например, отсутствия резервов пропускной способности. Так как все маршрутизаторы на пути передачи данных должны учесть запросы RSVP, описанная выше ситуация может привести к отклонению запроса, хотя, возможно, если бы был выбран другой путь, запросы были бы удовлетворены.

Неспособность протоколов маршрутизации учитывать вопросы качества обслуживания при выборе маршрута приводит к другой проблеме, связанной с протоколом RSVP. Это - масштабируемость. Каждый маршрутизатор должен принимать и обрабатывать информацию о состоянии всех контролируемых протоколом RSVP потоков данных, проходящих через него, а это может привести к перегрузке маршрутизатора, обслуживающего множество потоков. Проблема только отчасти сглаживается умением RSVP

объединять маршруты для групповой доставки данных. Сложности также возникают при обработке данных, которые перенаправляются по другим маршрутам, например, из-за возникновения перегрузок. Новые маршруты должны быть проложены в соответствии с требованиями RSVP с помощью специальных сообщений от других маршрутизаторов в потоке.

**Дифференцированное обслуживание.** Архитектура DiffServ предполагает существование связанных областей сети (DiffServ-доменов), в пределах каждой из которых проводится единая политика по классификации служб передачи пакетов. Классификация производится на основании анализа заголовков пакетов, но при этом могут приниматься во внимание и другие параметры, предусмотренные производителем маршрутизатора. В результате выполнения классификации каждому пакету ставится в соответствие номер некоторого класса обслуживания, реализованного в данном DiffServ-домене. Такой номер класса обслуживания называется DiffServ Code Point (DSCP). Выбранное значение DSCP записывается в заголовок IP-пакета в поле ToS. Для каждого класса обслуживания администратор DiffServ- домена может установить набор требований к параметрам QoS. После классификации пограничные устройства приводят параметры информационных потоков, поступающих в DiffServ-домен в соответствие с требованиями, устанавливаемыми для выбранных классов обслуживания. При этом часть пакетов может быть помещена в очередь или отброшена, если информация поступает быстрее, чем это разрешено для данного класса обслуживания. Архитектура модели DiffServ приведена в рис. 6.6.

Названная процедура необходима, так как почти всегда DiffServ-домен может обеспечить передачу потока информации в соответствии с некоторым классом обслуживания, только если при поступлении этот поток также соответствует некоторому набору параметров. Маршрутизаторы DiffServ-домена обрабатывают значение DSCP и в соответствии с его значением пересылают пакет следующему маршрутизатору, гарантируя при этом соблюдение определенного набора характеристик (Per-Hop Behavior - PHB),

обеспечиваемых на участке передачи между двумя соседними маршрутизаторами.

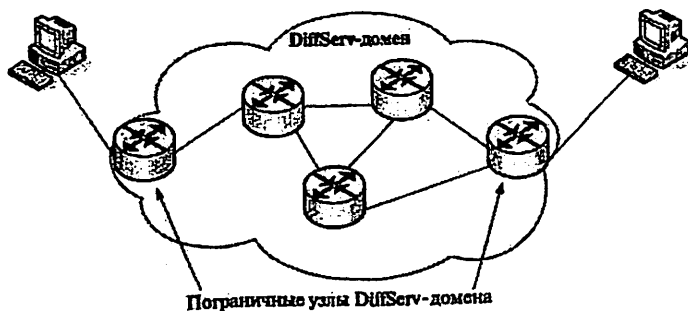


Рис. 6.6. Архитектура модели DiffServ

В DiffServ PNH являются минимальными строительными блоками, из которых строятся различные классы обслуживания, реализуемые в DiffServ-домене. Конкретные механизмы, которые могут быть использованы для создания различных PNH, отличаются в маршрутизаторах разных моделей или производителей. Как правило, PNH настраиваются на основе низкоуровневых механизмов, таких как, например, очереди с приоритетами или очереди с весами. Практически подтверждено: архитектура DiffServ действительно позволяет организовать внутри DiffServ-домена несколько так называемых виртуальных служб передачи информации, которые предназначены для выполнения пересылки потоков данных, обеспечивая при этом максимально возможное соответствие параметров передачи соответствующим классам обслуживания (но не гарантируя полного соответствия). Надо отметить, что в DiffServ не предусматривается каких-либо механизмов уведомления сетевых устройств со стороны приложений о том, сколько ресурсов им требуется или какое количество потоков они планируют пересылать. В этом плане архитектура DiffServ соответствует традиционной архитектуре сети Интернет, когда на сетевых устройствах не запоминается информация об

активных потоках, при этом в сетевых устройствах хранятся только правила обработки пакетов, а в каждом пакете содержится вся информация, необходимая для его доставки получателю. Корректная передача пакетов обеспечивается за счет того, что все промежуточные устройства выполняют идентичный алгоритм обработки пакетов.

**Интегро-дифференцированное обслуживание.** Интегро-дифференцированное обслуживание (Integrated Services Operation over DiffServ Networks) опубликованный в 2000 г. как стандарт RFC2998, описывает принципы организации взаимодействия IntServ/RSVP и DiffServ для предоставления QoS от источника получателю. Слабые места одной модели компенсируются соответствующими решениями другой. С одной стороны, плохо масштабируемая IntServ на магистральных участках сети может быть заменена на более простую DiffServ. С другой, с помощью RSVP решается вопрос с неопределенностью получаемого сервиса в DiffServ-сети.

Основная проблема при взаимодействии - соответствие ресурсов, запрашиваемых через RSVP и предоставляемых в DiffServ-регионе (так называется непрерывная последовательность DiffServ-доменов, в пределах которых могут оказываться дифференцированные услуги). Для реализации отображения ресурсов был предложен ряд решений.

