Хабаров С.П.

Основы сетевых технологий IP-телефонии и видеонаблюдения

Конспект лекций

Санкт-Петербург
2019

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Первые попытки отображения мультимедийной информации на компьютерах начались в середине XX века. Однако, прогресс в этой сфере был очень малым, вследствие высокой стоимости и ограниченных возможностей компьютеров тех времён. С конца 1980-х и до 1990-х компьютеры, доступные потребителям, уже могли отображать различные виды информации, но технической проблемой для потокового вещания являлось отсутствие достаточно производительного центрального процессора и каналов, работающих со скоростью необходимой для передачи мультимедийного потока данных. В период с 1990 до 2000 года пользователи Интернета получили:

- высокую пропускную способность сетей, в частности, на последней миле
- возросло количество абонентов сетей, особенно Интернета
- стали использоваться стандартизованные протоколы и форматы, такие как TCP/IP, HTTP и HTML
- появилась коммерция в Интернете

Эти достижения в области сетей в совокупности с высокопроизводительными домашними компьютерами и современными операционными системами сделали потоковую мультимедийную информацию доступной широкому кругу простых пользователей. Примерно в 2002 году интерес к единому унифицированному потоковому формату и широкое распространение Adobe Flash поспособствовало разработке формата потокового видео, который использовался во многих Flash-проигрывателях. Сегодня потоковые мультимедиа по умолчанию проигрываются в формате HTML5 видео, которые заменили Flash-проигрыватели.

Мультимедиа потоки бывают двух видов: по запросу или живыми. Потоки информации, вызываемой по запросу, хранятся на серверах продолжительный период времени. Живые потоки доступны короткий период времени, например, при передаче видео со спортивных соревнований. Мультимедиа информация занимает большие объёмы, затраты на ее хранение и передачу всегда велики. Поэтому, в большинстве случаев, передаваемая в поток информация сжимается при передаче в сеть вещания.

Мультимедийные потоки требуют большого количества ресурсов каналов и узлов. Эти ресурсы ограничены. При передаче большого объёма трафика и обработки мультимедийных данных узлы сети могут чаще выходить из строя, в линиях связи могут чаще возникать узкие места. Это особенно губительно сказывается на потоковом мультимедиа, для которого необходимо, чтобы потоки передавались без задержек и прерываний, что влияет на качество услуг, которые предоставляет данная сеть. Под услугами понимается не только предоставление мультимедийных данных, но и любых других.

Поскольку передача мультимедиа может вызвать дисбаланс в IP-сети, важно понимать, что представляют собой мультимедийные сети, каким образом можно

ими управлять. Для возможности работы по внедрению новых мультимедийных сервисов, а также для улучшения работы существующих мультимедийных сетей специалист в области информационных технологий должен иметь хотя бы общее представление о структуре и принципах работы существующих мультимедийных сетей, а также владеть вопросами управления потоками данных в существующих мультимедийных сетях.

Любую сеть передачи потокового мультимедиа можно представить в виде графа, вершинами которого могут быть сервера хранения мультимедийных данных, стримеры, репликаторы и плееры мультимедийных потоков. Под общим термином «репликатор» понимаем транскодеры, ретрансляторы и репликаторы. Линии графа обозначают потоки мультимедийных данных, которые передаются по каналам связи от одного узла к другому (рис.1.1). Узлы могут быть попарно связаны физическими каналами, по которым мультимедийные потоки данных не передаются.

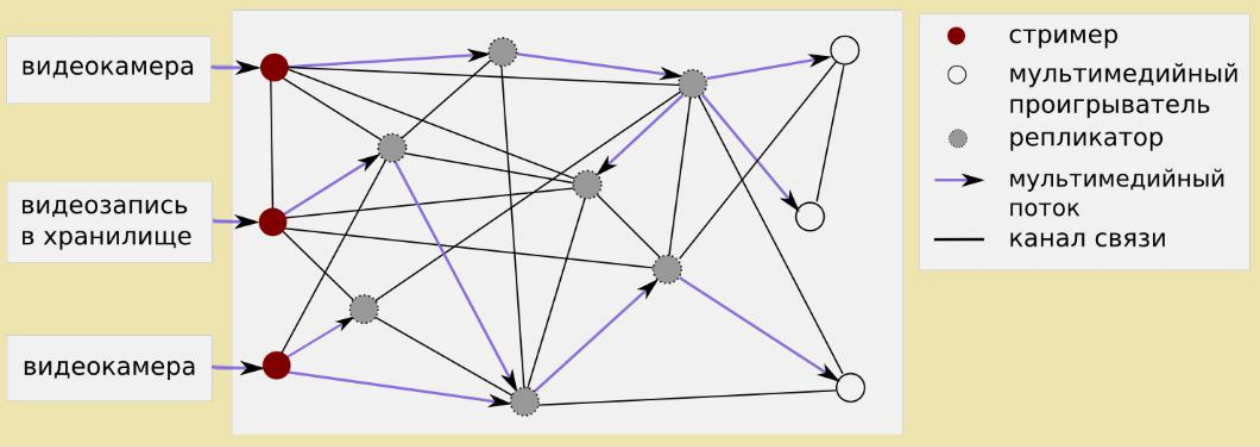

Рис.1.1. Пример структуры мультимедийной сети

В зависимости *от задач*, которые возлагаются на сеть передачи потокового мультимедиа, можно выделить:

- сети трансляции мультимедийного контента
- и мультимедийные сети общения.

В зависимости *от оборудования*, входящего в состав мультимедийной сети, можно выделить:

- сети ретрансляции мультимедийных данных,
- а также сети репликации и ретрансляции мультимедийных данных.

Возможно построение комбинированных мультимедийных сетей, которые сочетают в себе разные принципы организации.

Сети трансляции мультимедийного контента.

Задача сетей трансляции мультимедийного контента – предоставление клиентам услуги получения и просмотра мультимедийных потоков. Это могут быть, например, короткие видеоролики или трансляция событий в реальном времени. Принцип работы таких сетей можно описать следующим образом: есть момент начала трансляции и есть момент завершения трансляции. Если зритель подключился к сети во время её работы, он будет получать потоки данных не от

начала трансляции, а от момента подключения к трансляции. Это похоже на ситуацию, когда человек опаздывает к началу фильма в кинотеатре: фильм уже начался, и его не отмотают назад. Структура сети трансляции мультимедийного контента с точки зрения передачи мультимедийных данных представляет собой ориентированный граф:

- Вершинами инициации мультимедийных потоков являются стримеры, если идёт трансляция «живого» мультимедиа, и серверы хранения, если производится повтор.
- Концевыми вершинами графа являются мультимедийные плееры, которые используют зрители для просмотра, или стримеры и репликаторы, если зрителей у данного мультимедийного потока нет.
- Промежуточными узлами являются репликаторы и/или стримеры.
- Обратные мультимедийные потоки (от концевых вершин к вершинам инициации мультимедийных потоков) отсутствуют.

Количество входящих и исходящих потоков ограничивается возможностями узлов и количеством проигрывателей, принимающих мультимедийные потоки.

Сети трансляции используются в вебинарах, системах телеприсутствия, интернет-телевидении, интернет-радио и др.

Мультимедийные сети общения.

Задача этого класса сетей — предоставление клиентам услуги двух- и многостороннего общения. Структура сети общения с точки зрения передачи мультимедийных данных представляет собой ориентированный мультиграф.

- Вершинами инициации мультимедийных потоков являются стримеры.
- Концевыми вершинами являются мультимедийные плееры, которые используют пользователи.
- Промежуточными узлами являются репликаторы и/или стримеры.

Количество входящих и исходящих потоков ограничивается возможностями узлов и количеством проигрывателей, принимающих мультимедийные потоки.

Для сети общения важно выделять принципы организации связи: «один-к-одному» (приватный разговор), «один-ко-многим» (один из участников управляет трансляцией), «многие-ко-многим» (все участники равны). Пример сервиса общения клиентов: Skype, Google+ Hangouts, Vidicor и др.

Сети ретрансляции мультимедийных данных.

Сети ретрансляции мультимедийных данных могут лежать в основе сетей общения и сетей раздачи мультимедийного контента. В данном случае используются репликаторы для увеличения количества узлов и улучшения качества обслуживания (для увеличения количества зрителей, снижения нагрузки на конкретные узлы сети).

Сети ретрансляции мультимедийных данных могут передавать от вершины к вершине мультимедийные потоки одного качества, т.е. мультимедийный поток во время движения от вершины инициации до концевой вершины не изменяется.

Структура сети ретрансляции с точки зрения передачи мультимедийных данных может быть представлена как в виде ориентированного графа (раздача мультимедийного контента), так и в виде ориентированного мультиграфа (связь нескольких клиентов).

- Вершинами инициации мультимедийных данных могут быть стримеры, находящиеся в географической близости с устройством захвата «сырых» мультимедийных данных, и серверы хранения.
- Концевыми вершинами могут быть проигрыватели мультимедиа потоков и стримеры/репликаторы, если у мультимедийного потока нет зрителей.
- Промежуточными узлами графа могут быть репликаторы и/или стримеры.

Узлы, входящие в состав сети, принимают потоки и передают их далее. Преобразование и разделение одного потока на несколько не предусматривается. Количество входящих и исходящих потоков ограничивается возможностями узлов и количеством мультимедийных плееров, принимающих мультимедийные потоки.

Сети ретрансляции и репликации мультимедийных данных.

Сети ретрансляции и репликации мультимедийных данных также используются для увеличения количества узлов и улучшения качества обслуживания клиентов как при раздаче мультимедийного контента, так и при организации общения клиентов.

Сети репликации и ретрансляции могут передавать от вершины к вершине мультимедийные потоки разного качества, при этом существуют узлы, которые способны преобразовывать входящий мультимедийный поток (например, один поток разделить на несколько). Количество входящих и исходящих потоков ограничивается возможностями узлов и количеством проигрывателей. Структура сети аналогична той, что описывалась для сети ретрансляции.

Комбинированные мультимедийные сети.

Когда речь заходит о сложной системе, которая предполагает и трансляцию мультимедийного контента, и общение зрителей, встаёт вопрос организации сети, которая будет сочетать в себе разные структуры и принципы. В данном случае предполагается более одного источника мультимедийных данных.

Если говорить о комбинированном решении, можно отметить, что компании, предоставляющие услуги трансляции мультимедийного контента или сервиса общения, используют свои подходы к организации и управлению, которые являются ноу-хау. Таким образом, можно выделить сеть конкретной компании и множество однотипных сетей разных компаний, которые работают по своим принципам, со своим программным обеспечением, своей мультимедийной системой на едином пространстве — глобальной сети Интернет.

Комбинированная мультимедийная сеть может быть организована в рамках конкретного подхода, с использованием услуг одной компании, с конкретным

программным и аппаратным обеспечением. «Смешивание» не происходит на уровне сетей разных операторов услуги, разного программного и аппаратного обеспечения, что является существенным недостатком. Одни системы, например, могут быть хороши для трансляции видео, но плохи для общения, могут стоить дороже в сравнении с другими, требовать больше ресурсов и т.д..

Поэтому важным этапом в изучении мультимедийных сетей является не только разработка программного и аппаратного обеспечения для организации структуры конкретной мультимедийной системы и оптимизации работы существующего мультимедийного сервиса, но и разработка методов, алгоритмов, программного обеспечения, которые позволят связать мультимедийные сети разных компаний в единое мультимедийное пространство, которым можно управлять.

Единое мультимедийное пространство подразумевает не только взаимосвязь отдельных сетей, но и частичную замену программно-аппаратного обеспечения, внедрение новых программных средств в существующую сеть. Таким образом, можно сочетать лучшие стороны разных программно-аппаратных комплексов по предоставлению мультимедийных услуг в единой среде.

2. ИСПОЛЬЗОВАНИЕ ПРОТОКОЛОВ ИНТЕРНЕТА ДЛЯ ПЕРЕДАЧИ МУЛЬТИМЕДИЙНЫХ ДАННЫХ

Каждый терминал в сети TCP/IP имеет адреса трех уровней, а именно физический. сетевой и символьный:

- Физический (MAC-адрес) – это локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, куда входит данный узел.
- Сетевой (IP-адрес) – используется на сетевом уровне и, как правило, назначается администратором во время конфигурирования компьютеров и маршрутизаторов. Он состоит из двух частей: номера сети и номера узла. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла – гибкое, и граница между этими полями может устанавливаться весьма условно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.
- Символьный (DNS-имя) – идентификатор-имя. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена.

Интернет – это совокупность тысяч компьютеров, объединенных в сети, которые, в свою очередь, соединены между собой посредством маршрутизаторов. Сеть Интернет имеет иерархическую структуру, что позволяет идентифицировать компоненты Интернета посредством адресов, также имеющих иерархическую структуру. Старшие биты адреса идентифицируют сеть, в которой находится рабочая станция, а младшие - расположение рабочей станции в этой сети.

2.1. Протокол IP версии 6

Подавляющее большинство сетей сейчас использует протокол IPv4 (интернет-протокол версии 4), хотя уже разработана шестая версия протокола IP. Схема адресации протокола IPv4 предусматривает размер адресного поля 32 бита, что дает 2^32 (или 4 294 967 296) потенциальных адресов.

Самой насущной проблемой все чаще становится нехватка адресного пространства, что требует изменения формата адреса. Другой проблемой является недостаточная масштабируемость процедуры маршрутизации - основы IP-сетей. Быстрый рост сети вызывает перегрузку маршрутизаторов, которые уже сегодня вынуждены поддерживать таблицы маршрутизации с десятками и сотнями тысяч записей, а также решать проблемы фрагментации пакетов.

Облегчить работу маршрутизаторов можно, в частности, путем модернизации протокола IP. Наряду с вводом новых функций непосредственно в протокол IP,

целесообразно обеспечить более тесное взаимодействие его с новыми протоколами путем введения в заголовок пакета новых полей. В результате было решено подвергнуть протокол IP модернизации, преследуя следующие основные цели:

- создание новой расширенной схемы адресации;
- улучшение масштабируемости сетей за счет сокращения функций магистральных маршрутизаторов;
- обеспечение защиты данных.

Что касается расширения адресного пространства, то модификация протокола IP решает потенциальную проблему нехватки адресов за счет расширения разрядности адреса до 128. Однако такое существенное увеличение длины адреса было сделано в значительной степени не с целью снять проблему дефицита адресов, а для повышения эффективности работы сетей на основе этого протокола. Главной целью было структурное изменение системы адресации, расширение ее функциональных возможностей.

Вместо существующих двух уровней иерархии адреса (номер сети и номер узла) в протоколе IPv6 предлагается использовать четыре уровня, что предполагает трехуровневую идентификацию сетей и один уровень для идентификации узлов. Теперь адрес записывается в шестнадцатеричном виде, причем каждые четыре цифры отделяются друг от друга двоеточием, например:

```
FEDC:0A96:0:0:0:0:7733:567A
```

Для сетей, поддерживающих обе версии протокола IPv4 и IPv6, имеется возможность использовать для младших 4 байтов традиционную десятичную запись, а для старших - шестнадцатеричную:

```
0:0:0:0:FFFF 194.135.75.104
```

В рамках системы адресации IPv6 имеется также выделенное пространство адресов для локального использования, то есть для сетей, не входящих в Интернет. Существует две разновидности локальных адресов: для "плоских" сетей, не разделенных на подсети (Link-Local), и для сетей, разделенных на подсети (Site-Local), которые различаются значением префикса. Заголовок дейтаграммы IPv6 длиной 40 байтов имеет следующий формат (рис. 2.1).

<table>
<tr><td>0</td><td></td><td></td><td>31</td></tr>
<tr><td>Версия
(4 бита)</td><td>Класс трафика
(8 битов)</td><td colspan="2">Метка потока
(20 битов)</td></tr>
<tr><td colspan="2">Длина
(16 битов)</td><td>След. заголовок
(8 битов)</td><td>Лимит переходов
(8 битов)</td></tr>
<tr><td colspan="4">Адрес отправителя (128 битов)</td></tr>
<tr><td colspan="4">Адрес получателя (128 битов)</td></tr>
</table>

Рис. 2.1. Формат основного заголовка дейтаграммы IPv6

Поле Класс трафика (Traffic Class) эквивалентно по назначению полю Тип обслуживания (Type Of Service), а поле Лимит переходов (Hop Limit) - полю Время жизни (Time To Live) протокола IPv4.

Поле Метка потока (Flow Label) позволяет выделять и особым образом обрабатывать отдельные потоки данных без необходимости анализировать содержимое пакетов. Это очень важно с точки зрения снижения нагрузки на маршрутизаторы.

Поле Следующий заголовок (Next Header) является аналогом поля Протокол (Protocol) IPv4 и определяет тип заголовка, следующего за основным. Каждый следующий дополнительный заголовок также содержит поле Next Header.

2.2. Протоколы TCP и UDP

Протокол управления передачей информации TCP (Transmission Control Protocol) был разработан для поддержки интерактивной связи между компьютерами. Он обеспечивает надежность и достоверность обмена данными между процессами на компьютерах, входящих в общую сеть.

К сожалению, протокол TCP не приспособлен для передачи мультимедийной информации. Основная причина - наличие контроля за доставкой. Контроль отнимает слишком много времени для передачи более чувствительной к задержкам информации. Кроме того, TCP предусматривает механизмы управления скоростью передачи с целью избежать перегрузок сети. Аудио- и видеоданные требуют, однако, строго определенных скоростей передачи, которые нельзя изменять произвольным образом.

Протокол передачи пользовательских дейтаграмм (User Datagram Protocol - UDP) предназначается для обмена дейтаграммами между процессами компьютеров, расположенных в объединенной системе компьютерных сетей.

Протокол UDP базируется на протоколе IP и предоставляет прикладным процессам транспортные услуги, немногим отличающиеся от услуг протокола IP. Протокол UDP обеспечивает негарантированную доставку данных, то есть не требует подтверждения их получения. Кроме того, данный протокол не требует установления соединения между источником и приемником информации, то есть между модулями UDP.

2.3. Протоколы RTP и RTCP

2.3.1. Основные понятия

Транспортный протокол реального времени RTP (англ. Real-time Transport Protocol) обеспечивает сквозную передачу в реальном времени мультимедийных данных, таких как интерактивное аудио и видео. Этот протокол реализует распознавание типа трафика, нумерацию последовательности пакетов, работу с метками времени и контроль передачи.

Действие протокола RTP сводится к присваиванию каждому исходящему пакету временных меток. На приемной стороне временные метки пакетов указывают на то, в какой последовательности и с какими задержками их

необходимо воспроизводить. Этому во многом способствует протокол RTCP (англ. Real-Time Transport Control Protocol — протокол управления передачей в реальном времени)

Поддержка RTP и RTCP позволяет принимающему узлу располагать принимаемые пакеты в надлежащем порядке, снижать влияние неравномерности времени задержки пакетов в сети на качество сигнала и восстанавливать синхронизацию между аудио и видео, чтобы поступающая информация могла правильно прослушиваться и просматриваться пользователями.

Заметим, что RTP сам по себе не имеет никакого механизма, гарантирующего своевременную передачу данных и качество обслуживания, но для обеспечения этого использует службы нижележащего уровня. Он не предотвращает нарушения порядка следования пакетов, но при этом и не предполагает, что основная сеть абсолютно надежна и передает пакеты в нужной последовательности. Порядковые номера, включенные в RTP, позволяют получателю восстанавливать последовательность пакетов отправителя.

Протокол RTP поддерживает как двустороннюю связь, так и передачу данных группе адресатов, если групповая передача поддерживается нижележащей сетью. Этот протокол предназначен для обеспечения информации, требуемой отдельным приложениям, и в большинстве случаев интегрируется в работу приложения.

Хотя RTP считается протоколом транспортного уровня, он функционирует обычно поверх другого протокола транспортного уровня UDP (User Datagram Protocol). Оба протокола вносят свои доли в функциональность транспортного уровня. Следует отметить, что RTP и RTCP являются независимыми от нижележащих уровней - транспортного и сетевого, поэтому протоколы RTP/RTCP могут использоваться с другими подходящими транспортными протоколами. Протокольные блоки данных RTP/RTCP называются пакетами.

- Пакеты, формируемые в соответствии с протоколом RTP и служащие для передачи мультимедийных данных, называются информационными пакетами или пакетами данных (data packets). Пакет RTP включает в свой состав фиксированный заголовок, необязательное расширение заголовка переменной длины и поле данных.
- Пакеты, генерируемые в соответствии с протоколом RTCP и служащие для передачи служебной информации, которая требуется для надежной работы телеконференции, называют пакетами управления или служебными пакетами (control packets). Пакет RTCP начинается с фиксированной части (подобной фиксированной части информационных пакетов RTP), за которой следуют структурные элементы, имеющие переменную длину.

Для того чтобы протокол RTP был более гибким и мог применяться для различных приложений, некоторые его параметры сделаны преднамеренно неопределенными, но зато в нем предусмотрено понятие профиля.

- Профиль (profile) - это набор параметров протоколов RTP и RTCP для конкретного класса приложений, определяющий особенности их функционирования. В профиле определяются: использование отдельных

полей заголовков пакетов, типы трафика, дополнения к заголовкам и расширения заголовков, типы пакетов, услуги и алгоритмы обеспечения безопасности связи, особенности использования протокола нижележащего уровня и т. д. Каждое приложение обычно работает только с одним профилем, и задание типа профиля происходит путем выбора соответствующего приложения. Никакой явной индикации типа профиля номером порта, идентификатором протокола и т. п. не предусмотрено.

Таким образом, полная спецификация RTP для конкретного приложения должна включать дополнительные документы, к которым относятся описание профиля, а также описание формата трафика, определяющее, как трафик конкретного типа, такой как аудио или видео, будет обрабатываться в RTP.

2.3.2. Групповая аудио-конференцсвязь

Для того чтобы организовать групповую аудио-конференцсвязь требуется многопользовательский групповой адрес и два порта. При этом один порт необходим для обмена звуковыми данными, а другой используется для пакетов управления протокола RTCP. Информация о групповом адресе и портах передается предполагаемым участникам телеконференции. Если требуется секретность, то информационные и управляющие пакеты могут быть зашифрованы, в этом случае также должен быть сгенерирован и распределен ключ шифрования.

Приложение аудио-конференцсвязи, используемое каждым участником конференции, посылает звуковые данные малыми порциями, например, продолжительностью 20 мс. Каждой порции звуковых данных предшествует заголовок протокола RTP. Заголовок RTP и данные поочередно формируются (инкапсулируются) в пакет UDP. Заголовок RTP показывает, какой тип кодирования звука (например, ИКМ, АДИКМ или LPC) применялся при формировании данных в пакете. Это дает возможность изменять тип кодирования в процессе конференции, например, при появлении нового участника, который использует линию связи с низкой полосой пропускания, или при перегрузках сети.

В сети Интернет, как и в других сетях передачи данных с коммутацией пакетов, пакеты иногда теряются и переупорядочиваются, а также задерживаются на различное время. Для противодействия этим событиям заголовок RTP содержит временную метку и порядковый номер, которые позволяют получателям восстановить синхронизацию в исходном виде так, чтобы, например, участки звукового сигнала воспроизводились динамиком непрерывно каждые 20 мс. Эта реконструкция синхронизации выполняется отдельно и независимо для каждого источника пакетов RTP в телеконференции. Порядковый номер может также использоваться получателем для оценки количества потерянных пакетов.

Так как участники телеконференции могут вступать и выходить из нее во время ее проведения, то полезно знать, кто участвует в ней в данный момент и насколько хорошо участники конференции получают звуковые данные. Для этой

цели каждый экземпляр звукового приложения во время конференции периодически выдает на порт управления (порт RTCP) для приложений всех остальных участников сообщения о приеме пакетов с указанием имени своего пользователя. Сообщение о приеме указывает, как хорошо слышим текущий оратор, и может использоваться для управления адаптивными кодерами. В дополнение к имени пользователя может быть включена также другая информация идентификации для контроля полосы пропускания. При выходе из конференции сайт посылает пакет BYE протокола RTCP.

2.3.3. Видео конференцсвязь

Если в телеконференции используются и звуковые, и видеосигналы, то они передаются отдельно. Для передачи каждого типа трафика независимо от другого спецификацией протокола вводится понятие сеанса связи RTP. Сеанс определяется конкретной парой транспортных адресов назначения (один сетевой адрес плюс пара портов для RTP и RTCP). Пакеты для каждого типа трафика передаются с использованием двух различных пар портов UDP и/или групповых адресов. Никакого непосредственного соединения на уровне RTP между аудио- и видео- сеансами связи не имеется, за исключением того, что пользователь, участвующий в обоих сеансах, должен использовать одно и то же каноническое имя в RTCP-пакетах для обоих сеансов, чтобы сеансы могли быть связаны.

Одна из причин такого разделения состоит в том, что некоторым участникам конференции необходимо позволить получать только один тип трафика, если они этого желают. Несмотря на разделение, синхронное воспроизведение мультимедийных данных источника (звука и видео) может быть достигнуто при использовании информации таймирования, которая переносится в пакетах RTCP для обоих сеансов.

2.3.4. Понятие о микшерах и трансляторах

Не всегда все сайты имеют возможность получать мультимедийные данные в одинаковом формате. Рассмотрим случай, когда участники из одной местности соединены через низкоскоростную линию связи с большинством других участников конференции, которые обладают широкополосным доступом к сети.

- Вместо того чтобы вынуждать каждого использовать более узкую полосу пропускания и звуковое кодирование с пониженным качеством, средство связи уровня RTP, называемое микшером, может быть размещено в области с узкой полосой пропускания.
- Этот микшер повторно синхронизирует входящие звуковые пакеты для восстановления исходных 20-миллисекундных интервалов, микширует эти восстановленные звуковые потоки в один поток, производит кодирование звукового сигнала для узкой полосы пропускания и передает поток пакетов через низкоскоростную линию связи.

При этом пакеты могут быть адресованы одному получателю или группе получателей с различными адресами. Чтобы в приемных оконечных точках можно было обеспечивать правильную индикацию источника сообщений,

заголовок RTP включает для микшеров средства опознавания источников, участвовавших в формировании смешанного пакета.

Некоторые из участников аудио-конференции могут быть соединены широкополосными линиями связи, но могут быть недостижимы посредством групповой конференцсвязи с использованием протокола IP (IPM - IP multicast). Например, они могут находиться за брандмауэром прикладного уровня, который не будет допускать никакой передачи IP-пакетов.

Для таких случаев нужны не микшеры, а средства связи уровня RTP другого типа, называемые трансляторами. Из двух трансляторов один устанавливается вне брандмауэра и снаружи передает все групповые пакеты, полученные через безопасное соединение, другому транслятору, установленному за брандмауэром. Транслятор за брандмауэром передает их снова как мультивещательные пакеты многопользовательской группе, ограниченной внутренней сетью сайта.

Микшеры и трансляторы могут быть разработаны для ряда целей. Пример: микшер видеосигнала, который масштабирует видеоизображения отдельных людей в независимых потоках видеосигнала и выполняет их композицию в один поток видеосигнала, моделируя групповую сцену.

2.3.5. Протокол управления RTCP

Все поля пакетов RTP/RTCP передаются по сети байтами (октетами); при этом наиболее значащий байт передается первым. Все данные полей заголовка выравниваются в соответствии с их длиной. Октеты, обозначенные как дополнительные, имеют нулевое значение.

Протокол управления RTCP (англ. Real-Time Control Protocol) основан на периодической передаче пакетов управления всем участникам сеанса связи при использовании того же механизма распределения, что и протокол RTP. Протокол нижнего уровня должен обеспечить мультиплексирование информационных и управляющих пакетов, например, с использованием различных номеров портов UDP. Протокол RTCP выполняет четыре основные функции.

- Главная функция - обеспечение обратной связи для оценки качества распределения данных. Это неотъемлемая функция RTCP как транспортного протокола, она связана с функциями управления потоком и перегрузками других транспортных протоколов. Обратная связь может быть непосредственно полезна для управления адаптивным кодированием, но эксперименты с IP-мультивещанием показали, что обратную связь с получателями также важно иметь для диагностики дефектов при распространении информации. Посылка отчетов обратной связи о приеме данных всем участникам позволяет при наблюдении проблем оценивать, являются они локальными или глобальными. С механизмом распределения IPM для таких объектов, как поставщики услуг сети, можно также получать информацию обратной связи и действовать при диагностике проблем сети как монитор третьей стороны. Эта функция обратной связи обеспечивается отчетами отправителя и приемника RTCP.

- RTCP поддерживает устойчивый идентификатор источника данных RTP на транспортном уровне, называемый "каноническим именем" (CNAME - canonical name). Так как идентификатор SSRC может изменяться, если обнаружен конфликт или перезапущена программа, то получателям для отслеживания каждого участника требуется каноническое имя CNAME. Получатели также требуют CNAME для отображения множества потоков информации от данного участника на множество связанных сеансов RTP, например, при синхронизации звукового и видеосигнала.
- Первые две функции требуют, чтобы все участники посылали пакеты RTCP, следовательно, для предоставления возможности масштабирования числа участников протоколом RTP должна регулироваться частота передачи таких пакетов. При посылке каждым участником телеконференции управляющих пакетов всем остальным участникам, каждый может независимо оценивать общее число участников.
- Четвертая, дополнительная, функция RTCP должна обеспечивать информацию управления сеансом (например, идентификацию участника), которая будет отражена в интерфейсе пользователя. Наиболее вероятно, что это будет полезным в "свободно управляемых" сеансах, где участники вступают в группу и выходят из нее без контроля принадлежности или согласования параметров.

Функции с первой по третью являются обязательными, когда RTP используется в IP-мультивещании, и рекомендуемыми во всех остальных случаях. Разработчикам приложений RTP предлагается избегать механизмов, работающих только в двустороннем режиме и не масштабируемых для увеличения числа пользователей.

Интенсивность передачи пакетов RTCP

Протокол RTP позволяет приложению автоматически масштабировать представительность сеанса связи в пределах от нескольких участников до нескольких тысяч. Например, в аудио конференции трафик данных, по существу, является самоограничивающим, потому что только один или два человека могут говорить одновременно, и при групповом распределении скорость передачи данных на любой линии связи остается относительно постоянной, не зависящей от числа участников. Однако трафик управления самоограничивающим не является. Если отчеты приема от каждого участника посылаются с постоянной интенсивностью, то трафик управления с ростом числа участников будет расти линейно. Следовательно, должен быть предусмотрен специальный механизм понижения частоты передачи управляющих пакетов.

Для каждого сеанса предполагается, что трафик данных соответствует агрегированному пределу, называемому полосой пропускания сеанса связи, которая совместно используется всеми участниками. Эта полоса пропускания может быть зарезервирована, и ее предел установлен сетью. Полоса пропускания сеанса не зависит от типа кодирования мультимедийных данных, но выбор типа кодирования может быть ограничен полосой пропускания сеанса связи. Параметр

полосы пропускания сеанса, как ожидается, будет обеспечен приложением управления сеанса, когда оно вызовет мультимедийное приложение, но мультимедийные приложения могут также устанавливать значение по умолчанию, основанное на полосе пропускания данных с единственным отправителем для типа кодирования, выбранного для данного сеанса.

Вычисления полосы пропускания для трафика управления и данных выполняются с учетом нижележащих протоколов транспортного и сетевого уровней (например, UDP и IP). Заголовки уровня звена передачи данных (ЗПД) при вычислениях не учитываются, так как пакет по мере его передачи может инкапсулироваться с различными заголовками уровня ЗПД.

Трафик управления должен быть ограничен малой и известной частью полосы пропускания сеанса: малой настолько, чтобы не пострадала основная функция транспортного протокола - передача данных; известной так, чтобы трафик управления мог быть включен в спецификацию полосы пропускания, данную протоколу резервирования ресурсов, и так, чтобы каждый участник мог независимо вычислить свою долю. Предполагается, что часть полосы пропускания сеанса, выделяемая для RTCP, должна быть установлена равной 5 %. Все участники сеанса должны использовать одинаковую величину полосы пропускания RTCP, так, чтобы вычисленные значения интервала передачи пакетов управления были одинаковыми. Поэтому эти константы должны быть установлены для каждого профиля.

Алгоритм вычисления интервала между посылками составных пакетов RTCP для разделения среди участников полосы пропускания, выделенной для трафика управления, имеет следующие основные характеристики:

- отправители коллективно используют, по крайней мере, 1/4 полосы пропускания трафика управления так, как в сеансах с большим количеством получателей, но с малым числом отправителей; едва установив соединение, участники в течение короткого интервала времени получают CNAME передающих сайтов;
- требуется, чтобы расчетный интервал между пакетами RTCP, как минимум, превышал 5 секунд, чтобы избежать пачек пакетов RTCP, превышающих дозволенную полосу пропускания, когда число участников мало и трафик не сглаживается согласно закону больших чисел;
- интервал между пакетами RTCP изменяется случайно в пределах от половины до полутора расчетных интервалов во избежание непреднамеренной синхронизации всех участников. Первый пакет RTCP, посланный после вступления в сеанс связи, также задерживается случайным образом (до половины минимума интервала RTCP) в случае, если приложение начато во множестве сайтов одновременно, например, при объявлении о начале сеанса связи;
- для автоматической адаптации к изменениям в объеме передаваемой информации управления вычисляется динамическая оценка среднего

размера составного пакета RTCP с использованием всех полученных и посланных пакетов;

- этот алгоритм может использоваться для сеансов, в которых передача пакетов допустима для всех участников. В этом случае параметр полосы пропускания сеанса - это произведение полосы пропускания индивидуального отправителя на число участников, и полоса пропускания RTCP составляет 5 % от этой величины.

Взаимодействие RTP с протоколами сетевого и транспортного уровней

Если не установлено иначе спецификациями других протоколов, то при передаче "голосовых" пакетов применяются следующие основные правила.

Протокол RTP полагается на протоколы нижележащих уровней при обеспечении разделения потоков данных RTP и управляющей информации RTCP. Для протокола UDP и подобных ему протокол RTP использует четный номер порта, а соответствующий поток RTCP - порт с номером на единицу большим.

Информационные пакеты RTP не содержат никакого поля длины, следовательно, RTP полагается на нижележащий протокол и для обеспечения индикации длины. Максимальная длина пакетов RTP ограничивается только протоколами нижележащих уровней.

В одном блоке данных протокола нижележащего уровня, например, в пакете UDP, могут передаваться несколько пакетов протокола RTP. Это позволяет уменьшить избыточность заголовков и упростить синхронизацию между различными потоками.

2.4. Принципы построения протокола SIP

Протокол инициирования сеансов (Session Initiation – SIP) является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи (например, мультимедийных конференций, телефонных соединений). Пользователи могут принимать участие в существующих сеансах связи, приглашать других пользователей и быть приглашенными ими к новому сеансу связи.

Протокол SIP разработан группой MMUSIC комитета IETF, а спецификации протокола представлены в документе RFC 2543. В основу протокола заложены следующие принципы:

- *Персональная мобильность пользователей.* Пользователи могут перемещаться без ограничений в пределах сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится.
- *Масштабируемость сети.* Она характеризуется, в первую очередь, возможностью увеличения количества элементов сети при ее расширении. Серверная структура сети, построенная на базе протокола SIP, отвечает этому требованию.

- *Расширяемость протокола.* Она характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.
    - Расширение функций протокола SIP может быть произведено за счет введения новых заголовков сообщений, которые должны быть зарегистрированы в организации IANA. При этом если SIP-сервер принимает сообщение с неизвестными ему атрибутами, то он просто игнорирует их.
    - Для расширения возможностей протокола SIP могут быть также добавлены и новые типы сообщений.
- Интеграция в стек существующих протоколов Интернета, разработанных IETF. Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной IETF. Эта архитектура включает в себя также и другие протоколы: резервирования ресурсов (Resource Reservation Protocol – RSVP, RFC 2205), транспортный протокол реального времени (Real-Time Transport Protocol – RTP, RFC 1889), протокол передачи потоковой информации в реальном времени (Real-Time Streaming Protocol – RTSP, RFC 2326), протокол описания параметров связи (SDP, RFC 2327). Однако функции самого протокола SIP не зависят ни от одного из этих протоколов.
- Взаимодействие с другими протоколами сигнализации. Протокол SIP может быть использован совместно с протоколом H.323.

2.4.1. Интеграция протокола SIP с IP-сетями

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. Но в то же время предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDP. Следует оговориться, что для этого необходимо создать дополнительные механизмы надежной доставки сигнальной информации. К таким механизмам относятся повторная передача информации при ее потере, подтверждение приема и др. На рис. 2.2. показано место, занимаемое протоколом SIP в стеке протоколов TCP/IP

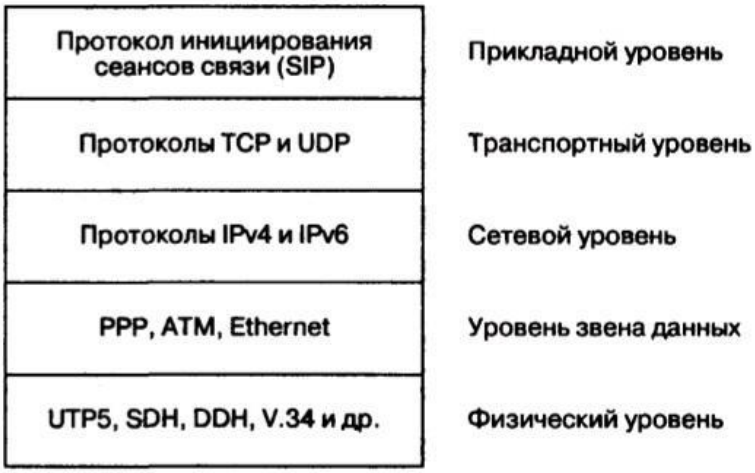

Рис. 2.2. Место протокола SIP в стеке протоколов TCP/IP

Сигнальные сообщения могут переноситься как протоколом транспортного уровня UDP, так и протоколом TCP. Протокол UDP позволяет быстрее, чем TCP, доставлять сигнальную информацию (даже с учетом повторной передачи неподтвержденных сообщений), а также вести параллельный поиск местоположения пользователей и передавать приглашения к участию в сеансе связи в режиме многоадресной рассылки. В свою очередь, протокол TCP упрощает работу с межсетевыми экранами (firewall), а также гарантирует надежную доставку данных. При использовании протокола TCP разные сообщения, относящиеся к одному вызову, могут либо передаваться по одному TCP-соединению, либо для каждого запроса и ответа на него может открываться отдельное TCP-соединение.

.По сети с маршрутизацией пакетов IP может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация. При организации связи между терминалами пользователей необходимо сообщить встречной стороне, какого рода информация может приниматься (передаваться), алгоритм ее кодирования и адрес, на который следует передавать информацию.

Таким образом, одним из обязательных условий организации связи при помощи протокола SIP является обмен между абонентами данными об их функциональных возможностях. Для этой цели чаще всего используется протокол описания сеансов связи – SDP (Session Description Protocol). Поскольку в течение сеанса связи может производиться его модификация, предусмотрена передача сообщений SIP с новыми описаниями сеанса средствами SDP.

Для передачи речевой информации комитет IETF предлагает использовать протокол RTP, рассмотренный выше, но сам протокол SIP не исключает возможность применения для этих целей и других протоколов.

Протокол SIP предусматривает организацию конференций трех видов:

- в режиме многоадресной рассылки (multicasting), когда информация передается на один multicast-адрес, откуда затем доставляется сетью конечным адресатам;
- при помощи контроллера управления конференции (MCU), к которому участники конференции передают информацию в режиме "точка-точка", а контроллер обрабатывает информацию (смешивает или коммутирует) и рассылает ее участникам конференции;
- путем соединения каждого пользователя с каждым в режиме "точка-точка".

Протокол SIP дает возможность присоединения новых участников к уже существующему сеансу связи, то есть двусторонний сеанс может перейти в конференцию.

2.4.2. Адресация

Для организации взаимодействия с существующими приложениями IP-сетей и для обеспечения мобильности пользователей протокол SIP использует адрес, подобный адресу электронной почты. В качестве адресов рабочих станций

используются специальные универсальные указатели ресурсов – так называемые SIP URL (Universal Resource Locators). Такие SIP-адреса бывают четырех типов:

```
имя@домен;
имя@хост;
имя@IP-адрес;
№телефона@шлюз.
```

и состоят из двух частей.

- Первая часть – это имя пользователя, зарегистрированного в домене или на рабочей станции. Если вторая часть адреса идентифицирует какой-либо шлюз, то в первой указывается телефонный номер абонента.
- Во второй части адреса указывается имя домена, рабочей станции или шлюза. Для определения IP-адреса устройства необходимо обратиться к службе доменных имен (DNS). Если же во второй части SIP-адреса размещается IP-адрес, то с рабочей станцией можно связаться напрямую.

В начале каждого SIP-адреса ставится слово "sip:", указывающее, что это именно SIP-адрес. Примеры SIP-адресов:

```
sip: als@rts.loniis.ru
sip: user1@192.168.100.152
sip: 294-75-47@gateway.ru
```

2.4.3. Архитектура сети SIP

На рис. 2.3 представлена упрощенная схема действия протокола.

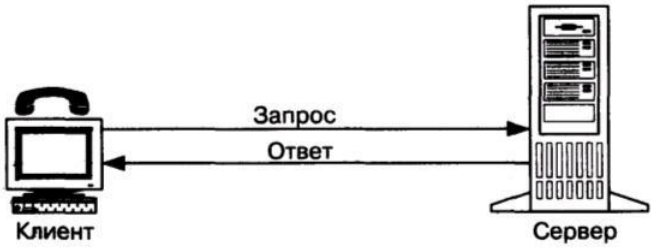

Рис. 2.3. Архитектура "клиент-сервер"

Клиент выдает запросы, в которых указывает, что он желает получить от сервера. Сервер принимает запрос, обрабатывает его и выдает ответ, который может содержать уведомление об успешном выполнении запроса, уведомление об ошибке или информацию, затребованную клиентом.

Управление процессом обслуживания вызова распределено между разными элементами сети SIP. Основным функциональным элементом, реализующим функции управления соединением, является терминал. Остальные элементы сети отвечают за маршрутизацию вызовов, а в некоторых случаях предоставляют дополнительные услуги. В протоколе SIP устанавливаются следующие основные компоненты:

- *Терминал.*

  В случае, когда клиент и сервер взаимодействуют непосредственно с пользователем, они называются, соответственно, клиентом агента

пользователя – User Agent Client (UAC) и сервером агента пользователя - User Agent Server (UAS).

- *Прокси-сервер.*

  Прокси-сервер принимает запросы, обрабатывает их и, в зависимости от типа запроса, выполняет определенные действия. Это может быть поиск и вызов пользователя, маршрутизация запроса, предоставление услуг и так далее. Прокси-сервер состоит из клиентской и серверной частей, поэтому может принимать вызовы, инициировать собственные запросы и возвращать ответы. Прокси-сервер может быть физически совмещен с сервером определения местоположения или существовать отдельно от него. Используют два типа прокси-серверов – с сохранением состояний (stateful) и без сохранения состояний (stateless).

  Сервер первого типа хранит в памяти входящий запрос, который явился причиной генерации одного или нескольких исходящих запросов. Эти исходящие запросы сервер также запоминает. Все запросы хранятся в памяти сервера только до окончания транзакции, т. е. до получения ответов на запросы.

  Он позволяет предоставить большее количество услуг, но работает медленнее, чем сервер второго типа. Он может применяться для обслуживания небольшого количества клиентов, например, в локальной сети. Прокси-сервер должен сохранять информацию о состояниях, если он:

  - использует протокол TCP для передачи сигнальной информации;
  - работает в режиме многоадресной рассылки сигнальной информации;
  - размножает запросы.

  Последний случай имеет место, когда прокси-сервер ведет поиск вызываемого пользователя сразу в нескольких направлениях, т. е. один запрос, который пришел к прокси-серверу, размножается и передается одновременно по всем этим направлениям.

  Сервер второго типа просто ретранслирует запросы и ответы, которые получает. Он работает быстрее, чем сервер первого типа, так как ресурс процессора не тратится на запоминание состояний, вследствие чего сервер этого типа может обслужить большее количество пользователей. Недостатком такого сервера является то, что на его базе можно реализовать лишь наиболее простые услуги. Впрочем, прокси-сервер может функционировать как сервер с сохранением состояний для одних пользователей и как сервер без сохранения состояний – для других.

  Алгоритм работы пользователей с прокси-сервером выглядит следующим образом.

  - Поставщик услуг IP-телефонии сообщает адрес прокси-сервера своим пользователям.

- Вызывающий пользователь передает к прокси-серверу запрос соединения.
- Сервер обрабатывает запрос, определяет местоположение вызываемого пользователя и передает запрос этому пользователю, а затем получает от него ответ, подтверждающий успешную обработку запроса, и транслирует этот ответ пользователю, передавшему запрос.

Прокси-сервер может модифицировать некоторые заголовки сообщений, которые он транслирует, причем каждый сервер, обработавший запрос в процессе его передачи от источника к приемнику, должен указать это в SIP-запросе для того, чтобы ответ на запрос вернулся по такому же пути.

- *Сервер переадресации.*

  Сервер переадресации предназначен для определения текущего адреса вызываемого пользователя. Вызывающий пользователь передает серверу сообщение с известным ему адресом вызываемого пользователя, а сервер обеспечивает переадресацию вызова на текущий адрес этого пользователя. Для реализации этой функции сервер переадресации должен взаимодействовать с сервером определения местоположения.

- *Сервер определения местоположения пользователей.*

  Пользователь может перемещаться в пределах сети, поэтому необходим механизм определения его местоположения в текущий момент времени.

  Для хранения текущего адреса пользователя служит сервер определения местоположения пользователей, представляющий собой базу данных адресной информации. Кроме постоянного адреса пользователя, в этой базе данных может храниться один или несколько текущих адресов.

  Этот сервер может быть совмещен с прокси-сервером или быть реализован отдельно от прокси-сервера, но иметь возможность связываться с ним.

3. IP-ТЕЛЕФОНИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ

IP-телефония (или *VoIP – Voice over Internet protocol*) – технология, которая использует сеть с пакетной коммутацией сообщений на базе протокола IP для передачи голоса в режиме реального времени.

- При разговоре голосовые сигналы преобразуются в пакеты данных.
- Затем они сжимаются и посылаются через Интернет приемной стороне.
- При поступлении к адресату, они декодируются в аналоговый голосовой сигнал.

Таким образом, IP-телефония представляет собой линию для передачи голоса, используя для этого специально выделенные цифровые каналы. Она привлекает к себе особенное внимание ввиду того, что позволяет:

- Существенно снизить затраты на традиционные телефонные разговоры, в особенности на междугородние и международные звонки.
- Также намного меньше затраты на инвестиции в оборудование. Высокие затраты телефонных компаний приводят к дорогим междугородным разговорам.
- Выделенное подключение (т. е. постоянный доступ к телефонной связи с телефонной станции) требует избыточной производительности за счет времени простоя в течение речевого сеанса. В таких случаях приходится оплачивать и то время, когда мы не используем телефонную линию.

3.1. Особенности IP-телефонии

В отличие от аналоговой телефонии, IP-телефония создает "подключение по запросу" и не имеет зарезервированных линий связи, что уменьшает затраты на телефонные разговоры.

Она частично использует существующие сети закрепленных за абонентами телефонных линий. Но в них она дополнительно применяет прогрессивную технологию *сжатия передаваемых сигналов*, которая более полно использует емкость телефонных линий.

- При обычной аналоговой телефонии используется канал пропускной способностью 64 Кбит/с независимо от того, разговаривает абонент или молчит во время соединения.
- В случае передачи речи по IP-сетям, за счет оцифровки и сжатия, речь в канал передается в виде цифровой информации. Причем, если абонент молчит или делает паузы в разговоре, цифровая информация в канал не передается и канал не заполняется.
- Это позволяет в одном канале 64 Кбит/с одновременно передавать от 8 и более соединений, что приводит к снижению тарифов, и, соответственно, к уменьшению счетов за оплату разговоров.

Кроме этого, IP-телефония привлекает и дополнительными возможностями, такими как *совмещенный доступ в Интернет*. Голосовые данные, факсимильные сообщения передаются уже с используемым набором IP-протоколов Интернета.