Возможна организация двух вариантов взаимодействия протоколов качества обслуживания:

- DiffServ-регион не поддерживает RSVP сигнализацию, и ресурсы выделяются на статической основе;

- обработка RSVP-сообщений производится в DiffServ-регионе.

В первом случае совместная работа основана на статическом соглашении клиента с оператором SLS (спецификация уровня сервиса). В простейшей ситуации описывается значение пропускной способности в DiffServ-сети, получаемое трафиком пользователя (рис. 6.8): Tx (отправитель) генерирует сообщения Path, которые направляются к узлу Rx (получатель) через DiffServ-регион.

## DiffServ-регион

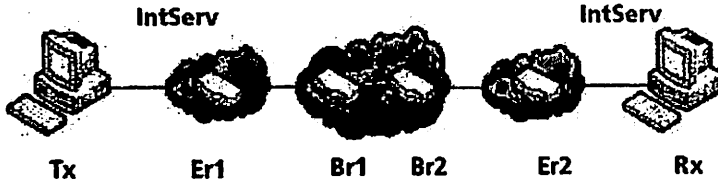


Рис. 6.8. Модель Интегро-дифференцированного обслуживания

При прохождении через DiffServ-регион содержимое RSVP-сообщений игнорируется, и они пересылаются как обычный пакет с данными. При получении узлом Rx сообщения Path генерируется запрос на резервирование RESV, который затем направляется обратно к узлу Tx. При успешной обработке запроса каждым совместимым RSVP-маршрутизатором и прохождении через DiffServ-регион сообщение RESV достигает маршрутизатора Er1, который на основании SLS производит сравнение ресурсов, запрашиваемых в сообщении RESV, и ресурсов, доступных в DiffServ-регионе. Если Er1 подтверждает запрос, информация RESV отсылается далее по направлению к узлу Tx. В ином случае сообщение отвергается, и узлу Rx отправляется оповещение об ошибке. В полученном узлом Tx сообщении могут содержаться данные о маркировании соответствующим кодом пакетов, адресуемых в узел Rx. Значение кода определяется по умолчанию или из сообщения RESV.

Второй вариант предполагает, что пограничные маршрутизаторы в DiffServ-регионе (например, маршрутизатор Br1) поддерживают протокол RSVP. Отметим, что, несмотря на поддержку RSVP-сигнализации, обрабатываются только агрегированные потоки, а не единичные, как в сети IntServ/RSVP. Порядок обмена RSVP-сообщениями такой же, как и в предыдущем случае. Однако благодаря поддержке RSVP в DiffServ-регионе блок управления доступом является частью DiffServ-сети. В результате.

маршрутизатор Bg1 имеет возможность непосредственно обработать RSVP-запрос, исходя из доступности ресурсов.

## ЛИТЕРАТУРА

- 1 Дж. Куроуз, К. Росс, «Компьютерные сети» 2-е издание, С.-Пб.: Издательский дом "Питер", 2004
- 2 Олифер В. Г., Олифер Н. А., «Компьютерные сети. Принципы, технологии, протоколы» 2-е издание, С.-Пб.: Издательский дом "Питер", 2004
- 3 Функциональная архитектура IPTV: Рекомендация ITU-T Y.1910. – 2008
- 4 М.А. Маколкина, «Методы оценки качества обслуживания IPTV» Учебное пособие, СПб ГУТ, САНКТ-ПЕТЕРБУРГ, 2012.
- 5 Gerard O'Driscoll , "Next Generation IPTV Services and Technologies", A John Wiley & Sons, Inc., Publication – 2007;
- 6 Francisco J. Hens and Jose' M. Caballero, "Triple Play - Building the converged network for IP, VoIP and IPTV", John Wiley & Sons Ltd. - 2008
- 7 Шринивас Вегешна, "Качество обслуживания в сетях IP", Издательский дом "Вильямс" - 2003.
- 8 Семенов Ю.А., "Телекоммуникационные технологии", book.iter.ru
- 9 "Журнал Кабельщик", www.cableman.ru
- 10 "Википедия – свободная энциклопедия", ru.wikipedia.org
- 11 "Интернет-журнал по широкополосным сетям и мультимедийным технологиям", [www.telemultimedia.ru](http://www.telemultimedia.ru)
- 12 "Broadcasting: Телевидение и Радиовещание", [www.broadcasting.ru](http://www.broadcasting.ru)
- 13 [www.citforum.ru](http://www.citforum.ru)



Методические указания «ИЗУЧЕНИЕ ПРИНЦИПОВ ТЕХНОЛОГИИ  
IPTV» к практическим занятиям по дисциплине СЛУЖБЫ  
МУЛЬТИМЕДИА.

Для магистрантов I курса обучающихся по направлению 5A350101-  
Телекоммуникационный инжиниринг

Рассмотрены на заседании кафедры С и СПД и рекомендованы к  
печати протокол № от 24.11.15 г.

Составители:



Джураев Р.Х.

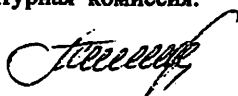
Ответственный редактор:



Джаббаров И.К.

Редакционно - корректурная комиссия:

Корректор:



Абдуллаева С.Х.

Формат 60x84 1/16. Печ. лист 5,25.  
Заказ № 25. Тираж 50.  
Отпечатано в «Редакционно издательском»  
отделе при ТУИТ.  
Ташкент ул. Амир Темур, 108.