Таким образом, голосовая информация и обычные данные могут передаваться по одной и той же сети. Это означает, что клиенты получают дополнительную полезную функцию от используемой сети, которая сочетает в себе свойства сети передачи обычных данных и телефонной сети.

По сути это означает, что, имея компьютерную сеть, можно "наложить" на нее телефонию, и голосовой трафик этой сети будет передаваться по тем же каналам, что и данные (рис. 3.1). Доступ в Интернет становится более универсальным.

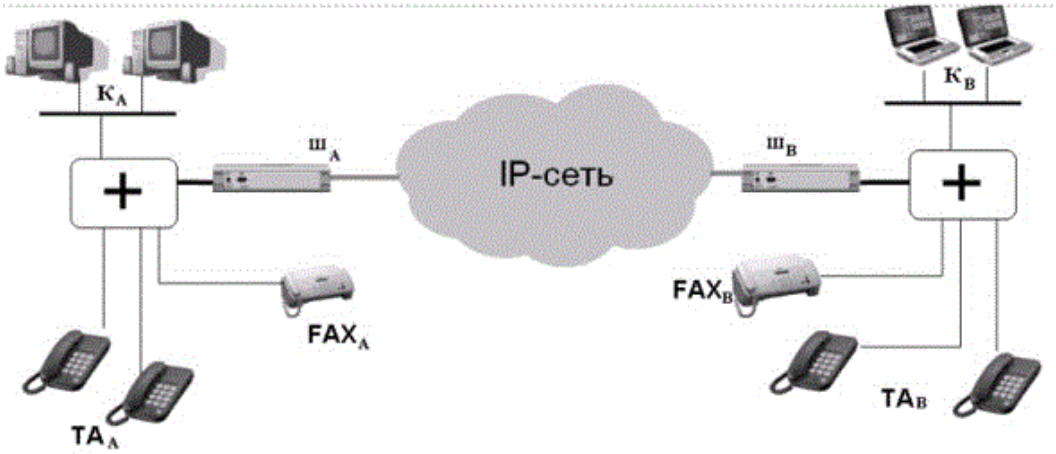

Рис. 3.1. Компьютерная сеть с наложенной на нее IP-телефонией

На данном рисунке использованы следующие обозначения:

- $К_А$, $К_В$ – компьютеры абонентов А и В соответственно.
- $Ш_А$ и ШВ – шлюзы абонентов А и В.
- $ТА_А$, $ТА_В$ и $FAX_А$, $FAX_В$ – телефоны и телефаксы абонентов А и В.

Еще одной важной особенность VoIP является их открытая архитектура. Положительным свойством VoIP является и наличие общих для IP-телефонии протоколов, таких как: H.323 (набор стандартов для передачи мультимедиа), MGCP (Media Gateway Control Protocol – протокол контроля медиашлюзов), SIP (Session Initiation Protocol — протокол установления сеанса) и т. д.

3.2. Принципы пакетной передачи

Для проведения сеанса связи мы набираем номер вызываемого абонента, после чего происходит соединение с сетевым шлюзом, как показано на рис. 3.2.

Рис. 3.2. Соединение с сетевым шлюзом

Голосовое сообщение абонента А с помощью микрофона преобразуется в электрический аналоговый сигнал, который претерпевает ряд преобразований

(кодируется). Внутри шлюза происходит оцифровка голосового сигнала, как условно показано на рис. 3.3.

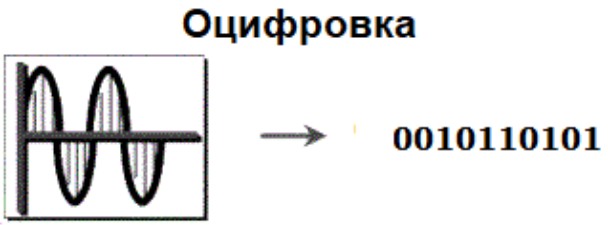

Рис. 3.3. Оцифровка голосового сигнала

После оцифровки цифровой сигнал, занимающий изначально, как и речь, канал в 64 Кбит/с, сжимается выбранным кодеком (рис. 3.4)

Рис. 3.4. Сжатие канала

и разбивается на пакеты в соответствии с выбранным типом кодирующего устройства (кодеком). В этом преобразовании участвуют как аппаратные, так и программные средства со стороны абонента А (рис. 3.5).

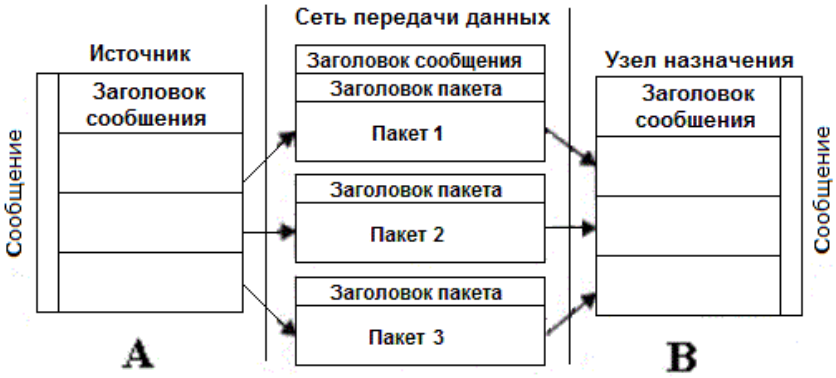

Рис. 3.5. Разбиение на пакеты

Сжатые данные отправляются в сеть. Абонент В имеет аналогичный набор устройств, производящих преобразования в обратном порядке.

Рис. 3.6. Соединение с приемной стороной

Пакеты из сети поступают в телефонный шлюз, подключенный к телефонной линии (рис. 3.6), и все операции повторяются в обратном порядке, то есть осуществляется декодирование цифрового сигнала и преобразование его в аналоговую форму, которая приводит в действие звуковой динамик.

Этапы преобразования сигналов и передачи выполняются за малые доли секунды, практически в реальном масштабе времени, что позволяет обеспечить дуплексный (двухсторонний) характер ведения разговора.

Архитектура технологии VoIP упрощенно может быть представлена в виде двух слоев или плоскостей:

- Верхний слой – это программные средства управления обслуживанием вызовов.
- Нижний слой – это базовая сеть с маршрутизацией IP пакетов, которая представляется комбинацией взаимосвязанных протоколов Интернета:
  - Это протокол RTP (Real Time Transport Protocol), который функционирует поверх протокола UDP (User Datagram Protocol),
  - При этом протокол UDP, в свою очередь, расположен в стеке протоколов TCP/IP над протоколом IP.

Основное назначение RTP в том, что он присваивает каждому исходящему пакету временные метки, которые обрабатываются на приемной стороне. Это позволяет принимать данные в надлежащем порядке, снижает влияние неравномерности времени прохождения пакетов по сети, восстанавливает синхронизацию между аудио и видео данными.

Таким образом, иерархия протоколов RTP/UDP/IP представляет собой своего рода *транспортный механизм* для речевого трафика. Отметим, что в сетях с маршрутизацией пакетов IP для передачи данных всегда предусматриваются механизмы повторной передачи пакетов в случае их потери.

При передаче голосовой информации в реальном масштабе времени этот прием неприменим. Речевая информация очень чувствительна к задержкам, но менее чувствительна к потерям, поэтому для передачи речи (как и видеоинформации) используется механизм *негарантированной доставки* информации RTP/UDP/IP. Рекомендации ITU-T допускают задержки в одном направлении, не превышающие 150 мс.

Как уже было сказано, верхний слой архитектуры VoIP управляет обслуживанием запросов связи, то есть адресацией, куда вызов должен быть направлен, и способом, каким должно быть установлено соединение между абонентами. Инструмент такого управления - телефонные системы сигнализации.

3.3. Виды соединений и взаимодействие с компьютерной сетью

Можно выделить три наиболее часто используемых сценария IP-телефонии:

- компьютер-компьютер;
- телефон-компьютер;
- телефон-телефон.

Первый сценарий "компьютер-компьютер" реализуется на базе стандартных компьютеров, оснащенных средствами мультимедиа и подключенных к сети Интернет. Компоненты этого сценария представлены на Рис. 3.7.

При этом сценарии аналоговые речевые сигналы, поступившие от микрофона абонента А, преобразуются в цифровую форму с помощью аналого-цифрового

преобразователя (АЦП). Отсчеты речевых данных в цифровой форме затем сжимаются кодирующим устройством для сокращения нужной для их передачи полосы в отношении 4:1, 8:1 или 10:1.

Выходные данные после сжатия формируются в пакеты, к ним добавляются заголовки протоколов, и затем пакеты передаются через IP-сеть в систему IP-телефонии, обслуживающую абонента Б. Когда пакеты принимаются системой абонента Б, заголовки протокола удаляются, а сжатые речевые данные поступают в устройство, развертывающее их в первоначальную форму, после чего речевые данные снова преобразуются в аналоговую форму с помощью цифро-аналогового преобразователя (ЦАП) и попадают в динамик телефона абонента Б.

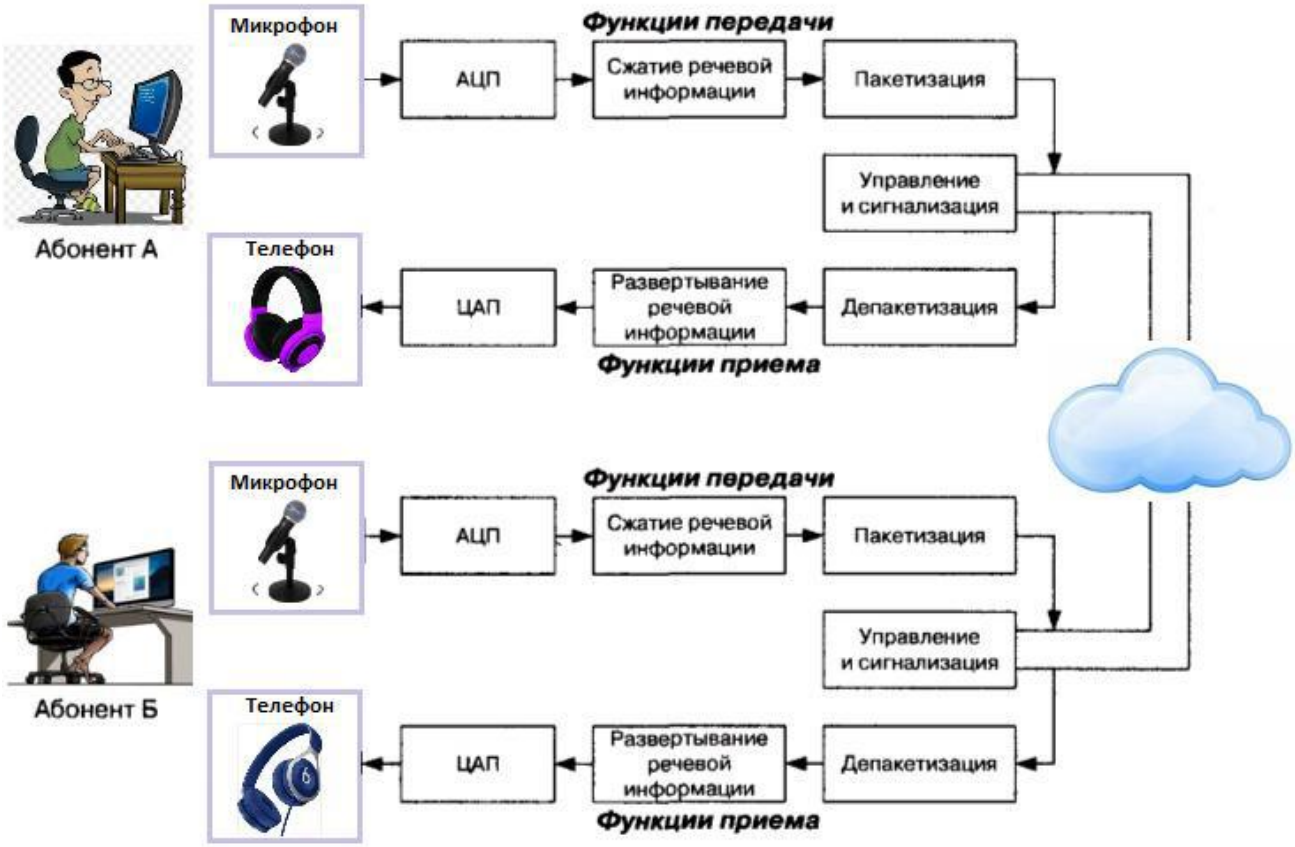

Рис. 3.7. Сценарий IP-телефонии "компьютер-компьютер"

Для обычного соединения между двумя абонентами системы IP-телефонии на каждом конце одновременно реализуют как функции передачи, так и функции приема. Под IP-сетью подразумевается либо глобальная сеть Интернет, либо корпоративная сеть предприятия Intranet.

Рассмотрим представленный на рис. 3.7 сценарий установления соединения более подробно. Для проведения телефонных разговоров друг с другом абоненты А и Б должны иметь доступ к Интернету или к другой сети с протоколом IP. Разберем возможный алгоритм организации связи между этими абонентами на примере протокола H.323.

- Абонент А запускает свое приложение IP-телефонии, поддерживающее протокол H.323.
- Абонент Б ранее уже запустил свое приложение IP-телефонии, которое поддерживающее протокол H.323.

- Абонент А, зная DNS имя абонента Б, вводит это имя в раздел "кому позвонить" в своем приложении IP-телефонии и нажимает кнопку Return.
- Приложение IP-телефонии обращается к DNS-серверу (который в данном примере реализован непосредственно в персональном компьютере абонента А) для того, чтобы преобразовать доменное имя абонента Б в IP-адрес.
- Сервер DNS возвращает IP-адрес абонента Б.
- Приложение IP-телефонии абонента А получает IP-адрес абонента Б и отправляет по этому адресу сигнальное сообщение “H.225 Setup”.
- При получении сообщения “H.225 Setup” приложение Б сигнализирует абоненту Б о входящем вызове.
- Абонент Б принимает вызов и приложение IP-телефонии отправляет ответное сообщение “H.225 Connect”.
- Приложение IP-телефонии у абонента А начинает взаимодействие с приложением у абонента Б в соответствии с рекомендацией H.245.
- После окончания взаимодействия по протоколу H.245 и открытия логических каналов абоненты А и Б могут разговаривать друг с другом через IP-сеть.

При этом блок "Управление и сигнализация" управляет пакетизацией и депакетизацией передаваемых фрагментов, а также осуществляет контроль при их передаче.

В приведенном примере не показаны некоторые служебные детали, которые необходимы поставщику услуг для развертывания сети IP-телефонии. Так, например, для поддержки сценария "компьютер-компьютер" поставщику услуг Интернет необходимо иметь отдельный сервер (GateKeeper), преобразующий имена пользователей в динамические адреса IP.

Надо отметить, что и сам сценарий "компьютер-компьютер" ориентирован на пользователя, которому сеть нужна в основном для передачи данных, а программное обеспечение IP-телефонии требуется лишь иногда для разговоров с коллегами.

Эффективное использование телефонной связи по сценарию "компьютер-компьютер" обычно связано с повышением продуктивности работы крупных компаний, например, при организации виртуальной презентации в корпоративной сети с возможностью не только видеть документы на Web-сервере, но и обсуждать их содержание с помощью IP-телефона.

Другие сценарии IP-телефонии

Ранее мы уже отмечалось, что наряду со сценарием "компьютер-компьютер" в сети используют и другие варианты сценариев IP-телефонии. При их описании в этом разделе далее вместо громоздкого изображения компонентов оконечного устройства будет использован упрощенный вид терминала IP-телефонии.

В качестве аналога Рис. 3.7 будет использоваться упрощенное представление того же сценария, которое представлено на Рис. 3.8. Что же касается процедур

аналогово-цифрового и цифро-аналогового преобразования, пакетизации, сжатия, и других, то они будут рассмотрены в последующих главах.

Рис. 3.8. Упрощенный сценарий"компьютер-компьютер"

Замена изображений имеет и более глубокий смысл. Название сценария "компьютер-компьютер" отнюдь не означает, что в распоряжении пользователя обязательно должен быть стандартный PC с микрофоном и колонками (рис. 3.8).

Главным требованием такой схемы является то, что оба пользователя должны иметь подключенные к сети персональные компьютеры – и эти PC должны быть всегда включены, подсоединены к сети и иметь в запущенном виде программное обеспечение IP-телефонии для приема входящих вызовов.

Принимая во внимание эти обстоятельства, под названием "компьютер" во всех сценариях мы будем понимать терминал пользователя, включенный в IP-сеть, а под названием "телефон" - терминал пользователя, включенный в сеть коммутации каналов любого типа: ТфОП, ISDN или GSM.

Сценарий "телефон-компьютер" находит применение в разного рода справочно-информационных службах Интернета, в службах сбыта товаров или в службах технической поддержки. Пользователь, подключившийся к Web-серверу какой-либо компании, имеет возможность обратиться к оператору справочной службы. Это вполне соответствует стилю жизни современных потребителей, связанному с потребностью в дополнительных удобствах и экономии времени.

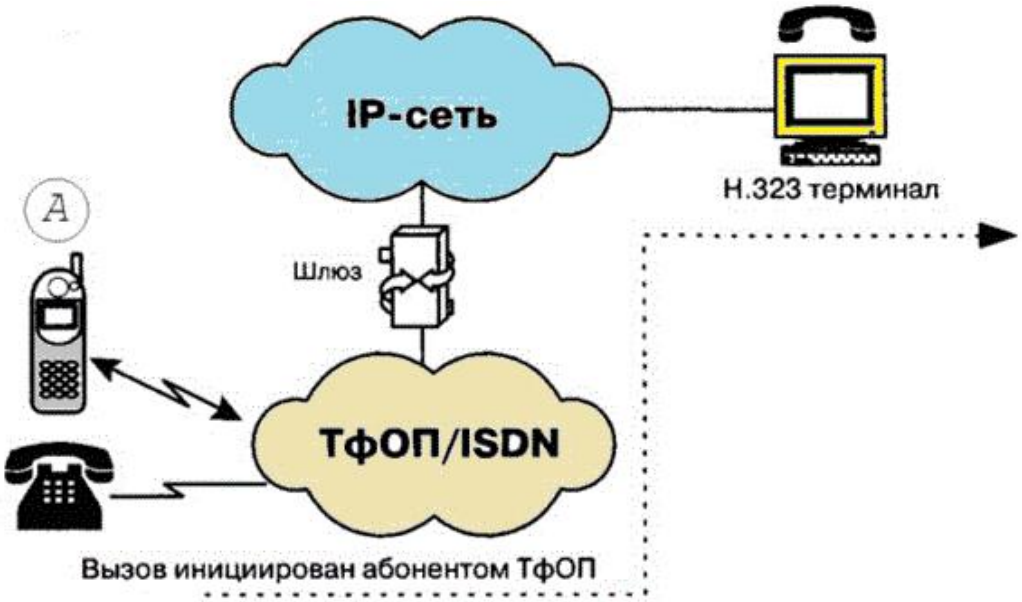

Рис. 3.9. Пользователя IP-сети вызывает абонент ТфОП по сценарию "телефон-компьютер"

При сценарии "телефон-компьютер" соединение устанавливается между пользователем телефонной сети общего пользования (ТфОП) и пользователем IP-сети (рис. 3.9). Предполагается, что установление соединения инициирует пользователь сети коммутации каналов.

- Шлюз для взаимодействия сетей ТфОП и IP может быть реализован как отдельным устройством, так и интегрированным в существующее оборудование ТфОП или IP-сети,
- Представленная на Рис. 3.9 сеть коммутации каналов может быть, как корпоративной сетью, так и сетью общего пользования.
- Возможна и иная разновидность сценария "телефон-компьютер", когда соединение устанавливается между пользователем IP-сети и абонентом ТфОП, но инициирует его создание абонент ТфОП.

Рассмотрим несколько подробнее представленной на Рис. 3.9 пример упрощенной архитектуры системы IP-телефонии по сценарию "телефон-компьютер".

- При попытке вызвать справочно-информационную службу, используя услуги пакетной телефонии и обычный телефон, на начальной фазе абонент А вызывает близлежащий шлюз IP-телефонии для минимизации затрат на услуги связи.
- От шлюза к абоненту А поступает запрос на ввод номера, к которому должен быть направлен вызов (например, номер службы), и личный идентификационный номер (PIN) для аутентификации и последующего начисления платы, если эта служба платная.
- Основываясь на вызываемом номере, шлюз определяет наиболее доступный путь к данной службе. Кроме того, шлюз активизирует свои функции.
- Разъединение с любой стороны передается противоположной стороне по протоколу сигнализации и вызывает завершение установленных соединений и освобождение ресурсов шлюза для обслуживания следующего вызова.

Эффективность объединения услуг передачи речи и данных является основным стимулом использования IP-телефонии по сценариям "компьютер-компьютер" и "телефон-компьютер", не нанося при этом ущерба интересам операторов традиционных телефонных сетей.

Сценарий соединения "телефон-телефон" в большой степени отличается от первых двух сценариев IP-телефонии своей социальной значимостью, поскольку целью его применения является предоставление обычным абонентам ТфОП альтернативной возможности междугородной или международной телефонной связи.

Как правило, обслуживание вызовов по такому сценарию предполагает, что поставщик услуг IP-телефонии подключает свой шлюз к коммутационному узлу ТфОП по сети Интернет или по выделенному каналу к аналогичному шлюзу, находящемуся в другом городе или другой стране.

- Типичная услуга IP-телефонии по этому сценарию использует обычный IP-телефон, а вместо междугороднего компонента телефонной сети задействует либо частную IP-сеть, либо сеть Интернет.
- Благодаря маршрутизации телефонного трафика по IP-сети стало возможным обходить сети общего пользования и, соответственно, не платить за междугороднюю/международную связь операторам этих сетей.

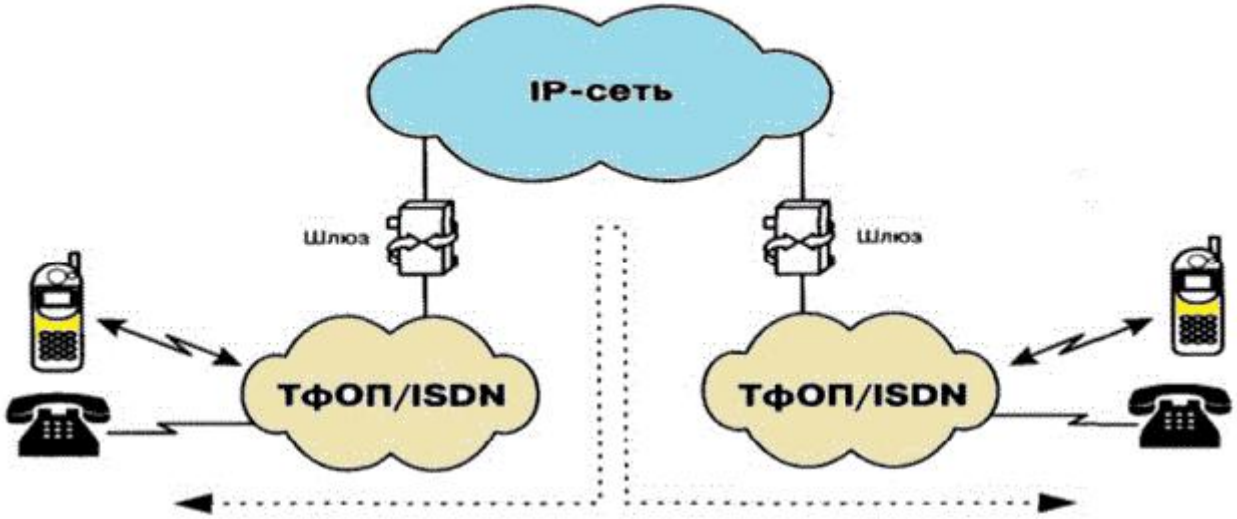

Рис. 3.10. Соединение абонентов ТфОП через транзитную IP-сеть по сценарию "телефон-телефон"

Как показано на рис. 3.10, поставщики услуг IP-телефонии предоставляют услуги "телефон-телефон" путем установки шлюзов IP-телефонии на входе и выходе IP-сетей.

- Абоненты подключаются к шлюзу поставщика услуг IP-телефонии через ТфОП, набирая специальный номер доступа.
- Абонент получает доступ к шлюзу, используя персональный идентификационный номер (PIN) или услугу идентификации номера вызывающего абонента (Calling Line Identification).
- После этого шлюз просит ввести телефонный номер вызываемого абонента, анализирует этот номер и определяет, какой шлюз имеет лучший доступ к нужному телефону.
- Как только между входным и выходным шлюзами устанавливается контакт, дальнейшее установление соединения к вызываемому абоненту выполняется выходным шлюзом через его местную телефонную сеть.

Полная стоимость такой связи будет складываться для пользователя из расценок ТфОП на связь с входным шлюзом, расценок интернет-провайдера на транспортировку данных и расценок удаленной ТфОП на связь выходного шлюза с вызванным абонентом.

Один из алгоритмов связи по сценарию "телефон-телефон" состоит в том, что пользователь, желающий позвонить в другой город, набирает номер поставщика данной услуги, затем в режиме донабора вводит идентификационный PIN-код, а после процедуры аутентификации набирает телефонный номер адресата.

3.4. Современные программные продукты для IP-телефонии

Появление IP-телефонии стало важным этапом все еще продолжающейся революции в сфере телекоммуникаций. Эта технология бросила вызов господству традиционной стационарной связи. Популяризация таких сервисов как Skype вызвала настоящий “бум” на рынке программного обеспечения для VoIP. Постоянно создаются новые приложения, позволяющие “обойти” традиционные телефонные сети и совершать звонки посредством Интернета.

Преимущества использования программ для IP-телефонии оценили миллионы людей во всем мире, из самых разных слоев общества. Ниже дается краткое описания наиболее распространенных программных продуктам, работающим в среде VoIP.

Ekiga – этот программный продукт представляет собой бесплатный софтфон с открытым кодом, поддерживающий платформы Linux и Windows. К числу основных его характеристик следует отнести:

- Поддержка наиболее популярных протоколов – SIP, H323, STUN;
- Возможность мгновенного обмена сообщениями;
- Функция переадресации вызова;
- Переброс беседы на другой терминал;
- Проведение видеоконференций.

Рис. 3.11. Вид интерфейса программы Ekiga.

Она является свободным программным обеспечением, и распространяется в соответствии с условиями в GNU (General Public License). В дистрибутиве Ubuntu Ekiga (www.ekiga.org) используется в качестве приложения для IP-телефонии и проведения видеоконференций. Полностью совместима с другими приложениями SIP и Microsoft NetMeeting. Поддерживает большинство высококачественных аудио и видео кодеков. Программа переведена на русский язык.

MicroSIP – представляет собой программу, позволяющую осуществлять вызовы с применением протокола SIP. Несмотря на то, что это небольшой, “портативный” клиент, он отличается хорошей функциональностью и более удобен для пользователя, в сравнении с масштабным ПО типа Skype. Помимо голосового общения, MicroSIP обеспечивает следующие возможности:

- Мгновенные сообщения;
- Видео-вызовы;
- Статус присутствия;
- P2P соединение без применения SIP-сервера.

Ventrilo – простота настройки и использования программы Ventrilo сделала ее очень популярной среди геймеров. При общении групп до 8 человек, она является бесплатной для пользователей. Основные функции:

- Конференц-связь;
- Чат;
- “Text-to-speech” (формирование голосового сигнала на основе печатного текста).

Mumble – это VoIP-приложение, поддерживающее Windows, Linux, MAC OS. Обеспечивает высокое качество звука, поскольку предусмотрена функция автоматического выравнивания звукового сигнала. Плюсы:

- Шифрование связи;
- Поддержка подключаемых модулей;
- Возможность создания списков контроля доступа.

Jitsi (SIP Communicator) – Поддерживает несколько операционных систем и интернет-протоколов. Возможности:

- Мгновенные сообщения;
- Видео-звонки;
- Шифрование вызовов и чатов;
- Удержание звонка;
- Запись вызова.

Для работы с VoIP-приложениями, так называемые софтфонами, вашему компьютеру необходима звуковая карта, колонки и микрофон. Альтернативное решение – это покупка специальной IP-гарнитуры и USB-телефона.

4. ПЕРЕДАЧА РЕЧИ ПО IP-СЕТИ

4.1. Взаимодействие протоколов VoIP

При использовании протоколов, которые непосредственно имеют дело с VoIP, важно правильное понимание спецификации, вносимой этими протоколами. На рис. 4.1 представлен стек протоколов VoIP. Здесь отсутствует верхний уровень, который подразумевает в себе любую разговорную речь. Данный рисунок характеризует исключительно передачу голосовых данных.

7.	- - - - -
6.	Уровень представления G.729 / G.711
5.	Уровень сеанса H.323 / H.323, шлюз / SIP / SDP
4.	Транспортный уровень, протоколы RTP / UDP / RSVP
3.	Сетевой уровень IP / LLQ
2.	Канальный уровень MLPPP / FR / ATM AALS
1.	Физический уровень

Рис. 4.1. Стек протоколов VoIP.

1. Технология VoIP может работать в любой *физической среде*, которая может использоваться обычным IP протоколом. Это могут быть кабели витой пары (используемой в традиционном Ethernet), телефонные провода, беспроводные соединения (протокол IEEE 802.11) и др.

2. Второй уровень этой модели, *канальный уровень*, указывает, что протокол IP для создания фреймов может использовать различные форматы. Как видно из рис. 2.1, он включает многоканальный PPP (Multilink PPP), Frame Relay (FR) и ATM. При построении сети возможны и другие варианты, поскольку передавать голос могут также Ethernet, Wi-Fi и другие технологии ЛВС.

3. На третьем, *сетевом уровне* используется IP в качестве способа передачи голоса. Однако обычный IP должен быть дополнен специальными средствами.

- Поскольку возникают проблемы с задержками, то протоколу IP требуется использовать какой-либо способ установления очередности для того, чтобы голосовым данным не пришлось ожидать передачи в условиях конкуренции с обычными данными.
- На маршрутизаторах надо использовать очередность с малой задержкой (Low-Latency queuing – LLQ) или какую-либо иную современную схему установки очередности, чтобы голосовые данные отправлялись раньше обычных данных.
- Кроме того, должны использоваться схемы маркировки (marking) с заданием приоритетов (coloring), называемые IP-приоритетами, для обеспечения того, чтобы голосовые данные рассматривались системой как более важные для первоочередной передачи, чем обычные данные.

4. Следующим уровнем является *транспортный*. Поскольку для передачи голоса используется протокол UDP, системе не хватает механизма установки очередности пакетов, чтобы пакеты доставлялись в требуемой последовательности.

- Транспортный протокол реального времени RTP (Real-Time Transport Protocol) для выполнения этого требования добавляет номер пакета в последовательности передачи и механизм расстановки временных меток.
- Также может использоваться протокол резервирования RSVP (Resource Reservation Protocol) для резервирования полосы пропускания вдоль пути следования голоса по IP-сети. Этот протокол исключает использование зарезервированной полосы пропускания пакетами обычных данных.

5. Пятый уровень модели – *сеансовый*. На сегодня сети VoIP переходят со стандарта ITU-T H.323 на другой протокол инициирования сеанса SIP (Session Initiation Protocol) и протокол описания сеанса SDP (Session Description Protocol).

6. Шестым уровнем модели является *уровень представлений*. Как определено в модели OSI, уровень представлений анализирует и интерпретирует форматы данных. В терминах передачи голоса уровень представлений обеспечивает методы кодирования и сжатия, используемые для передачи голоса.

Все уровни стека протоколов совместно применяются для того, чтобы решить проблемы *минимизации задержки* и обеспечить *требуемый порядок* следования пакетов.

4.2. Качество передачи речевой информации по IP-сети

IP-телефония является одной из областей передачи данных, где все процессы передачи информации должны происходить в режиме реального времени, и где особенно важна динамика передачи сигнала, которая обеспечивается за счет современных методов кодирования и передачи информации. В результате чего увеличивается пропускная способность каналов по сравнению с традиционными телефонными сетями.

Хорошо изучены факторы, влияющие на качество IP-телефонии. Они могут быть разделены на две категории:

- Качества IP-сети характеризуют:

  максимальная пропускная способность, *задержка* (это суммарное время передачи пакета через сеть), *джиттер* (промежуток времени между двумя последовательными пакетами) и общие *потери* пакетов в сети.

- Качества шлюза характеризуют:
  - задержка – время, необходимое цифровому сигнальному процессору DSP (Digital Signal Processor) для кодирования и декодирования речевого сигнала;
  - объем буфера джиттера для сохранения пакетов данных до тех пор, пока все пакеты не будут получены; затем можно будет передать часть речевой информации в требуемой последовательности и таким образом минимизировать джиттер;

- возможность потери пакетов – потеря пакетов при сжатии и/или передаче в оборудовании IP-телефонии;
- наличие функции подавления эха, возникающего при передаче речи по сети.

Протокол TCP может решить проблему нарушения порядка следования пакетов данных. Однако для передачи голоса используется UDP, а не TCP, применение которого в технологии VoIP обусловлено тем, что:

- У посылающего устройства перед отправкой следующих пакетов нет необходимости ожидать подтверждений от принимающего устройства.
- Данные VoIP отправляются тем же способом, который используется при отправке аудио- или видеоданных в сети Интернет.
- Потеря небольшого количества голосовых пакетов считается приемлемой и может быть компенсирована механизмом кодирования/декодирования, а также различными методами интерполяции речи, то есть посредством заполнения отсутствующих звуков с помощью DSP-технологии. Это технология цифровой обработки сигналов, которая, анализируя форму звукового колебания, может предсказать отсутствующий звук.

4.3. Задержка и меры по уменьшению ее влияния

Организация ITU-T серьезно занималась исследованием проблем, связанных с задержками при передаче голоса по сети. В результате был разработан стандарт ITU-T G.114, который рекомендует, чтобы задержка при передаче голоса в одном направлении не превышала 150 миллисекунд.

Также стандарт рекомендует рассматривать задержку от 150 до 400 мс как приемлемую, если говорящий и слушающий понимают наличие задержки и готовы с ней смириться. При задержке 400 мс и более, она становится заметной.

Для сравнения можно привести пример общение через спутник. Задержка спутниковой связи в одном направлении составляет примерно 170 мс, при этом не учитывается задержка, возникающая в устройствах, расположенных на земле. Стандарт также устанавливает, что при передаче голоса задержка более 400 мс является неприемлемой.

Возможны случаи, когда при передаче речи по IP-сети возникают задержки, которые намного больше, чем в обычных телефонных линиях. К тому же, они изменяются случайным образом. Этот факт представляет собой проблему и сам по себе, но кроме того, он еще усложняет проблему эха.

Задержка (или время запаздывания) определяется как промежуток времени, затрачиваемый на то, чтобы речевой сигнал прошел расстояние от говорящего до слушающего. Рассмотрим, что и как влияет на количественные характеристики этого промежутка времени. Можно выделить следующие причины задержек при передаче речи от источника к приемнику (рис. 4.2):

- *Задержка накопления* (алгоритмическая задержка): она обусловлена необходимостью сбора кадра речевых отсчетов, выполняемой речевым кодером. Зависит от типа речевого кодера (от 0,125 мкс до 10-20 мс).

- *Задержка обработки*: процесс кодирования и сбора закодированных отсчетов в пакеты для их передачи в сеть зависит от скорости работы процессора и используемого типа алгоритма обработки.
- *Сетевая задержка:* обусловлена физической средой и протоколами, применяемыми для передачи речевых данных, а также буферами, используемыми для удаления джиттера пакетов на приемном конце.

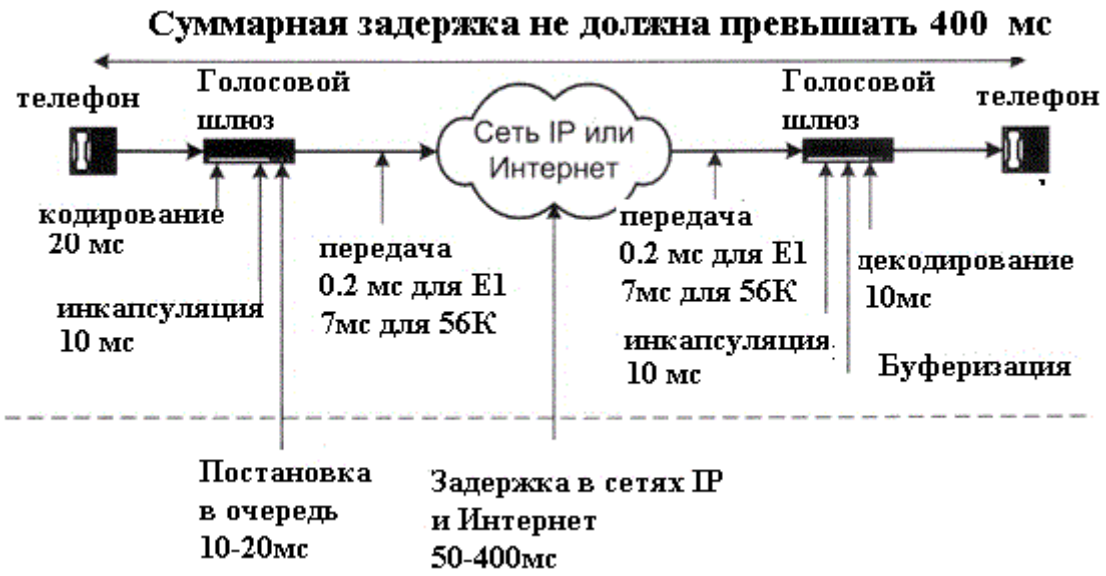

Рис. 4.2. Источники задержки при передаче речи по IP-сети

Важно отметить тот факт, что задержки в сетях с коммутацией пакетов влияют не только на качество передачи речевого трафика в реальном времени. Не менее существенно, что данные задержки в определенных ситуациях могут нарушить правильность функционирования телефонной сигнализации в цифровых трактах типа E1/T1 на стыке голосовых шлюзов с оборудованием коммутируемых телефонных сетей.

4.4. Явление джиттера и меры по уменьшению его влияния

Когда речь или данные разбиваются на пакеты для передачи через сеть, то они часто в пункт назначения прибывают в разной последовательности и в разное время. Разброс времени доставки пакетов (*джиттер*) приводит к специфическим нарушениям в передаче речи, воспринимаемый как треск и щелчки. Различают три формы джиттера:

- Джиттер, зависимый от данных (DDJ, Data Dependent Jitter) – происходит в случае ограниченной полосы пропускания или при нарушениях в сетевых компонентах.
- Искажение рабочего цикла (DCD, Duty Cycle Distortion) – обусловлено задержкой распространения между передачей снизу вверх и сверху вниз.
- Случайный джиттер (RJ, Random Jitter) – результат теплового шума.

Величины возникающих задержек и их вероятности важны для организации процедуры обработки и выбора параметров обработки. Понятно, что временная структура речевого пакетного потока меняется. Возникает необходимость применения буфера для фильтрации пакетной речи, отягощенной случайными

задержками в канале и возможными перестановками пакетов, в непрерывный естественный речевой сигнал в масштабе реального времени. Можно выделить следующие причины появления джиттера:

Влияние сети.

Время прохождения пакета через сеть неустойчиво и плохо предсказуемо. Если нагрузка сети относительно мала, маршрутизаторы и коммутаторы могут обрабатывать пакеты практически мгновенно, а линии связи бывают доступны почти всегда.

Если загрузка сети достаточно велика, пакеты могут довольно долго ожидать обслуживания в очередях. Чем больше маршрутизаторов, коммутаторов и линий в маршруте, по которому проходит пакет, тем больше время его запаздывания и тем больше вариация этого времени, то есть джиттер.

Влияние операционной системы.

Большинство приложений IP-телефонии (особенно клиентских) представляет собой обычные программы, выполняемые в среде какой-либо ОС, например, Windows или Linux. Эти программы обращаются к периферийным устройствам (платам обработки речевых сигналов) через интерфейс прикладных программ для взаимодействия с драйверами этих устройств, а доступ к IP-сети осуществляют через Socket-интерфейс.

Большинство операционных систем не могут контролировать распределение времени центрального процессора между разными процессами с точностью, превышающей несколько десятков миллисекунд, и не могут обрабатывать за такое же время более одного прерывания от внешних устройств. Это приводит к тому, что задержка в продвижении данных между сетевым интерфейсом и внешним устройством речевого вывода составляет, независимо от используемого алгоритма кодирования речи, величину такого же порядка или даже больше.

Из сказанного следует, что выбор ОС является фактором, влияющим на общую величину задержки. Чтобы минимизировать влияние операционной системы, некоторые производители шлюзов и IP-телефонов применяют так называемые ОС реального времени (VxWorks, pSOS, QNX Neutrino и т. д.), которые используют более сложные механизмы разделения времени процессора, действующие таким образом, чтобы обеспечивать более быструю реакцию на прерывания и более эффективный обмен потоками данных между процессами.

Другой, более плодотворный подход – это переложить все функции, которые необходимо выполнять в жестких временных рамках (обмен данными между речевыми кодеками и сетевым интерфейсом, поддержку RTP и т. д.), на отдельный быстродействующий специализированный процессор.

При этом пересылка речевых данных осуществляется через выделенный сетевой интерфейс, а ОС рабочей станции поддерживает только алгоритмы управления соединениями и протоколы сигнализации, то есть задачи, для выполнения которых жестких временных рамок не требуется. Этот подход реализован в платах для приложений IP-телефонии, производимых фирмами Dialogic, Audiocodes, Natural Microsystems.

Влияние джиттер-буфера.

Проблема джиттера весьма существенна в пакетно-ориентированных сетях. Отправитель речевых пакетов передает их через фиксированные промежутки времени (например, через каждые 20 мс), но при прохождении через сеть задержки пакетов оказываются неодинаковыми, так что они прибывают в пункт назначения через разные промежутки времени. Это иллюстрирует рис. 4.3.

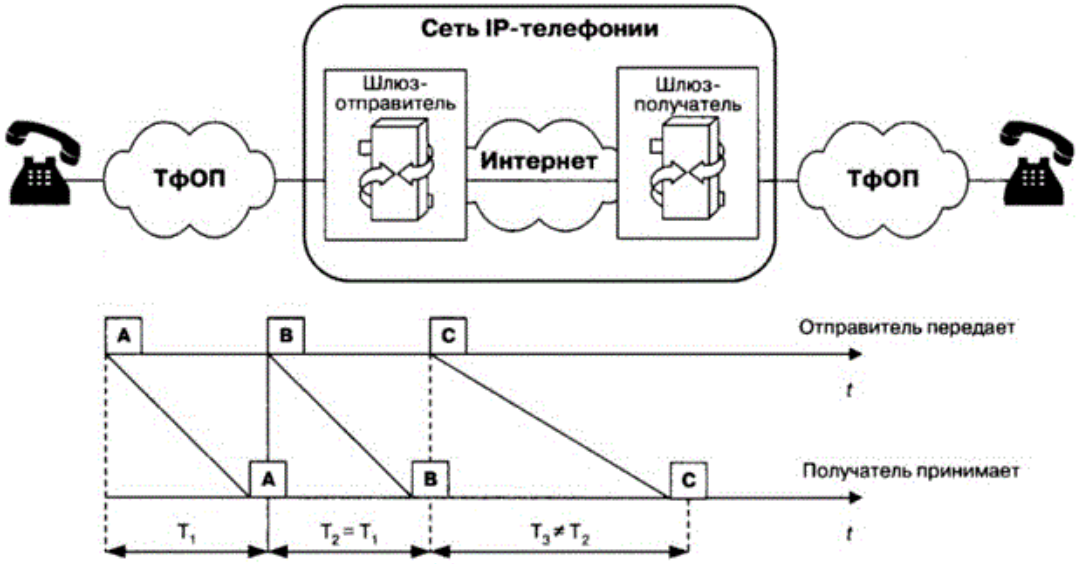

Рис. 4.3. Различие интервалов между моментами прибытия пакетов (джиттер)

Задержка прохождения пакетов по сети (Ti) может быть представлена как сумма постоянной составляющей Ts (время распространения плюс средняя длительность задержки в очередях) и переменной величины j, являющейся результатом джиттера: $Ti = Ts \pm j$.

Для компенсации влияние джиттера, на приемной стороне используется так называемый джиттер-буфер. Он хранит в памяти прибывшие пакеты в течение времени, определяемого его объемом. Пакеты, прибывающие слишком поздно, когда буфер заполнен, отбрасываются.

- Интервалы между пакетами восстанавливаются на основе значений временных меток RTP-пакетов. В функции джиттер-буфера обычно входит и восстановление исходной очередности следования пакетов, если при транспортировке по сети они оказались "перепутаны".
- Слишком короткий буфер будет приводить к слишком частым потерям "опоздавших" пакетов, а слишком длинный – к неприемлемо большой дополнительной задержке.

Обычно предусматривается динамическая подстройка длины буфера в течение всего времени существования соединения. Для выбора наилучшей длины используются эвристические алгоритмы.

Влияние кодека и количества передаваемых в пакете кадров.

Большинство современных алгоритмов кодирования/декодирования речи ориентировано на передачу информации кадрами, а не последовательностью кодов отдельных отсчетов. Поэтому в течение времени, определяемого длиной

кадра кодека, должна накапливаться определенной длины последовательность цифровых представлений отсчетов. Кроме того, некоторым кодекам необходим предварительный анализ большего количества речевой информации, чем должно содержаться в кадре. Это неизбежное время накопления и предварительного анализа входит в общий бюджет длительности задержки пакета.

На первый взгляд кажется, что чем меньше длина кадра, тем меньше должна быть задержка. Однако из-за значительного объема служебной информации, передаваемой в RTP/UDP/IP-пакетах, передача маленьких порций данных очень неэффективна, так что при применении кодеков с малой длиной кадра приходится упаковывать несколько кадров в один пакет. Кроме того, кодеки с большей длиной кадра более эффективны, поскольку могут "наблюдать" сигнал в течение большего времени и, следовательно, могут более эффективно моделировать этот сигнал.

4.5. Принципы кодирования речи

При переходе от аналоговых сетей связи к цифровым встала необходимость в преобразовании аналогового электрического сигнал в цифровой формат на передающей стороне, то есть *закодировать*, и затем после приема перевести его обратно в аналоговую форму, то есть *декодировать*.

Цель любой системы кодирования заключается в том, чтобы получить такую цифровую последовательность, которая

- во-первых, требует минимальной скорости передачи по сети,
- во-вторых, цифровую последовательность, из которой декодер может восстановить исходный речевой сигнал с минимальными искажениями.

При преобразовании речевого сигнала в цифровую форму, так или иначе, всегда имеют место два процесса (рис. 4.4):

- *дискретизация* (sampling) по времени, то есть формирование дискретных во времени отсчетов амплитуды сигнала,
- и *квантование* по уровню – дискретизация полученных отсчетов по амплитуде, то есть кодирование непрерывной величины (амплитуды) числом с конечной точностью.

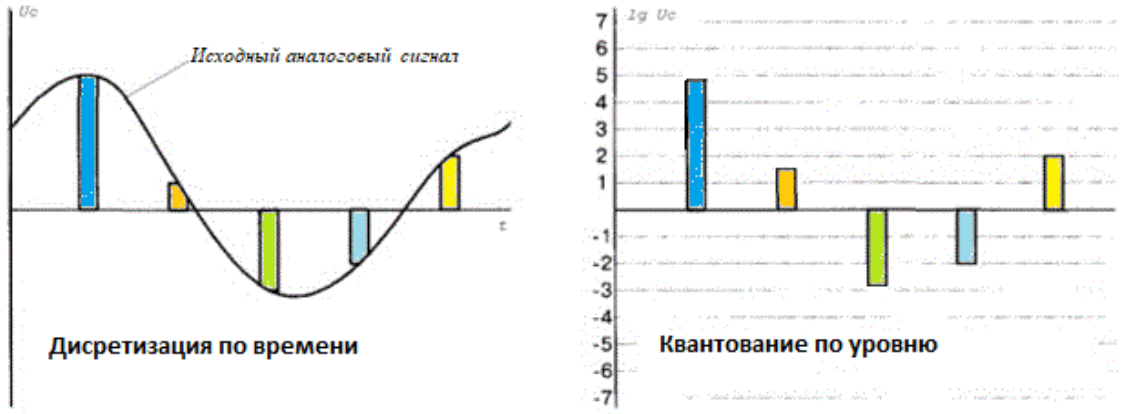

Рис. 4.4. Дискретизация и квантование аналогового речевого сигнала

Эти две функции выполняются аналого-цифровыми преобразователями (АЦП), которые размещаются в современных АТС на плате абонентских комплектов, а в случае передачи речи по IP-сетям – в терминале пользователя, то есть в компьютере или IP-телефоне.

Так называемая теорема отсчетов гласит, что аналоговый сигнал может быть успешно восстановлен из последовательности выборок с частотой, которая превышает как минимум вдвое максимальную частоту, присутствующую в спектре передаваемого сигнала.

- В телефонных сетях полоса частот речевого сигнала намеренно, посредством специальных фильтров, ограничена диапазоном 0,3-3,4 кГц, что не влияет на разборчивость речи и позволяет узнавать собеседника по голосу.
- По этой причине частота дискретизации при аналого-цифровом преобразовании выбрана равной 8 кГц, причем такая частота используется во всех телефонных сетях на нашей планете.

При квантовании непрерывная величина отображается на множество дискретных значений, что, естественно, приводит к потерям информации. Для того чтобы обеспечить в такой схеме достаточный динамический диапазон (способность передавать без искажений как сильные, так и слабые сигналы), дискретная амплитуда сигнала кодируется 12/13-разрядным двоичным числом по линейному закону.

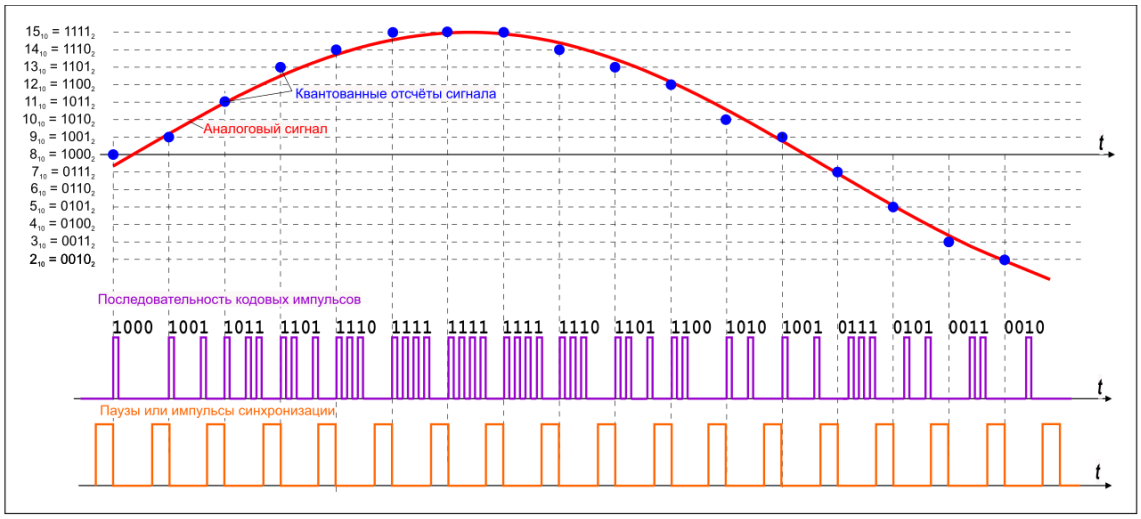

Рис. 4.5. Пример 4-битной 16-уровневой ИКМ (https://ru.wikipedia.org/).

Процесс аналого-цифрового преобразования получил применительно к системам связи название *импульсно-кодовой модуляции* (ИКМ). На рис. 4.5 дан пример 4-битной, то есть 16-уровневой ИКМ. Показано квантование аналогового сигнала и пачки импульсов, кодирующих отсчёты. Передача в канал идет старшими битами вперёд

Чтобы снизить необходимую скорость передачи битов, применяют нелинейный (логарифмический) закон квантования, то есть квантованию подвергается не амплитуда сигнала, а ее логарифм.

В данном случае происходит процесс "сжатия" динамического диапазона сигнала, а при восстановлении сигнала выполняется обратный процесс. На сегодня применяются две основные разновидности ИКМ:

- с кодированием по μ-закону (https://ru.wikipedia.org/wiki/Мю-закон);
- с кодированием по А-закону (https://ru.wikipedia.org/wiki/А-закон).

В результате сжатия сигнал с амплитудой, которая квантуется 12-13 битами, представляется всего восемью битами. Различаются эти разновидности ИКМ используемыми алгоритмами сжатия.

Исторически сложилось так, что в Северной Америке и Японии используется кодирование по μ-закону, а в Европе - по А-закону. Поэтому при международной связи во многих случаях требуется преобразование μ-кодирования в А-кодирование, ответственность за которое несет страна, где используется μ-закон кодирования.

Расчет пропускной способности канала с ИКМ

Следует отметить, что в обоих случаях каждый отсчет кодируется 8 битами, или одним байтом, который можно считать звуковым фрагментом. Для передачи последовательности таких фрагментов необходима пропускная способность канала, равная 64 Кбит/с. Это можно определить, если принять во внимание, что максимальная частота речевого сигнала ограничена 4 кГц. Тогда пропускную способность канала можно найти, используя последовательность простейших арифметических действий:

$$4\ 000\ Гц * 2 = 8\ 000\ отсчетов/с\ ;$$

$$8\ 000\ отсчетов/с * 8\ битов = 64\ Кбит/с\ .$$

Технология ИКМ была первой стандартной технологией, получившей широкое применение в цифровых системах передачи информации. Поэтому пропускная способность канала, равная 64 Кбит/с стала всемирным стандартом для цифровых сетей всех видов.

Причем стандартом, который обеспечивает передачу речи с очень хорошим качеством. Соответствующие процедуры кодирования и декодирования стандартизованы ITU-T в рекомендации G.711.

Подчеркнем, что такое высокое качество передачи речевого сигнала, которое принимается за эталон при оценке качества других схем кодирования, достигнуто в системах ИКМ за счет явно избыточной, при современном уровне технологии, скорости передачи информации.

Подходы к снижению полосы пропускания VoIP канала

Чтобы уменьшить присущую ИКМ избыточность и снизить требования к полосе пропускания, последовательность чисел, полученная в результате преобразования речевого аналогового сигнала в цифровую форму, подвергается математическим преобразованиям, позволяющим уменьшить необходимую скорость передачи.

Эти преобразования "сырого" цифрового потока в поток меньшей скорости называют "сжатием", рассматривая при этом ИКМ как некую промежуточную форму представления. Существует множество подходов к "сжатию" речевой информации, все их можно разделить на три категории:

- кодирование формы сигнала (waveform coding),
- кодирование исходной информации (source coding)
- гибридное кодирование, сочетание двух предыдущих подходов.

Наибольший интерес представляют сложные алгоритмы, позволяющие снизить требования к полосе пропускания. В них осуществляется кодирование формы сигнала и используется то обстоятельство, что между случайными значениями нескольких следующих подряд отсчетов существует некоторая зависимость.

Проще говоря, значения соседних отсчетов обычно мало отличаются одно от другого. Это позволяет с довольно высокой точностью предсказать значение любого отсчета на основе значений нескольких предшествовавших ему отсчетов. При построении конкретных алгоритмов кодирования названная закономерность используется двумя способами.

- Во-первых, есть возможность изменять параметры квантования в зависимости от характера сигнала.
- Во-вторых, существует подход, называемый дифференциальным кодированием, или линейным предсказанием. Вместо того чтобы кодировать входной сигнал непосредственно, кодируют разность между входным сигналом и "предсказанной" величиной, вычисленной на основе нескольких предыдущих значений сигнала.

Простейшей реализацией последнего подхода является так называемая дельта-модуляция (ДМ), алгоритм которой предусматривает кодирование разности между соседними отсчетами сигнала только одним информационным битом, обеспечивая передачу, по сути, только знака разности.

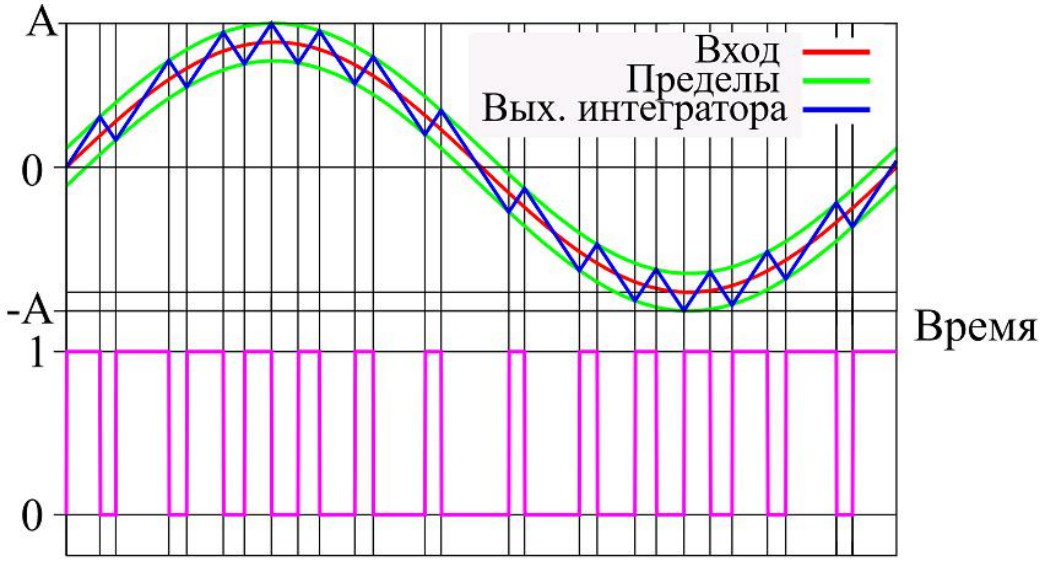

Рис. 4.6. Преобразование сигнала при дельта-модуляции.

Фактически, дельта-модуляция представляет собой разновидность ИКМ, в которой число уровней квантования равно двум. При ДМ по каналу связи передаётся не абсолютное значение сигнала, а разность между исходным аналоговым сигналом и аппроксимирующим напряжением (сигнал ошибки). По сравнению с ИКМ дельта-модуляция характеризуется меньшей сложностью технической реализации, более высокой помехозащищённостью и гибкостью изменения скорости передачи

Наиболее совершенным алгоритмом является алгоритм адаптивной дифференциальной импульсно-кодовой модуляции (АДИКМ). Он предусматривает формирование сигнала ошибки предсказания и его последующее адаптивное квантование. Подобные методы кодирования часто используются в современных устройствах кодирования речи.

4.6. Требования к алгоритмам кодирования сигнала

Скорость передачи, которую предусматривают имеющиеся сегодня узкополосные кодеки, лежит в пределах 1.2-64 кбит/с. Естественно, что от этого параметра прямо зависит качество воспроизводимой речи. Существует множество подходов к проблеме определения качества.

Что такое MOS (Mean Opinion Score)?

Для оценки качества голоса и видео обычно используются качественные оценки типа хорошее или плохое, но кроме качественного описания достаточно удобно использовать количественные методы, чтобы выражать оценку в числовом виде.

Такая оценка существует и называется Mean Opinion Score (MOS) – усредненная оценка разборчивости речи. Она дает численное представление о качестве передаваемой медиа информации после сжатия с помощью кодеков и передачи по каналам связи.

Выражается он числовым значением от 1 до 5. MOS довольно субъективная оценка, так как она основана на восприятии качества голоса людьми. Однако, есть приложения, которые умеют измерять MOS и их данные более объективны. Значения не обязательно целые числа, например,

- Значение от 4,0 до 4,5 соответствует качеству передачи речи в ISDN.
- Значения 3,5 до 4 (toll quality) соответствует качеству передачи ТфОП. Оно аналогично качеству речи, передаваемой с помощью кодека АДИКМ при скорости 32 Кбит/с и обеспечивается в большинстве телефонных разговоров.
- Мобильные сети обеспечивают качество чуть ниже toll quality, а значения ниже 3,5 для многих пользователей оказываются неприемлемыми

Что такое R-Factor?

Это второй способ оценки качества звука, который имеет более расширенную шкалу от 0 до 120, что позволяет делать более точную оценку. R-Factor рассчитывается с учетом ощущений пользователя и объективных факторов,

которые влияют на общее качество VoIP-системы, сетевой R-Factor и пользовательский R-Factor рассчитываются отдельно.

Уровень удовлетворенности пользователей	MOS	R-Factor
Максимальный с применением G.711	4.4	93
Очень довольны	4.3-5.0	90-100
Довольны	4.0-4.3	80-90
Некоторые пользователи довольны	3.6-4.0	70-80
Многие пользователи недовольны	3.1-3.6	60-70
Практически все пользователи недовольны	2.6-3.1	50-60
Работа не рекомендуется	1.0-2.6	Менее 50

Подавление периодов молчания. При диалоге один из его участников говорит в среднем только 35 процентов времени. Таким образом, если применить алгоритмы, которые позволяют уменьшить объем информации, передаваемой в периоды молчания, то можно значительно сузить полосу пропускания.

В двустороннем разговоре такие меры позволяют достичь сокращения объема передаваемой информации до 50%, а в децентрализованных многоадресных конференциях (за счет большего количества говорящих) – и того более. Нет смысла организовывать многоадресные конференции с числом участников больше 5-6, не подавляя периоды молчания.

Генератор комфортного шума. В момент, когда в речи активного участника беседы начинается период молчания, терминалы слушающих могут просто отключить воспроизведение звука. Однако это было бы неразумно.

Если в трубке возникает "гробовая тишина", то есть фоновый шум, который был слышен во время разговора, внезапно исчезает, то слушающему кажется, что соединение по каким-то причинам нарушилось, и он обычно начинает спрашивать, слышит ли его собеседник. Генератор CNG (Comfort Noise Generator) служит для генерации фонового шума.

Чувствительность к потерям кадров. Такие потери неотъемлемый атрибут IP-сетей. Но потери пакетов и потери кадров не всегда связаны между собой, так как существуют подходы, например, применение кодов с исправлением ошибок ("forward error correction"), позволяющие уменьшить число потерянных кадров при заданном числе потерянных пакетов. Необходимая для этого дополнительная служебная информация распределяется между несколькими пакетами, так что при потере некоторого числа пакетов кадры могут быть восстановлены.

Кодеры G.723.1 разработаны так, что они функционируют без существенного ухудшения качества в условиях некоррелированных потерь до 3% кадров, однако при превышении этого порога качество ухудшается катастрофически.

4.7. Кодеки IP-телефонии

В данном разделе дается краткая справка по наиболее распространенным типам кодеков, которые используются в VoIP устройствах.

Кодек G.711 – один из первых цифровых кодеков речевых сигналов, который является минимально необходимым. Это означает, что любое VoIP устройство

должно поддерживать этот тип кодирования. Кодек G.723.1 является базовым для приложений IP-телефонии. Он предусматривает две скорости передачи: 6.3 Кбит/с (MOS = 3,9) и 5.3 Кбит/с (MOS = 3,7). Режим работы может меняться динамически от кадра к кадру.

Кодек G.726 – обеспечивает кодирование цифрового потока со скоростью 40, 32, 24 или 16 Кбит/с, гарантируя MOS на уровне 4,3 (32 кбит/с), что принимается за эталон уровня качества телефонной связи (toll quality). Однако в приложениях IP-телефонии этот кодек практически не используется, так как он не обеспечивает достаточной устойчивости к потерям информации.

Кодек G.728 специально разрабатывался для оборудования уплотнения телефонных каналов, при этом было необходимо обеспечить возможно малую величину задержки (менее 5 мс), чтобы исключить необходимость применения эхо компенсаторов.

Кодек G.729 очень популярен в приложениях передачи речи по сетям Frame Relay. Кодек использует кадр длительностью 10 мс и обеспечивает скорость передачи 8 Кбит/с. Однако для кодера необходим предварительный анализ сигнала продолжительностью 5 мс. Существуют две разновидности кодека: G.729 и упрощенный вариант G.729A.

Таблица 4.1.

Основные характеристики кодеков

Кодек	Метод компрессии	Скорость кодирования	Сложность реализации	Качество	Задержка
G.726	ADPCM	32/24/16 Кбит/с	Низкая (8 MIPS)	Хорошее(32К), плохое(16К)	Очень низкая (0,125 мс)
G.729	CS-ACELP	8 Кбит/с	Высокая (30 MIPS)	Хорошее	Низкая (10 мс)
G.729A	CA-ACELP	8 Кбит/с	Умеренная (20 MIPS)	Среднее	Низкая (10 мс)
G.723.1	MP-MLQ	6.4/5.3 Кбит/с	Умеренная (16 MIPS)	Хорошее(6,4), среднее(5,3)	Высокая (37 мс)
G.728	LD-CELP	16 Кбит/с	Очень высокая (40 MIPS)	Хорошее	Очень низкая (3-5 мс)

Количественными характеристиками ухудшения качества речи являются единицы QDU (Quantization Distortion Units): Значение QDU = 1 соответствует ухудшению качества при оцифровке с использованием стандартной процедуры ИКМ; значения QDU для других методов компрессии приведены в таблице 4.2.

Таблица 4.2.

Ухудшение качества речи для различных методов компрессии

Метод компрессии	QDU
ADPCM 32 кбит/с	3,5
ADPCM 24 кбит/с	7
LD-CELP 16 кбит/с	3,5
CS-CELP 8 кбит/с	3,5

Дополнительная обработка речи всегда ведет к дальнейшей потере качества. Согласно рекомендациям МСЭ-Т, для международных вызовов величина QDU не должна превышать 14.

- Причем передача разговора по международным магистральным каналам ухудшает качество речи, как правило, на 4 QDU.
- При передаче разговора по национальным сетям должно теряться не более 5 QDU.
- Поэтому для качественной передачи речи процедуру компрессии/декомпрессии желательно применять в сети только один раз.

В некоторых странах это является обязательным требованием регулирующих органов по отношению к корпоративным сетям, подключенным к сетям общего пользования. Современная аппаратура IP-телефонии применяет разные кодеки, как стандартные, так и нестандартные. Конкурентами являются кодеки GSM (13,5 Кбит/с) и кодеки МСЭ-Т серии G, использование которых предусматривается стандартом H.323 для связи по IP-сети.

4.8. Оценка качества воспринимаемой информации

Ниже в таблице 4.3 приведены значения MOS для различных стандартов кодеров, используемых в IP-телефонии.

Таблица 4.3.

Средние субъективные оценки качества различных методов кодирования

Кодек	Скорость передачи, Кбит/с	MOS	Размер кадра, мс
G.711 PCM	64	4,3	0,125
G.726 Multi-rate ADPCM	16-40	2-4,3	0,125
G.723 MP-MLQ ACELP	5.3; 6.3	3,7; ,	8 30
G.728 LD-CELP	16	4,1	0,625
G.729 CS-ACELP	8	4,0	10
G.729A CA-ACELP	8	3,4	10
GSM RPE-LPC	13	3,9	30

В каналах Интернета важными для IP-телефонии параметрами являются следующая группа параметров:

- действительная пропускная способность, определяемая наиболее "узким местом" в виртуальном канале в данный момент времени;
- трафик, также являющийся функцией времени;
- временная задержка пакетов, которая определяется трафиком, числом маршрутизаторов, реальными физическими свойствами каналов передачи, образующими в данный момент времени виртуальный канал, задержками на обработку сигналов, возникающими в речевых кодеках и других устройствах шлюзов;
- потеря пакетов, обусловленная наличием "узких мест", очередями;
- перестановка пакетов, пришедших разными путями.

5. МОБИЛЬНОСТЬ IP-ТЕЛЕФОНИИ

Аннотация: Тема связана с проблемами и методами решения мобильности IP-телефонии. Разновидности мобильности. Проблемы идентификации терминалов и пользователей в мобильной среде. Сценарии мобильности в сетях IP-телефонии учитывая использование протоколов SIP, H.323. Затронута задача IP-телефонии для пользователей сетей сотовой подвижной связи

5.1. Разновидности мобильности

Сети IP-телефонии поддерживают четыре типа мобильности.

- Мобильность пользователя - возможность пользователя соединяться с сетью IP телефонии, используя для соединения различные типы терминалов.
- Мобильность терминала - возможность терминала менять физическое местонахождение, сохраняя способность соединения с сетью. В свою очередь мобильность терминала подразделяется на два вида:
- дискретная мобильность терминала (roaming) - изменение физического местонахождения терминала за пределами сеанса связи с сетью;
- непрерывная мобильность терминала (handover) - изменение физического местонахождения терминала в пределах сеанса связи с сетью с потерей или без потери передаваемых данных.
- Мобильность обслуживания предоставляет абоненту возможность воспользоваться услугой, на которую он подписался, вне зависимости от местонахождения и типа терминала.
- Режим виртуальной домашней сети - то же самое, что и мобильность обслуживания, но касается не одной услуги, а пакета услуг. При этом в зависимости от конкретной услуги, предоставляемой абоненту, в его обслуживание может быть вовлечен только сервер домашней сети или необходимо взаимодействие сервера домашней сети с сервером внешней сети.

Доступ к сетям IP-телефонии могут получить и абоненты сотовых сетей. Одной из перспективных технологий, обеспечивающих доступ мобильного абонента сотовой связи к сетям передачи данных, является система пакетной радиосвязи общего пользования (GPRS). К тому же взаимодействие IP-телефонии с технологиями беспроводного доступа (сейчас Wi-Fi, а в будущем и WiMAX) может дать толчок развитию принципиально нового направления - интернет-провайдеры с внешними каналами высокой производительности (ширина канала) могут превратиться в телефонные компании, обеспечивающие качественную международную связь. При наличии городских беспроводных сетей снимаются ограничения на мобильность пользователей, в результате качественная телефонная связь станет возможной в любой точке города.

В качестве SIP-терминалов абонент может воспользоваться несложными в обращении программными средствами, повторяющими функциональность телефонов. Настройка таких программ, называемых softphone, не требует глубоких знаний в области VoIP. Для осуществления вызовов достаточно ввести номер (SIP ID) в специальное окно ввода и нажать кнопку вызова.

5.2. Идентификация терминала и пользователя

Для реализации услуг мобильности пользователя и терминала требуется их идентификация на различных уровнях. Терминал может быть идентифицирован как оборудование или как телефонное приложение IP, которое может управлять различными элементами сети.

Терминал имеет следующие идентификаторы:

- идентификатор собственно терминала (транспортный адрес, идентификатор оборудования);
- идентификатор приложения (идентификатор конечной точки, точки доступа, адреса приложений транспортного уровня).

Для определения пользователя используются следующие идентификаторы:

- идентификатор пользователя (уровень приложений);
- абонентский идентификатор (транспортный уровень);
- роуминговый идентификатор пользователя (по существу, абонентский идентификатор прикладного уровня, который может отличаться или не отличаться от абонентского идентификатора транспортного уровня).

5.3. Сценарии мобильности в сетях IP-телефонии

Все объекты, участвующие в процедуре мобильности, можно подразделить на следующие функциональные элементы.

- IP Application Point of Attachment (APoA) - точка подключения IP-приложения. Это компонент, например шлюз, в котором терминал регистрируется на прикладном уровне, например, терминал H.323. В функции APoA входит обеспечение соединения мобильного абонента с сетью на прикладном уровне.
- Home Entity (HE) - домашний компонент, например шлюз, который управляет установлением соединения с вызываемым абонентом, хранит данные о наборе характеристик (профиле) абонента, предоставляет APoA данные о текущем местоположении абонента.
- Network Point of Attachment (NPoA) - точка подключения сети. Это компонент, который обеспечивает соединение между различными IP-сетями. В его функции входит обеспечение связи мобильного абонента с сетью на транспортном уровне. Примером NPoA является маршрутизатор доступа.
- Subnet - подсеть, обслуживаемая одним NPoA.
- Serving Area - зона обслуживания, которая может включать несколько подсетей, обслуживаемых одним APoA.

Перечисленные элементы сети IP-телефонии, участвующие при реализации функций мобильности, показаны на рис. 5.1.

Рис. 5.1. Функциональные элементы, вовлеченные в обслуживание абонента при мобильности

В сетях IP-телефонии возможны следующие четыре сценария мобильности:

- Мобильность между подсетями.
- Мобильность между зонами обслуживания.
- Мобильность между подсетями и зонами обслуживания одновременно.
- Мобильность между подсетями, находящимися в разных зонах обслуживания.

На рис. 5.2-5.5 показаны различные сценарии мобильности абонента в сети IP-телефонии.

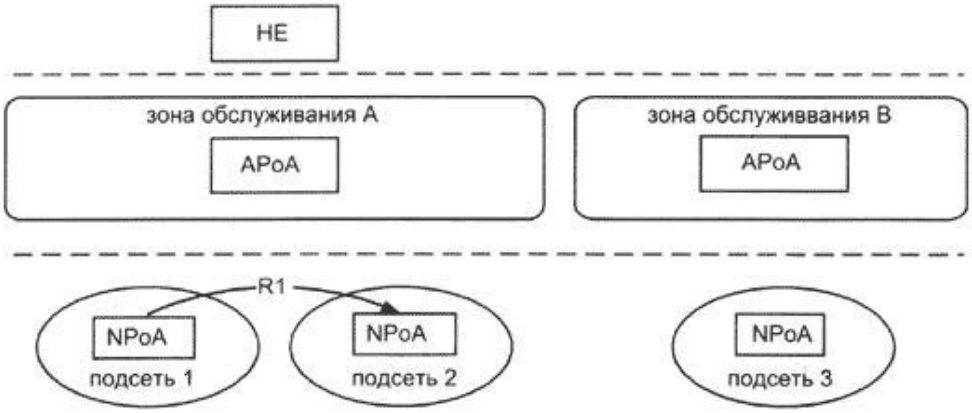

Рис. 5.2. Мобильность между подсетями в пределах одной зоны обслуживания.

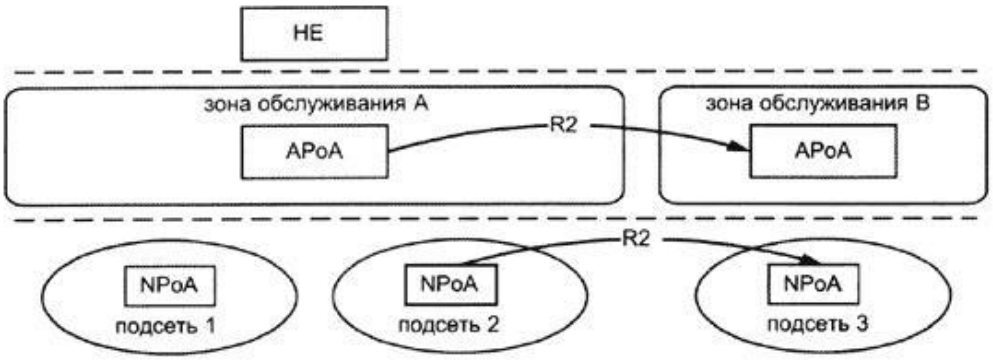

Рис. 5.3. Мобильность между подсетями и между зонами обслуживания

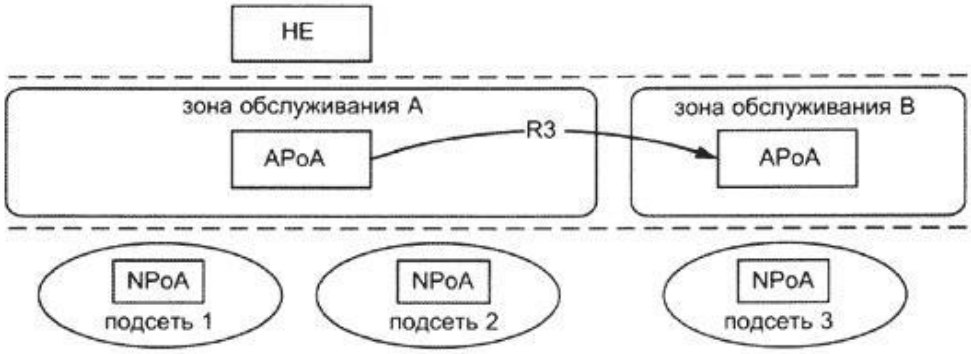

Рис. 5.4. Мобильность между зонами обслуживания

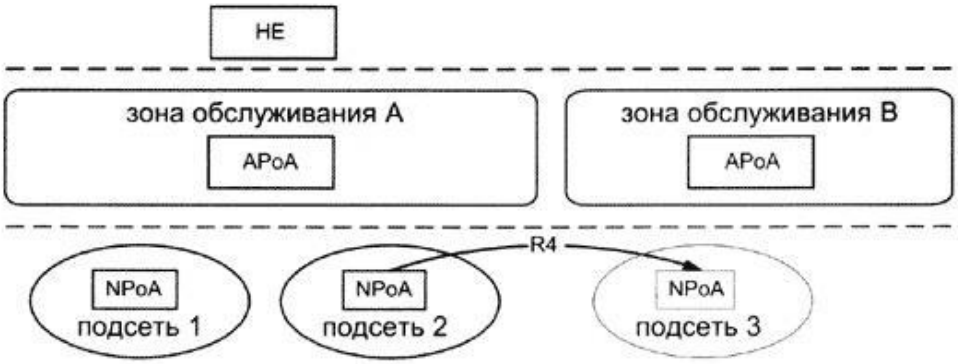

Рис. 5.5. Мобильность между подсетями, находящимися в разных зонах обслуживания

5.4. Мобильность в сети IP-телефонии на базе протокола SIP и H.323

Мобильность пользователя в SIP-протоколе основана на применении уникального персонального идентификатора, в то время как мобильность пользователя IP-телефонии в стандарте H.323 возможна, но до конца не определена. В соответствии с процедурами стандарта сначала устанавливается сигнальное соединение со шлюзом зоны H.323, а следовательно, адрес вызываемого абонента может быть определен перед установлением соединения, поэтому возможно перенаправление сигнального соединения с полной обработкой на прикладном уровне.

Для регистрации пользователей используется сервер-регистратор Registrar для регистрации SIP-терминалов, после того как он присылает запрос о регистрации. Далее сервер-регистратор сообщает домашнему серверу пользователя, где тот зарегистрирован.

Каждый пользователь сети может вызвать другого абонента с помощью сообщения-приглашения. После выдачи сервером-регистратором информации о нахождении абонента Proxy-сервер устанавливает соединение между пользователями.

Достоинством SIP часто называют мобильность, причем этот термин имеет несколько смыслов. Во-первых, под мобильностью можно подразумевать независимость от производителя оборудования: действительно, решения от разных производителей практически всегда оказываются совместимы друг с другом, что, например, в сравнении с протоколом H.323 является

преимуществом. Второе понимание - это мобильность самого абонента: благодаря системе серверов локализации и переадресации вам всегда можно звонить на один и тот же номер (адрес), а SIP-сервер самостоятельно разыщет вас там, где вы находитесь.

В то же время протокол H.323 предоставляет больше возможностей управления услугами, как в части аутентификации и учета, так и в части контроля использования сетевых ресурсов.

Протокол SIP имеет хороший набор средств поддержки персональной мобильности пользователей, в число которых входит переадресация вызова к новому местоположению пользователя, одновременный поиск по нескольким направлениям (с обнаружением зацикливания маршрутов) и т. д. В протоколе SIP это организуется путем регистрации на сервере определения местоположения, взаимодействие с которым может поддерживаться любым протоколом. Персональная мобильность поддерживается и протоколом H.323, но менее гибко. Так, например, одновременный поиск пользователя по нескольким направлениям ограничен тем, что шлюз, получив запрос определения местоположения пользователя LRQ, не транслирует его к другим шлюзам.

5.5. IP-телефония для клиентов сетей сотовой подвижной связи

Многими компаниями сотовой связи, например, компанией Motorola, были созданы новые линейки продукции, которые призваны объединить мобильную связь и домашнюю телефонию, давая пользователям возможность общаться, используя один телефонный номер и один мобильный терминал вне зависимости, находятся ли они дома или за его пределами.

Минимально достаточное решение включает в себя беспроводную точку доступа стандарта 802.11b/g, четырехпортовый маршрутизатор и адаптер VoIP-телефонии. При условии применения специальных терминалов dual-mode handset (DMH), работающих как в беспроводной домашней сети, так и в сотовых сетях, технология позволит незаметно для пользователя переключаться между сетями в зависимости от удаленности пользователя и качества сигнала.

Подобные устройства также могут применяться как многофункциональные, через которые может быть организована передача не только потоков данных IP-телефонии, но и самые разнообразные данные, полученные через широкополосное соединение на любые устройства, подключенные к домашней беспроводной сети.

Преимуществами подобного варианта являются: возможность для терминала использовать сотовый канал или Wi-Fi, в зависимости от качества приема; приоритетность трафика IP-телефонии перед прочими, позволяющая добиться максимально возможного качества звука при использовании Wi-Fi и VoIP; поддержка функций идентификации входящего звонка, удержания вызова, конференц-связи, переадресации звонка; шифрование данных для защиты от несанкционированного прослушивания.

6. ОСНОВЫ СЕТЕВОГО ВИДЕОНАБЛЮДЕНИЯ

Сетевое видеонаблюдение, которое часто называют IP-видеонаблюдением, основано на системах, которые дают пользователям возможность вести наблюдение и записывать видео и/или звуковые потоки по IP-сетям (локальные, глобальные сети, Интернет). Сетевое видеонаблюдение можно использовать в самых разнообразных сферах применения, но наибольшее применение получило в системах охранного телевидения (СОТ) и системах удаленного мониторинга за труднодоступными технологическими процессами.

6.1. Немного истории

В середине девяностых годов XX века на рынке оборудования СОТ появился новый вид оборудования – цифровые видео регистраторы. Они сочетали в себе решения своих предшественников: видеомагнитофона и мультиплексора. Но при этом обладали функцией цифровой записи видео информации. Через некоторое время функционал видео регистратора дополнился возможностью просматривать видео удаленно (мониторинг+архив). В первое время для этой цели использовали модем, а затем стали использовать сетевой Ethernet порт.

Рис. 6.1. Сетевая телекамера AXIS 200.

В 1996 году компания Axis разработала первую в мире сетевую телекамеру AXIS 200 (рис.6.1). Она передавала информацию низкого качества со скоростью 1 кадр в секунду. При таких характеристиках ее нельзя было использовать в системах безопасности. Но через несколько лет IP-камеры резко улучшили свои технические параметры: разрешение изображения стало не хуже, чем у аналоговых видео камер, скорость передачи достигло 30 к/с, плюс появился встроенный видео детектор. Это уже стало интересно для специалистов службы безопасности, но пропускная способность большинства сетей на тот момент была всего 10 Мбит/сек, что затрудняло передачу данных.

В 2000 году появились 100-мегабитные сети, что и решило проблему. А через пять-семь лет появились гигабитные сети, которые позволяли передавать видеопотоки от нескольких сотен сетевых камер и с высоким разрешением и высокой скоростью.

В настоящее время системы сетевого видеонаблюдения могут включать в себя несколько тысяч телекамер. Но при этом, сколько же необходимо операторов? На помощь пришло интеллектуальное видеонаблюдение. Программное обеспечение СОТ позволяет самостоятельно вести мониторинг и извещать оператора в случае необходимости.

Немаловажным достижением IP-видеонаблюдения явилось его сравнительно легкая интеграция (по сравнению с аналоговым видеонаблюдением) с другими системами безопасности: ОПС, СКУД. Интегрированные системы безопасности на базе IP-сетей находят широкое применение на различных объектах: на производстве, в банковской сфере, в торговле, на транспорте, в образовании. Хронологически и функционально можно проследить несколько ступеней/ уровней “взросления” сетевого видеонаблюдения:

- Аналоговые СОТ на базе цифровых регистраторов (DVR).
- Аналоговые СОТ на основе DVR с сетевым функционалом.
- СОТ на базе сетевых видеосерверов, которые оцифровывают и сжимают видео, поступающее от аналоговых телекамер, и передают его в сеть.
- Сетевые СОТ на базе сетевых видеорегистраторов (NVR), которые работают только с IP-камерами.
- СОТ на базе гибридных видеорегистраторов, которые работают как с аналоговыми, так и с IP-видеокамерами.
- Сетевые СОТ на базе IP-камер и компьютера (сервера) с установленным ПО системы видеонаблюдения.

Из всего разнообразия функциональных решений дать точное определение сетевого видеонаблюдения довольно сложно, что-то можно не учесть. Поэтому ограничимся определением только для случая 100%-цифрового варианта.

Сетевое видеонаблюдение - это система видеонаблюдения, в которой видеопоток (видео + аудио) передается от сетевой видео камеры по IP-сети через сетевые коммутаторы и поступает на компьютера (сервера) с установленным на нем программным обеспечением для мониторинга и записи. Основными преимуществами сетевых СОТ являются:

- Получение видео с более высоким разрешение, чем от аналоговых камер.
- Качество изображения не зависит от дистанции передачи.
- Возможность контроля текущей обстановки на объекте удаленно по Интернет с помощью ноутбука или мобильного телефона из любой точки земного шара.
- Доступность организации всего одного центральный пункт наблюдения на несколько объектов, а также возможность удаленно конфигурировать сетевые телекамеры.
- По одному кабелю типа «витая пара» можно передавать: видео, аудио, сигналы управления поворотными IP-камерами, а также питание (PoE). Это приводит к экономии кабеля, материалов и на монтажных работах. При этом существует и возможность беспроводной передачи данных.

- Доступность проведения видеоанализа, при которой цифровая обработка мегапиксельных изображений позволяет анализировать отдельные области кадра. Например, распознавать номер автомобиля или лицо нарушителя и т.д.
- Лучшая интеграция с другими системами безопасности: ОПС, СКУД.

6.2. Компоненты сетевых систем видеонаблюдения

Рассмотрим обобщенную структурную схему сетевой системы видеонаблюдения (ВН) и основные компоненты её составляющие. Как правило, структура современных систем видеонаблюдения (рис. 6.2) включает в свой состав следующие компоненты:

- Сетевые видеокамеры.
- Сервер с программным обеспечением видеонаблюдения.
- Устройства хранения информации.
- Сетевые видеосерверы.
- IP-сеть.

Рис. 6.2. Структурная схема сетевой системы видеонаблюдения.

Одним из положительных качеств сетевых систем ВН является то, что сервер, устройство хранения информации и компоненты сети – это общедоступное стандартное компьютерное оборудование, у которого каждые 1,5 – 2 года удваивается производительность процессоров и объем устройств хранения данных. Что касается остальных составляющих: сетевые телекамеры, сетевые видеосерверы и программное обеспечение IP-видео – это специализированные продукты, присущие только сетевому видеонаблюдению.

Если в системах аналогового ВН передача информации от каждой телекамеры осуществляется по отдельному кабельному каналу на вход регистратора, то в IP системах цифровой видео и аудио потоки передаются по проводным или беспроводным сетям, что позволяет снимать информацию в любом месте IP-сети.

Кратко охарактеризуем каждый компонент сетевых систем видеонаблюдения, некоторые из которых в дальнейшем будут рассмотрены более подробно.

- *Сетевая телекамера.*

  Ключевой элемент системы, который позволил совершить качественный скачок в сетевом видеонаблюдении. Наличие у IP-камеры собственных вычислительных ресурсов предполагает большие, чем у аналоговых камер, функциональные возможности. В частности, возможна реализация видеоанализа непосредственно в самой камере, не говоря уже о значительном превосходстве в качестве/разрешении передаваемого изображения.

  IP-камера не только формирует видеосигнал, но и оцифровывает его (устройство АЦП), сжимает с помощью кодеков (в MPEG-4, MJPEG, H.264) и передает через сетевой порт Ethernet. Поскольку IP-камеры имеют встроенный веб-сервер, изображение с них можно просматривать в окне стандартного браузера.

- *Сервер с программным обеспечением видеонаблюдения*

  В основном для этих целей используют стандартные компьютерные серверы с операционной системой Windows. Конфигурация сервера системы определяется в основном количеством сетевых камер и объемом передаваемой информации. Для небольших систем (15-20 камер) можно использовать младшие модели двухядерных процессоров, а для больших систем (более 100 камер) и при максимальной скорости трансляции необходимо задействовать сервера на базе многоядерных процессоров.

  Программное обеспечение сетевого видеонаблюдения обеспечивает необходимые сервисы для мониторинга, записи, управления, а также видеоанализа информации. В настоящее время на рынке представлено множество программных продуктов и от различных производителей как отечественных (Интеллект, VideoIQ7, Smart Video, VideoInspector, Видео Гарант, VideoNet, Трассир, Эвклид, BEWARD, и др.), так и зарубежных монстров Axis, Sony, Bosch, Panasonic.

  Если необходимо просматривать информацию с одной - двух сетевых камер, то достаточно будет задействовать стандартный веб-браузер, установленный на самой камере. Одна из задач, решаемых ПО для IP-видео, это интеграция с другими системами: система контроля доступом, охранно-пожарная, автоматическое управление инженерией зданий и др.

- *Устройства хранения информации*

  На практике часто устройства хранения и программное обеспечение сетевого видеонаблюдения реализуются на базе одного стандартного сервера. Для хранения информации используют обычный накопитель на

жестких магнитных дисках (HDD). Для хранения видеоинформации на жестком диске необходимо иметь четко организованную структуру, она может быть достаточно простой: дерево каталогов, в каталоги которого вложены файлы. Видеозаписи могут храниться в виде стандартных файлов: JPEG, MPEG, AVI и др. Для повышения надежности хранения информации применяют RAID-массивы. Если сетевая система состоит из сотен или тысяч IP-телекамер, то для хранения могут быть использованы NAS (Network Attached Storage – сетевые устройства хранения) или SAN (Storage Area Network – сети хранения данных).

- *Сетевой видеосервер*

  Это устройство, предназначенное для работы в составе аналогово-цифровой системы видеонаблюдения и преобразования аналогового видеосигнала в цифровой формат для последующей передачи его по IP-сети (рис. 6.3).

Рис. 6.3. Сетевой видеорегистратор.

Из определения следует, что видеосерверы, как правило, применяют там, где уже имеется аналоговая система ВН и есть необходимость в передаче информации от нескольких аналоговых камер по сети, при этом не придется избавляться от существующего оборудования.

В сетевых видеосерверах обычно есть один или четыре аналоговых входа – для подключения аналоговых камер и один сетевой разъем для подключения к сети Ethernet. Для систем с большим числом аналоговых камер разработаны серверы стоечного исполнения на 48 и 84 аналоговых входов. Видеосервер имеет: аналого-цифровой преобразователь, кодек сжатия, встроенный веб-сервер, операционную систему. Так как по всему миру установлены и работают не один миллион аналоговых телекамер, то видеосерверы имеют и еще долго будут иметь большой спрос.

- *Коммуникационная IP-сеть*

  Как уже отмечалось, в качестве сети для сетевого видеонаблюдения, используются стандартные проводные и беспроводные IP-сети. Они просты и экономичны в развертывании, во многих случаях уже есть там, где планируется установить сетевое видеонаблюдение.

После описания краткой характеристики каждого компонента сетевых систем видеонаблюдения перейдем к более подробному рассмотрению каждого из этих компонентов, их принципу работы и техническим характеристикам. И начнем, естественно, с сетевых видеокамер.

6.3. Сетевые IP видеокамеры

Под сетевой IP-камерой понимают цифровую видеокамеру, особенностью которой является передача видеопотока в цифровом формате по сети Ethernet, использующей протокол IP. Являясь сетевым устройством, каждая IP-камера в сети имеет свой IP-адрес. По сути IP-камера – это телекамера плюс компьютер. Большинство IP-камер имеют дополнительный функционал:

- детекторы движения,
- отправка сообщений по e-mail,
- подключение внешних датчиков и пр.

Пользователи могут обращаться к камере посредством стандартного браузера. В зависимости от настроек, доступ к информации от IP-камеры, может быть доступен всем пользователям сети или только авторизованным пользователям.

В отличие от аналоговых камер, после получения видеокадра с IP-камеры, изображение остаётся цифровым вплоть до отображения на мониторе; высокое качество изображения постоянно на всем трафике прохождения сигнала и не зависит от длины трафика.

Рис. 6.4. Общий вид цифровой видеокамеры.

Как правило, перед передачей, полученное с матрицы изображение сжимается с помощью покадровых (MJPG) и межкадровых (MPEG-4, H.264) методов видеосжатия. Существуют специализированные IP-камеры, осуществляющие передачу видео в несжатом виде.

Благодаря тому, что сетевым камерам не требуется передавать аналоговый сигнал в формате PAL или NTSC, где разрешение ограничено соответствующими стандартами CCIR/PAL – 720x576 и 720x480 в EIA/NTSC, в IP-камерах могут использоваться и большие разрешения, включая мегапиксельные.

Типовые значения разрешения для сетевых IP-камер составляет 640x480 точек, а для мегапиксельных – 1280x1024 или 1600x1200. Благодаря отказу от использования стандартов аналогового телевидения, IP-камеры могут передавать видеокадры с требуемой частотой. Существуют IP-камеры с частотой передачи больше 60 кадров в секунду.

Как следует из определения IP-камера – это, прежде всего телекамера, имеющая признаки аналоговой, но и имеющая свою специфику. Рассмотрим алгоритм работы и основные компоненты сетевой телекамеры (рис. 6.4).

Упрощенный алгоритм работы сетевой телекамеры:

- Отраженный от объекта световой поток попадает в зону объектива, фокусируется в нем, попутно проходит через ИК-фильтр и попадает на оптоэлектронный сенсор изображения (рис. 6.5).
- Сенсор изображения преобразует сфокусированное изображение в электрический сигнал.
- Этот сигнал поступает в процессор изображения (обработки сигнала), где оптимизируется по яркости, контрастности, цветности и т. п..
- В модуле сжатия изображения осуществляется компрессия видеопотока.
- Центральный процессор, Флэш-память (Flash memory) и оперативная память (DRAM) являются "мозгами" или компьютерной частью камеры. Они созданы специально для поддержки сетевых приложений.
- Посредством Ethernet-интерфейса цифровой видеопоток уходит в IP-сеть.

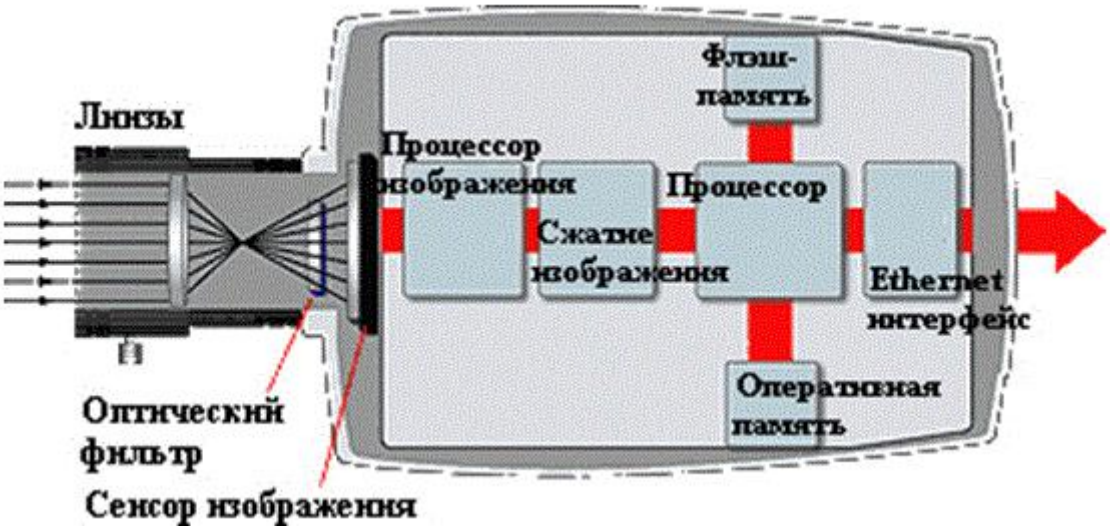

Рис. 6.5. Структура и основные компоненты цифровой видеокамеры.

Основные компоненты любой цифровой видеокамеры:

- *Объектив*

  Оптическое устройство для создания действительного оптического изображения. Обычно объектив состоит из набора линз, рассчитанных для взаимной компенсации аберраций (погрешности изображения) и собранных в единую систему внутри оправы. В конструкцию объектива могут входить вспомогательные элементы: диафрагма, для управления количеством проходящего света, система фокусировки.

- *Сенсор изображения* – оптико-электронная фотоприемная матрица

  Является основным элементом, самым технологически сложным и дорогим в денежном эквиваленте любой видеокамеры. Именно матрица определяет основные технические характеристики камеры. Современные телекамеры строятся на 2-х типах матриц:

  - ПЗС (CCD) матрица (Charge-Coupled Device. прибор с зарядовой связью) – специальная аналоговая интегральная микросхема,

состоящая из светочувствительных фотодиодов, выполненная на основе кремния, использующая технологию ПЗС. Основные размеры матриц: 1/3, 1/2 и 2/3 дюйма.

- КМОП (CMOS) – сокращение от «комплементарная логика на транзисторах металл-оксид-полупроводник» (Complementary Metal-Oxide Semiconductor). Это светочувствительная матрица, выполненная по КМОП-технологии, преимуществом которой является единство технологии, т.е. объединение на одном кристалле аналоговой, цифровой и обрабатывающей части. Не только «захват» света, но и процесс преобразования, обработки и очистки сигналов. Это послужило основой для миниатюризации камер для самого разного оборудования и снижения их стоимости ввиду отказа от дополнительных процессорных микросхем.
- Примечание: Для уменьшения общей стоимости сетевой телекамеры, чаще используют более дешевые CMOS-матрицы, теряя при этом в качестве продукта.

- *Процессор изображения или процессор обработки видеосигнала*

Это устройство выполняет в камере следующие функции: управление экспозицией, регулировкой баланса белого цвета, контрастностью и другими компонентами качества изображения. К числу таких функций относятся:

AGC – автоматическая регулировка усиления,

DSS – электронное увеличение чувствительности,

AWB – автоматическая регулировка баланса белого цвета ,

BLC – компенсация фоновой засветки, ,

DNR – цифровой алгоритм подавления шумов.

WDR (Wide Dynamic Range) – расширенный динамический диапазон.

Специфические компоненты сетевой телекамеры:

- *Модуль сжатия изображения*

Основная функция компрессия видеопотока, выполнен на базе DSP-микросхемы. Это процессор с памятью, в которую загружены программы алгоритма сжатия. Основные алгоритмы сжатия:

- H.264 – межкадровый алгоритм сжатия, в данное время один из основных стандартов компрессии видеоданных. Используется практически во всех типах IP-телекамер. Коэффициент сжатия у кодека H.264 достигает до 70:1.
- Кроме межкадрового алгоритма сжатия, существует и стандарт MJPEG (Motion JPEG) – это покадровый метод видеосжатия, основной особенностью которого является сжатие каждого отдельного кадра видеопотока с помощью алгоритма сжатия изображений JPEG. Коэффициент сжатия достигает до 15:1. Основным преимуществом видеосжатия Motion JPEG является

простота реализации, что делает MJPEG подходящим для реализации в устройствах с ограниченными вычислительными ресурсами.

- *Центральный процессор,*

Флэш-память и оперативная память являются компьютерной частью IP-камеры с CPU, памятью и операционной системой, как правило Linux. Основные функции: общее управление работой телекамеры, выполнение различных алгоритмов видеоанализа. Перенос аналитики на борт телекамеры привносит два положительных момента: анализируется докомпрессионный качественный видеопоток и функционально частично разгружается видеорегистратор.

При использовании флеш-карты пользователь получает не только возможность мониторинга, но и возможность управлять режимами записи, просмотра и скачивания архива по IP-сети.

- *Веб-сервер,*

это сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными. Короче, прописывая у себя на компьютере в адресной строке веб-браузера IP-адрес телекамеры, веб-сервер IP-камеры высылает нам HTML-страницу с видеопотоком и другими данными.

- *Сетевой интерфейс/ адаптер*

Функция: подключение сетевой телекамеры к IP-сетям. Могут поддерживать функцию PoE (Power over Ethernet), предоставляя камере возможность получать по одному кабелю, как данные, так и питание.

6.4. Основные типы сетевых телекамер

В настоящее время имеется большой выбор сетевых камер, которые соответствуют самым разнообразным требованиям потребителя. Классифицировать камеры можно в зависимости от места их установки: в закрытых помещениях и уличный вариант исполнения.

В частности, для уличных сетевых камер нужен термокожух (если она не поставляется в уличном исполнении) и объектив с автоматической регулировкой диафрагмы (АРД). Внешний защитный кожух может защищать не только от “минусовых” температур, влаги и пыли, но и от вандализма. Обычно выделяют следующие типы IP-камер:

- Корпусные фиксированные.
- Купольные фиксированные.
- Поворотные сетевые.
- Купольные поворотные.
- Миниатюрные.
- Мегапиксельные.

Корпусные/фиксированные сетевые телекамеры

Это такие сетевые телекамеры, поле зрения которых зафиксировано и не изменяется после их установки. При необходимости объектив можно поменять. Наиболее распространенный тип IP-телекамер (рис. 6.6).

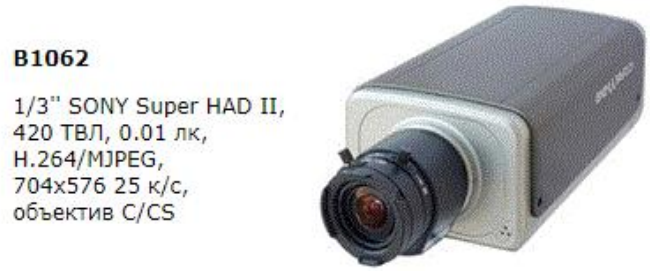

Рис. 6.6. Пример корпусной сетевой камеры.

Купольные фиксированные сетевые телекамеры

Это фиксированные IP-телекамеры, которые помещены в купольный кожух (рис. 6.7). Данные видеокамеры оснащаются: объективами с постоянным фокусным расстоянием и варифокальными объективами. Выбор объектива ограничивается габаритами купольного кожуха. Эти телекамеры могут комплектоваться различными типами кожухов: антивандальными, зеркальными. Места крепления: потолок, стены.

Рис. 6.7. Пример купольной фиксированной сетевой камеры

Поворотные сетевые телекамеры

Эти телекамеры, в отличие от фиксированных видеокамер, можно развернуть в любом направлении и увеличить нужный участок изображения. Управление осуществляется вручную или автоматически. Имеют возможность полного поворота на 360 градусов. Большинство камер обладает оптическим увеличением (до 26-кратного). На практике не получили должного применения, так как быстро выходит из строя механика. Значительно более востребованы купольные поворотные телекамеры. (рис. 6.8).

Рис. 6.8. Пример поворотной сетевой камеры

Купольные поворотные сетевые телекамеры

Благодаря возможности поворачиваться на 360 градусов в горизонтальной плоскости и 180 градусов по вертикали, и наличию оптического увеличения в диапазоне от 10 до 36-кратного данные IP-камеры могут вести наблюдение за обширными площадями. Все управляющие PTZ-команды, как и передача видеопотока осуществляются по IP-сети. Поскольку вся механика, электроника и оптика защищены гермокожухом, то данный тип камеры отличается высокой надежностью (рис. 6.9).

Рис. 6.9. Пример купольной поворотной сетевой камеры

Поворотные IP-видеокамеры нередко поддерживают большое количество запрограммированных предустановок, обычно от 20 до 100, кроме того можно создавать маршруты патрулирования. В режиме патрулирования одна телекамера такого типа может заменить несколько фиксированных, их часто применяют в системах охранного телевидения с участием оператора.

Одним из основных технических параметров является скорость перемещения/вращения в горизонтальной плоскости. Поэтому их ещё называют скоростными (0.4-320°/сек). Монтируют купольные поворотные IP-камеры: на потолках внутри помещений, мачтах и столбах, на фасадах или углах зданий.

Миниатюрные сетевые телекамеры

Корпусные фиксированные камеры, выполненные в миниатюрном корпусе. Естественно их технические характеристики скромнее по сравнению с другими типами камер. Часто используют в торговых центрах для предотвращения хищений. Скрытную систему из 2-х или 4-х миниатюрных IP-камер (как правило, беспроводных) легко развернуть в конкретном отделе. Данная система мобильна, и её можно быстро перенести на другой подозрительный участок.

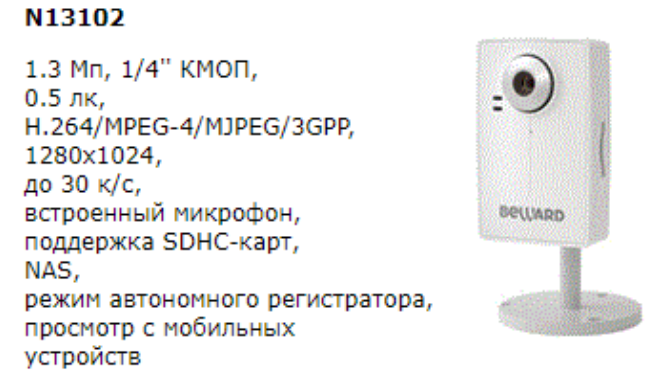

Рис. 6.10. Пример миниатюрной сетевой камеры

Мегапиксельные сетевые телекамеры

Используют в качестве фотоприемника матрицу мегапиксельного разрешения для получения картинки, которая состоит из более чем миллион пикселов. Обычно минимальный формат кадра этих камер составляет 1280x1024 = 1,3 Мпс, максимальный более 10 Мпкс. Мегапиксельные видеокамеры используют для получения высокой детализации изображения и для наблюдения за обширной частью территории отсюда и область их применения: в розничной торговле, видеонаблюдение городского масштаба, ситуация на дорогах и т.д.

К недостаткам этого типа телекамер отнесем более низкую чувствительность по сравнению с камерами стандартного разрешения. Все дело в том, что чувствительность определяется количеством светового потока попадающего на ячейку матрицы. При примерно одинаковых размерах мегапиксельных и стандартных матриц, количество пикселей у первых значительно больше

1,3МПкс=1300000Пкс против *640x480=307200Пкс* у VGA матрицы

Следовательно размеры пикселя у мегапиксельной матрицы значительно меньше (например у 2-х МПкс матрицы формата 1/3” размер ячейки составляет 3мкм, а у VGA того же формата 7,5 мкм). Света на маленькую ячейку приходится соответственно меньше, отсюда и меньше чувствительность.

Рекомендации при выборе сетевой телекамеры

В настоящее время на рынке сетевых телекамер представлено огромное количество производителей как давно известных, так только, что появившихся. Как выбрать необходимую телекамеру, тем более у IP-камер функционал значительно шире в сравнении с аналоговыми камерами? Для этого необходимо задать себе и продавцу несколько вопросов:

- Какой тип телекамеры требуется? Корпусная, купольная, поворотная. Проводная/ беспроводная?
- Место установки? В помещении или на улице. Если на улице, то надо думать о термокожухе. Продумать защиту от вандалов, если есть такая необходимость. Нужно открытое или скрытое видеонаблюдение?
- Заранее определить все зоны видеонаблюдения, с целью избегания не охваченных зон и дублирования видео обзора. Продумать использование одной мегапиксельной телекамеры или нескольких фиксированных? Обзорное или детализированное изображение? Необходимы камеры с высокой детализацией, например для контроля кассовых операций?
- Насколько важно качество изображения? У разных камер качество отличается. Требования к светочувствительности камеры? Требования к освещенности? Необходим функционал: «День/Ночь»? Есть ли необходимость в ИК-прожекторах?
- Разрешение? Достаточно ли будет разрешения формата VGA или потребуется мегапиксельное разрешение. Необходимо оптическое увеличение?
- Будет ли в процессе видеонаблюдения участвовать оператор ВН?

- Интеллектуальные функции. Есть ли в техническом задании функции видеоанализа?
- Поддерживает ли выбранная сетевая камера все необходимые сетевые протоколы?
- Производитель. На рынке сейчас более 200 производителей сетевых телекамер. Вопрос: будет ли выбранный бренд существовать через год-два? Какой технический сервис Вам предложен? Гарантийное обслуживание?

6.5. Сетевые видеосерверы

Сетевой видеосервер – это устройство, предназначенное для работы в составе аналогово-цифровой системы видеонаблюдения и преобразования аналогового видеосигнала в цифровой формат для последующей передачи его по IP-сети. Различают несколько типов видеосерверов: одноканальные (рис. 6.11), четырехканальные - это наиболее распространенный вариант (рис. 6.12) и многоканальные (до 84-х входов) в стоечном исполнении (рис. 6.13).

Рис. 6.11. Одноканальный видеосервер

Рис. 6.12. Четырехканальный видеосервер

В настоящее время аналоговое видеонаблюдение всё ещё доминирует на рынке систем охранного телевидения (СОТ), более 90% установленных телекамер – аналоговые, и продолжительность эксплуатации камеры примерно 5-7 лет.

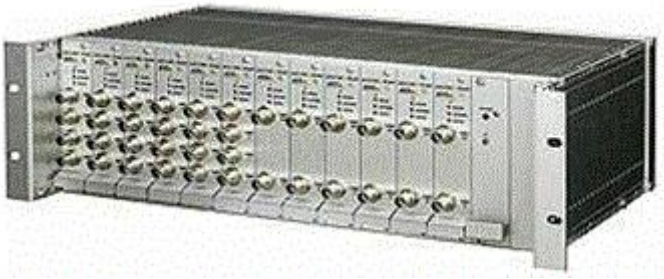

Рис. 6.13. Многоканальный видеосервер

При этом требования к функциональности системам видеонаблюдения растут год от года – это архивация большого объема видеоданных, быстрая передача видеопотоков на удаленные мониторы через сеть в том числе и удаленное управление телекамерами, интеграция с другими системами безопасности. В связи с этим перед производителями встала задача разработать переходное звено

между аналоговым и сетевым видеонаблюдением. Этим звеном и стал сетевой видеосервер (рис. 6.14).

Видеосерверы позволяют сохранить аналоговые видеокамеры и в то же время получить доступ к возможностям IP-видеонаблюдения. Через сетевой сервер можно осуществлять доступ и управление аналоговой камерой по сети, а аналоговые видеорегистраторы и аналоговые мониторы можно поменять на стандартные компьютерные мониторы и сервера.

Основные компоненты сетевого видеосервера

- *Система оцифровки сигнала*

  Представляет собой одну или несколько плат видеозахвата. Система принимает аналоговый сигнал и оцифровывает его для дальнейшей работы. Тип установленной платы определяет стандарт видеосервера PAL/NTSC. Количество плат оцифровки определяет потенциальное число подключаемых к видеосерверу телекамер.

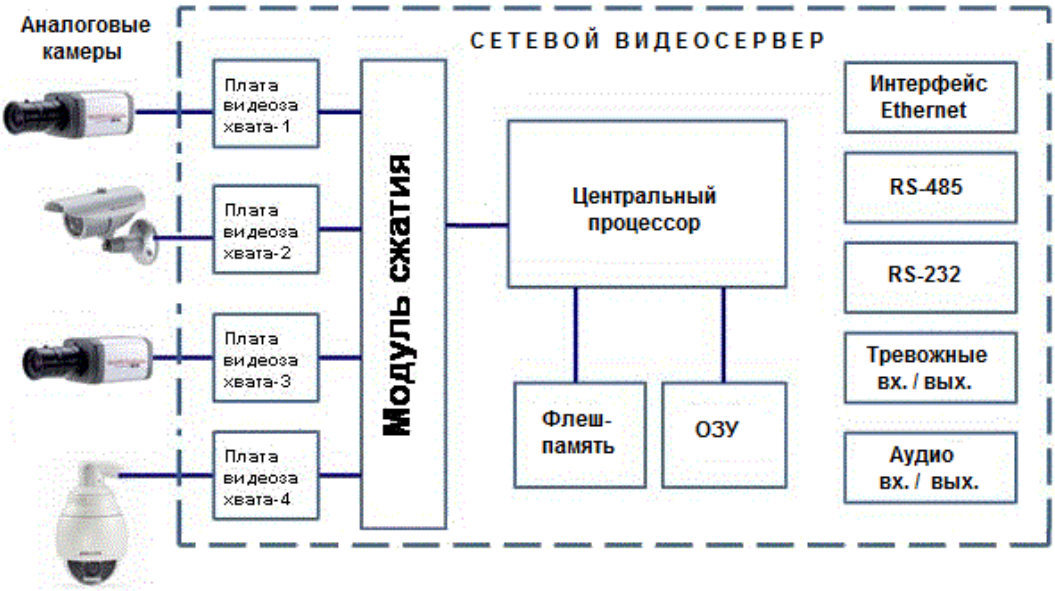

Рис. 6.14. Структурная схема сетевого видеосервера

- *Модуль сжатия изображения*

  Оцифрованный видеосигнал поступает в модуль сжатия видеосервера, где происходит преобразование видео в один из форматов сжатия H.264 - межкадровый алгоритм сжатия и MJPEG — покадровый. Процесс сжатия может быть реализован аппаратно или программно. Видеосерверы с программным сжатием - дешевле, но в них обработка сигнала происходит с задержкой, которая обусловлена повышенной нагрузкой на центральный процессор. Где необходимо создание системы видеонаблюдения реального времени, лучше использовать видеосервер с аппаратной компрессией.

- *Центральный процессор, флэш-память и оперативная память*

  Являются "мозгами" сетевого видеосервера с CPU, памятью и операционной системой, как правило, Linux. Основными функциями являются операции по выводу оцифрованного и сжатого видеосигнала в

сеть, а также выполнение программ веб-сервера и встроенного программного обеспечения.

В качестве процессора в видеосервере используют DSP-процессор или специализированную микросхему. Именно процессор определяет производительность сетевого сервера: максимальное количество кадров максимального разрешения в секунду. Как правило, лучшие представители передают изображение с разрешением D1 (720x576) со скоростью 25 кадров в секунду в PAL.

Флэш-память служит для хранения программного обеспечения, управляющего работой видеосервера:

- операционной системы,
- управляющих программ,
- различных приложений
- и пользовательских HTML-страниц.

ОЗУ сетевого видеосервера служит для хранения временных данных, которые генерируются при выполнении программ. В большинстве видеосерверов некоторая часть ОЗУ представляет собой так называемый видеобуфер.

Видеобуфер – это часть ОЗУ, используемая для временного хранения текущей видеоинформации. Наличие видеобуфера предоставляет оператору возможность восстановления видеоинформации, связанной с сигналом тревоги. В процессе работы видеосервер записывает поступающую видеоинформацию в видеобуфер и постоянно ее обновляет.

Если видеосервер получает сигнал тревоги от подключенных к нему охранных извещателей или с детектора движения, то им автоматически формируется и отсылается на заранее заданный адрес e-mail или FTP набор кадров, предшествующих, следующих и соответствующих сигналу тревоги.

- *Сетевой интерфейс/ адаптер*

Система доступа к IP-сети представляет собой, как правило, типовые интерфейсы локальных сетей Ethernet или 10BaseT/100BaseTX. Большинство моделей современных видеосерверов поддерживает стандартные сетевые протоколы TCP/IP, UDP, SMTP, IGMP, ARP, RAPP, FTP и т.д., что позволяет передавать видеосигнал, как по локальным, так и по глобальным сетям.

- *Последовательные порты (R-232 и RS-485)*

Позволяют управлять через видеосервер PTZ-функциями поворотных камер или подключить видеосервер к соответствующему интерфейсу видеозаписывающего устройства.

Если необходимо установить удаленное соединение видеосервера с сетью Интернет, то через последовательный порт можно также подключить модем.

Основные функциональные возможности сетевого видеосервера

- Управление телеметрией.

  Встроенный приемник телеметрии позволяет управлять поворотным устройством подключенной аналоговой видеокамеры и изменением фокусного расстояния объектива. Управление телеметрией дает возможность фокусировать видеокамеру на отдельных деталях и наблюдать за обширным пространством с разных ракурсов. Видеосерверы поддерживают множество различных протоколов телеметрии для видеокамер наиболее известных производителей.

- Видеодетектор движения

  Это программный или аппаратный модуль, основной задачей которого является обнаружение перемещающихся объектов в поле зрения видеокамеры. Детектор движения не только обнаруживает движение, но и определяет габариты объекта и скорость его движения.

- Обработка тревожных событий.

  Почти все видеосерверы имеют блок цифровых входов, которые служат для подключения к видеосерверу внешних охранных датчиков. Таким образом оператор может настроить видеосервер на срабатывание по внешнему событию. С помощью релейного выхода можно установить выполнение определенных действий, например, подачу питания на электромеханический замок двери. Если видеосервер имеет видеобуфер, то при поступлении сигнала тревоги он может посылать по сети набор кадров, поступивших на видеосервер до, после и в момент тревоги.

- Передача звука.

  Большинство видеосерверов оснащено аудиоканалом для однонаправленной или двунаправленной передачи звука по сети. Как правило, аудиосигнал, синхронизирован с видео.

- Поддержание функции PoE,

  Данная функция позволяет запитывать по сети не только видеосервер, но и аналоговые видеокамеры.

- Программное обеспечение.

  Просмотр видеоизображения и управление видеокамерой при наличии видеосервера можно осуществлять с помощью стандартного веб-браузер. Тем не менее, многие производители поставляют вместе с видеосерверами собственное программное обеспечение, помогающее удаленно просматривать видеоинформацию, осуществлять настройку параметров камер. Как правило, такое программное обеспечение совместимо только с видеосерверами и другим сетевым оборудованием того же производителя и поставляется бесплатно.

Рекомендации при выборе сетевого видеосервера

В данное время на рынке видеосерверов существует большое количество производителей. Как выбрать необходимое оборудование, тем более, что все оно

обладает разными функциональными возможностями. Какие вопросы возникают при выборе сетевого видеосервера

- Сможет ли он обеспечить высокое качество изображения? Реализован ли деинтерлейсинг (англ. Deinterlacing – устранение чересстрочности) — процесс создания одного кадра из двух полукадров чересстрочного формата для дальнейшего вывода на экран с прогрессивной развёрткой, такой как компьютерный монитор.
- Какие форматы кадра поддерживает?
- Какие форматы сжатия поддерживает?
- Сколько каналов, и при какой максимальной скорости транслирует кадр максимального разрешения?
- Насколько прост в инсталляции и обслуживании?
- Стоечное или настольное исполнение?

При выборе сетевого сервера ключевыми характеристиками должны быть надежность и качество.

6.6. Устройства записи и хранения

При регистрации и хранении больших массивов видеоинформации обычно сталкиваются с двумя основными проблемами, которые связанны с работой жёстких дисков. Это сравнительно низкая скорость записи/чтения диска и необходимость повышения их отказоустойчивости.

Одними из направлений, которые позволяют избежать или, по крайней мере, существенно снизить отмеченные выше недостатки является использование RAID-массивов. Что же это такое, и почему они помогают в разрешении указанных выше проблем?

6.6.1. RAID-массивы

RAID (англ. Redundant Array of Independent Disks) – это избыточный массив независимых дисков, который состоит из нескольких дисков, управляемых одним контроллером, связанных между собой скоростными каналами передачи данных и воспринимаемых внешней системой как единое целое.

В зависимости от типа используемый массив может обеспечивать различные степени отказоустойчивости и быстродействия. Служит для повышения надёжности хранения данных и/или для повышения скорости чтения/записи. За счет параллельного выполнения операций ввода-вывода обеспечивается высокое быстродействие системы, а повышенная надежность хранения информации достигается дублированием данных или вычислением контрольных сумм.

Чтобы не снижать быстродействие системы, рекомендуется использовать аппаратные RAID-контроллеры, а не программные. Существует несколько уровней RAID-массивов с разной степенью избыточности. Сейчас наиболее распространены уровни: RAID-0 и RAID-1.

RAID-0 – это дисковый массив из двух или более жёстких дисков без резервирования. То есть, по сути, эти устройства RAID-массивом не являются.

Они работают под управлением общего для всех дисков контроллера, и при их использовании записываемая/считываемая информация разбивается на блоки данных фиксированной длины и записывается на оба или несколько дисков одновременно (рис. 6.15).

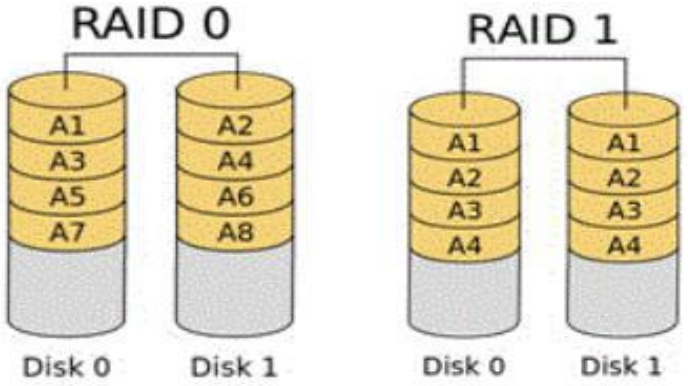

Рис. 6.15. Структурная схема RAID-0 и RAID-1.

Преимущества:

- повышается производительность, от количества дисков зависит кратность увеличения производительности;
- простота реализации;
- низкая стоимость;
- максимальная эффективность использования дискового пространства, которая составляет почти 100%.

Недостатки:

- не является настоящим RAID-массивом, поскольку не поддерживает отказоустойчивость;
- надёжность RAID-0 заведомо ниже надёжности любого из дисков в отдельности. Она падает с увеличением количества входящих в RAID-0 дисков, так как отказ любого из дисков приводит к неработоспособности всего массива.

RAID-1 (mirroring – «зеркалирование») – массив из двух дисков, являющихся полными копиями друг друга. Информация, которая записывается на один HDD, полностью дублируется ещё на одном или нескольких жестких дисках.

Преимущества:

- Имеет высокую надёжность– работает до тех пор, пока функционирует хотя бы один диск в массиве. Вероятность выхода из строя сразу двух дисков равна произведению вероятностей отказа каждого диска, т.е. значительно ниже вероятности выхода из строя отдельного диска. На практике при выходе из строя одного из дисков следует срочно принимать меры — вновь восстанавливать избыточность.

Недостатки:

- По цене двух дисков пользователь фактически получает лишь один.

На практике широкое применение получили RAID-5 с чередованием и контролем четности. Данные и контрольные суммы распределяются по трем и

более жестким дискам, объем массива будет равен сумме емкости всех HDD минус емкость одного. Массив RAID-6, аналогичен массиву RAID-5, но с двумя контрольными суммами. Требуется минимум четыре HDD, но при этом можем выдержать выход из строя сразу двух жестких дисков, объем массива будет равен сумме емкости всех HDD минус емкость двух жестких дисков. При реализации RAID-массива необходимо учесть, что диски должны быть одного объема, так как в противном случае часть объема большего носителя останется неиспользованной.

Следует отметить, что в современных сетевых системах видеонаблюдения наряду с RAID-массивами используются и иные системы хранения данных – это сетевые устройства хранения (NAS) и высокоскоростные специализированные сети хранения данных (SAN).

6.6.2. Сетевые устройства и сети хранения данных

NAS (Network Attached Storage)[1] – это сетевое устройство хранения, то есть хранилище данных, подключаемое непосредственно в сеть. При подключении NAS в IP-сеть пользователям для хранения информации становятся доступны дисковые ресурсы, представленные как сетевые папки. Передача данных осуществляется по файловым протоколам обмена.

Технология NAS позволяет осуществлять доступ к каталогам пользователям различных операционных систем и имеет очень гибкую настройку по правам доступа. Системы NAS просты в установке и не требуют клиентских лицензий ПО на доступ к хранилищу (рис. 6.16). Последнее особенно важно при большом числе подключений.

Рис.6.16. NAS-система для малого бизнеса от компании NetGear.

Системы NAS содержат один или несколько жестких дисков, которые объединены в RAID-массивы с возможностью восстановления данных при сбое. Сейчас часто используется RAID 5,6. В NAS системах используются такие сетевые протоколы, как NFS (UNIX), SMB (Windows NT), AFP (Apple Macintosh) или NCP (OES и Novell NetWare). Обычно у систем NAS присутствует множество протоколов.

SAN (Storage Area Network)[2] – высокоскоростная специализированная сеть, объединяющая устройства хранения. Пользователи могут обращаться к любому

[1] https://ru.wikipedia.org/wiki/NAS
[2] https://ru.wikipedia.org/Сеть_хранения_данных

из этих устройств хранения через серверы, общий объем SAN может достигать нескольких сотен терабайт. Концепция централизованного хранения упрощает администрирование и предоставляет гибкое и высокоскоростное решение для мультисерверных систем.

Основное отличие SAN от NAS состоит в том, что в NAS-устройствах файл целиком сохраняется на жестком диске, а в сетях SAN файл разбивается на блоки и записывается на нескольких HDD.

Большинство сетей хранения данных использует протокол SCSI для связи между серверами и устройствами хранения данных на уровне шинной топологии. Так как протокол SCSI не предназначен для формирования сетевых пакетов, в сетях хранения данных используются низкоуровневые протоколы, такие как:

- Fibre Channel Protocol (FCP), транспорт SCSI через Fibre Channel.
- iSCSI, транспорт SCSI через TCP/IP.

iSCSI (англ. Internet Small Computer System Interface)[3] – протокол, который базируется на TCP/IP и разработан для установления взаимодействия и управления системами хранения данных, серверами и клиентами.

В процессе проектирования системы видеонаблюдения на этапе выбора сервера и системы хранения данных важным является решения проектировщика по следующей группе вопросов:

- Имеются ли предпочтения в выборе программной или аппаратной платформы?
- Требуется система видеонаблюдения с централизованной или децентрализованной структуры?
- Какой уровень надежности системы требуется? Какой уровень избыточности RAID-массива?
- Какой требуется объем и глубина архива архива? Методику расчета глубины архива можно найти в сети Интернет по адресу http://daily.sec.ru/publication.cfm?pid=38858, https://www.jvsg.com/online-calculator-arhiva-videonablyudeniya/
- Сколько будет сетевых телекамер? Какого разрешения будут видеокамеры? Будет их наращивание? Применяйте расчет пропускной способности сети. Типовой расчет можно найти по адресу: http://daily.sec.ru/publication.cfm?pid=38706.
- Требуется ли отдельный сервер мониторинга? На практике, если количество сетевых телекамер более 30, используют раздельные сервер записи и сервер мониторинга.

6.7. Программное обеспечение сетевых систем видеонаблюдения

Программное обеспечение (ПО) является неотъемлемой составляющей всех систем сетевого видеонаблюдения. Оно обеспечивает необходимые сервисы для мониторинга, записи, управления и видеоанализа информации. Правильный

[3] https://ru.wikipedia.org/wiki/ISCSI

выбор программной платформы требует учета многих факторов в зависимости от масштаба, гибкости и функциональности системы.

Если необходимо просматривать информацию с одной или двух сетевых камер, то достаточно использовать стандартный веб-сервер, установленный на самой камере или видеосервере. Если система состоит из большего числа камер, то рекомендуется использовать специализированное ПО. При этом существует два варианта поставки программных платформ для сетевого видео:

- программное обеспечение, которое устанавливается на сервер или ПК;
- на базе сетевого видеорегистратора (англ. Network Video Recorder, NVR).

Решение на базе сервера или ПК предполагает использование стандартных компьютерных составляющих, а требуемое ПО работает под управлением ОС Windows или Linux. ПО может поставляться отдельно с его последующей установкой самим пользователем либо с “заводской” установкой.

Системы на базе сервера полностью масштабированы. То есть система лицензирования предусматривает, что для добавления IP-телекамер требуются лицензии, которые можно последовательно добавлять при подключении дополнительных камер.

Рис. 6.17. Вариант системы видеонаблюдения на базе сервера

Вариант на базе NVR представляет собой законченное аппаратное решение с уже установленным ПО. Его софт предназначен строго для определенных задач: записи, мониторинга и анализа видео. На сетевые видео регистраторы нельзя установить другие программы. Аппаратная конфигурация строго привязана к его программному обеспечению.

Аппаратная составляющая NVR чаще всего имеет специализированный характер. Сетевой регистратор рассчитан на работу с определенным количеством IP-телекамер, то есть менее гибкий вариант. Данное решение, как правило, проще

в установке и настройке и используется в системах сетевого видеонаблюдения, в которых количество телекамер не превышает максимум входов NVR и не предполагается наращивание.

Рис. 6.18. Вариант системы видеонаблюдения на базе сервера

Собственные программные платформы имеются и у производителей IP-телекамер и у производителей сетевых видеосерверов. Как правило, такие производители поддерживают только собственные продукты. Существуют открытые программные платформы, которые поддерживают устройства различных производителей, в большинстве случаев открытые платформы обеспечивают максимальную гибкость для пользователя при проектировании системы сетевого видеонаблюдения.

Сетевые телекамеры/видеосерверы имеют встроенный веб-сервер с IP-адресом, поэтому просмотр и конфигурацию можно осуществлять в обычном веб-браузере после ввода в его адресной строке IP-адреса устройства. Подключившись к сетевому устройству, на мониторе компьютера Вы увидите его стартовую страницу с окном просмотра изображения и ссылки на страницы конфигурирования. Запись видео и получение отдельных снимков зачастую осуществляется нажатием правой кнопки мышки в окне просмотра. Конфигурирование и администрирование через его встроенный веб-сервер имеет смысл при незначительном количестве IP-устройств.

Большинство программных средств имеют собственный оконный интерфейс. Для крупномасштабных систем и когда требуется удаленная станция мониторинга, клиентское ПО для просмотра устанавливается на отдельный компьютер, а не на сервер записи, на котором установлено основное программное обеспечение системы видеонаблюдения. Клиентское приложение позволяет пользователю выполнять все те же функции, что и основное ПО установленное на сервере. Программные платформы систем видеонаблюдения имеют следующие основные функции:

- Одновременный просмотр изображений от нескольких телекамер.

- Запись видео. Имеется несколько режимов записи: постоянно, по детекции движения, по расписанию, по сигналу от тревожного входа. Предусмотрен выбор параметров качества записи: MJPEG, H.264. Выбор скорости записи.
- Запись аудио. Реализуется за счет встроенных микрофонов в сетевую телекамеру. Важна синхронизация видео и аудио потоков.
- Администрирование и конфигурирование телекамер. Программное обеспечение предоставляет возможность добавлять новые видеокамеры и конфигурировать их параметры, скорость трансляции, формат сжатия кадра.
- Управление тревожными событиями.
- Поиск в видеоархиве. Просмотр видео в архиве. Большинство программных платформ используют для хранения записей стандартную файловую систему Windows. Программные платформы позволяют хранить данные более чем на одном устройстве: на основном HDD, на локальные диски, сетевые диски и т.п. Можно задать время в течение, которого запись будет храниться. Многие программы обладают функцией синхронного просмотра видеозаписей с нескольких камер, это позволяет оператору получить детальную картину события.
- Видиодетектор движения - стал стандартной функцией в программном обеспечении систем видеонаблюдения. Принцип действия основан на сравнении последовательности кадров и обнаружении в них изменений. Если в/детектор отсутствует в IP-телекамере, то его может предоставить ПО видеонаблюдения, т.е. сетевая телекамера посылает изображение на сервер, а программное обеспечение уже анализирует его. Видиодетектор движения существенно сокращает объем записываемой видеоинформации. Видиодетектор может анализировать как часть изображения, так и целиком. Программно пользователь может устанавливать различный уровень чувствительности для работы в условиях нормальной и низкой освещенности. При обнаружении движения ПО может: активизировать внешние устройства (включить свет, сирену), начать запись видео от выбранных телекамер, послать сообщение по электронной почте и т.п.
- Разграничение прав пользователя. Ведение журнала системных событий. Программное обеспечение поддерживает следующие функции: авторизация пользователей, пароль, разграничение прав доступа: администратор, оператор, пользователь. Системный журнал необходим, если нужно установить, кто и когда имел доступ к системе и какие при этом совершались действия в системе сетевого видеонаблюдения.

Программные платформы IP-видеонаблюдения могут быть интегрированы с другими системами, которые используют протокол IP для передачи данных. Например, интеграция со СКУД, ОПС, контрольно-кассовыми системами. При такой интеграции информация, полученная от других систем безопасности, будет являться триггером для запуска режима записи, а пользователь получает один

интерфейс для управления несколькими системами. На рынке доступно ПО, как отечественных производителей (Интеллект, VideoInspector, Smart Video, Видео Гарант, VideoNet, Трассир, Эвклид, BEWARD, и др.), так и зарубежных гигантов Axis, Sony, Bosch, Panasonic.

Рекомендации при выборе программных платформ:

- На чем стоит остановить свой выбор: сетевой видеорегистратор или компьютерный сервер?
- Масштабируемость. Некоторые программы имеют ограничения по возможности наращивания количества IP-телекамер, но за то просты в инсталляции и в работе. А другие работают с тысячами камер.
- Функциональность. Достаточно ли простой системы (просмотр, запись) или необходим большой набор видеоаналитики.
- Открытая программная платформа или платформа привязанная к одному производителю.
- Нужна ли Вам интеграция с другими системами безопасности?

6.8. Основные понятия и технические характеристики видеокамер

6.8.1. Основные стандарты видеокамер

С целью совместимости различных видов оборудования (видеокамер и мониторов) и различных производителей были разработаны телевизионные стандарты. В Стокгольме в 1961 году на международной конференции были приняты стандарты телевизионных вещательных систем, определяющие основные характеристики телевизионного сигнала для каждой системы.

Рис. 6.19. Советская портативная телекамера КТ-190

Телевизионный стандарт – это метод передачи изображений в виде электрических сигналов. Понятие телевизионного стандарта включает в себя значительное количество параметров: несущая частота, частота разверток, систем цветности и т.д. В аналоговом телевидении существуют три основных системы передачи сигналов цветного телевидения:

- PAL (Phase Alternation Line - изменение фазы от строки к строке) - западногерманская система.
- SECAM (Sequentiel couleur a memoire - последовательная передача цветов с запоминанием) - советско-французская система.
- NTSC (National Television System Committee) - американская система.

Эти стандарты несовместимы друг с другом. Так, например, телекамера стандарта PAL не могла работать с монитором SECAM, без специального оборудования (декодер), и наоборот.

Первоначальное значение слова «видеокамера соответствовало комбинация телевизионной передающей камеры и устройства для видеозаписи. Впервые слово «видеокамера» стало использоваться применительно к миниатюрным ручным телекамерам, предназначенным для записи домашнего видео на бытовой видеомагнитофон. Впоследствии слово «видеокамера» практически вытеснило слова «телевизионная камера» и «телекамера» (ТВ-камера), заменив их.

Создание *цифровых видеокамер* базируется на двух существенных научно-технических достижениях конца прошлого века, это:

- Возможность использование для сканирования изображения вместо передающих электронных телевизионных трубок твёрдотельных датчиков изображения, на основе приборов с зарядовой связью или КМОП-матриц.
- Разработка эффективных алгоритмов сжатия видео, поскольку высокие требования, предъявляемые к объёмам памяти и пропускной способности каналов, делали работу с несжатым видео не реалистичной.

Наиболее важным алгоритмом сжатия в этом отношении является дискретное косинусное преобразование (ДКП), метод сжатия с потерями, который впервые был предложен в 1972 году. Появление реальных цифровых видеокамер стало возможно благодаря ДКП стандартам сжатия видео, включая стандарты кодирования видео H.26x и MPEG, введённые с 1988 года. В настоящее время по качеству разрешения выделяют следующие типы видеокамер:

- Стандартной чёткости (SD, Standard Definition):
  - для аналоговых видеокамер: 576 строк при 25 кадрах в сек (PAL) или 480 строк при 30 кадрах в сек (NTSC);
  - для цифровых видеокамер: 720x576 точек при 25 кадрах в сек и 720x480 точек при 30 кадрах в сек.
- Высокой чёткости (HD, High Definition):
  - HD Ready: 720 строк (1280x720 точек);
  - Full HD: 1080 строк (1920x1080 точек);

Некоторые типы видеокамер могут использоваться для съёмки цифрового кино, но кинематографические стандарты разрешения 2K, 4K и другие, поддерживают только цифровые кинокамеры

Веб-камера – это цифровая видео- или фотокамера, способная в реальном времени фиксировать изображения, предназначенные для дальнейшей передачи по сети Интернет (в программах типа Skype или другом видео приложении).

Первая в мире веб-камера была запущена в 1991 году и показывала кофеварку в Троянской комнате Кембриджского университета (рис. 6.20). Сейчас она не работает, так как была отключена 22 августа 2001 года. Последний фотоснимок, сделанный этой камерой, ещё можно видеть на ее странице в Интернете.

Веб-камеры, доставляющие изображения через Интернет, закачивают изображения на веб-сервер либо по запросу, либо непрерывно, либо через регулярные промежутки времени.

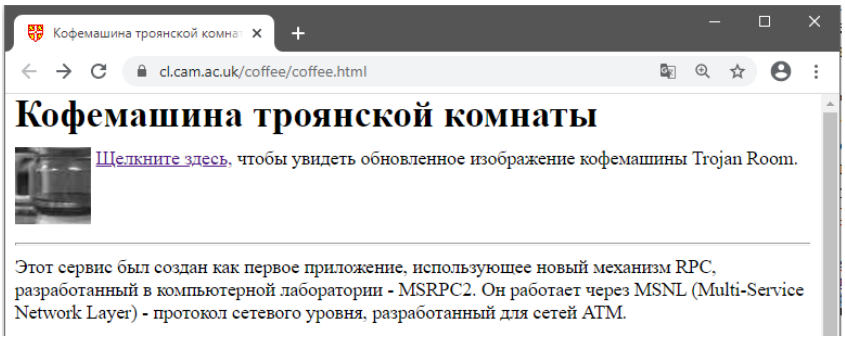

Рис. 6.20. Домашняя страница первой в мире веб-камеры.

Это достигается путём подключения камеры к компьютеру или благодаря возможностям самой камеры. Некоторые современные модели обладают аппаратным и программным обеспечением, которое позволяет камере самостоятельно работать в качестве веб-сервера, FTP-сервера, FTP-клиента и (или) отсылать изображения электронной почтой.

6.8.2. Типы фотоприемных матриц, используемых в видеокамерах

Основным элементом, самым технологически сложным и дорогим в денежном эквиваленте, любой видеокамеры является фотоприемная матрица. Именно матрица определяет основные технические характеристики камеры. Рассмотрим этот вопрос более подробно. Современные видеокамеры строятся на 2-х типах матриц:

- ПЗС-матрица (CCD, Charge-Coupled Device. прибор с зарядовой связью)
- КМОП-матрица на транзисторах металл-оксид-полупроводник (CMOS, Complementary Metal-Oxide Semiconductor).

Основное преимущество ПЗС-матриц заключается в их достаточно высокой чувствительности.

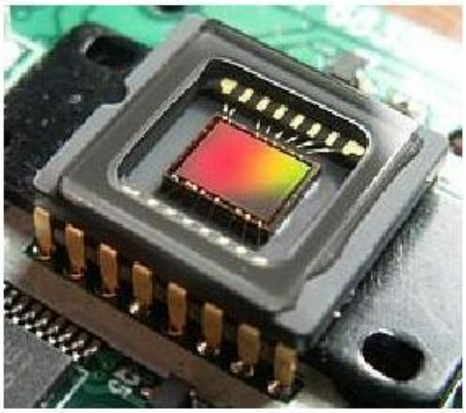

Рис. 6.21. Внешний вид ПЗС-матрицы.

ПЗС-матрица – специализированная аналоговая интегральная микросхема, состоящая из светочувствительных фотодиодов, выполненная на основе кремния, использующая технологию ПЗС — приборов с зарядовой связью. Основные размеры матриц: 1/3, 1/2 и 2/3 дюйма.

CCD-матрица – это кремниевый чип, покрытый множеством маленьких электродов, которые называются фотоэлементами/фотосайтами (Photosites). Фотоэлементы выстроены в виде решетки, и каждый из них соответствует одному пикселю на полученном кадре. То есть, количество фотоэлементов соответствует разрешению изображения. Изображение будет состоять из стольких пикселей, сколько элементов содержит матрица.

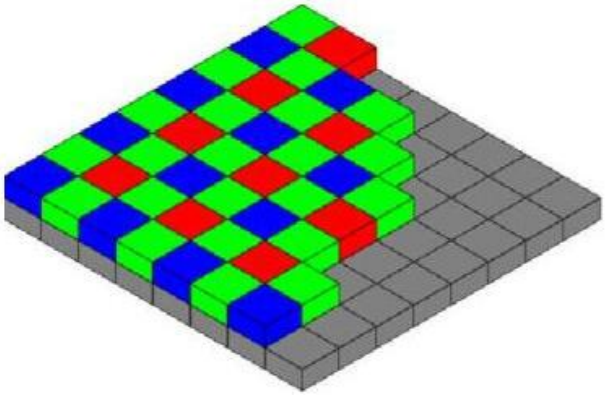

Рис. 6.22. Устройство цветной ПЗС-матрицы.

Фотосайты не различают цветов, они воспринимают только интенсивность света. Чтобы получить цветное изображение, используют цветовые фильтры (маски) для матрицы. Самой распространенной является схема, основанная на шаблоне Байера (рис. 6.22).

Этот шаблон состоит из 4 фильтров - двух зеленых, одного красного и одного синего. Глаз человека воспринимает зеленый цвет лучше, чем остальные, поэтому изображение, насыщенное зеленым, субъективно воспринимается более натуральным. Из-за своей структуры схема Байера иногда называется GRGB (зеленый-красный-зеленый-синий).

Обозначения на схеме субпикселя ПЗС:

1. фотоны света, прошедшие через объектив фотоаппарата;
2. микролинза субпикселя;
3. R — красный светофильтр субпикселя, фрагмент фильтра Байера;
4. прозрачный электрод из поликристаллического кремния или сплава индия и оксида олова;
5. оксид кремния;
6. кремниевый канал n-типа: зона генерации носителей — зона внутреннего фотоэффекта;
7. зона потенциальной ямы (карман n-типа), где собираются электроны из зоны генерации носителей заряда;
8. кремниевая подложка p-типа.

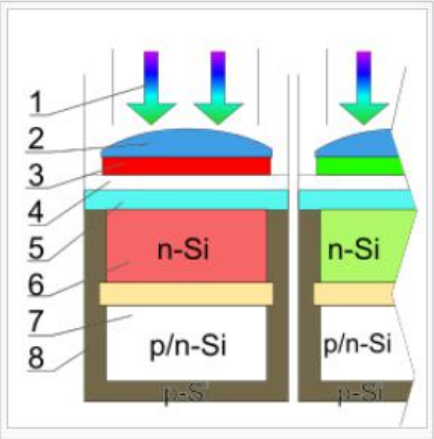

Рис. 6.23. Схема субпикселей ПЗС-матрицы с карманом n-типа (на примере красного фотодетектора)[4].

Современные технологии CCD-матриц отличаются тем, что они обладают повышенной светочувствительностью, которая в свою очередь способствует существенному улучшению качества принимаемого изображения. Среди таких технологий можно выделить две основные:

[4] https://ru.wikipedia.org/wiki/ПЗС-матрица

Super HAD CCD – технология повышения чувствительности CCD-матрицы. Разработчиком является компания Sony. Для повышения светочувствительности над каждым фотоэлементом (пикселем) сформирована специальная микролинза, которая собирает свет из «мёртвых» зон между пикселями, сводя к минимуму потери отражённого света, а кроме этого полупроводниковая система HAD (Hole-Accumulation Diode) позволяет уменьшить влияние шума.

Super HAD II CCD – усовершенствованная, вторая версия, технологии повышения светочувствительности ПЗС-матрицы. По сравнению с первой версией были увеличены апертура и область фотоэлемента, чувствительная к свету. Оптимизированы высота и форма микролинз, за счёт чего матрица стала ещё меньше. Усовершенствованы цветовые фильтры. Чувствительность к свету увеличилась на 7 Дб.

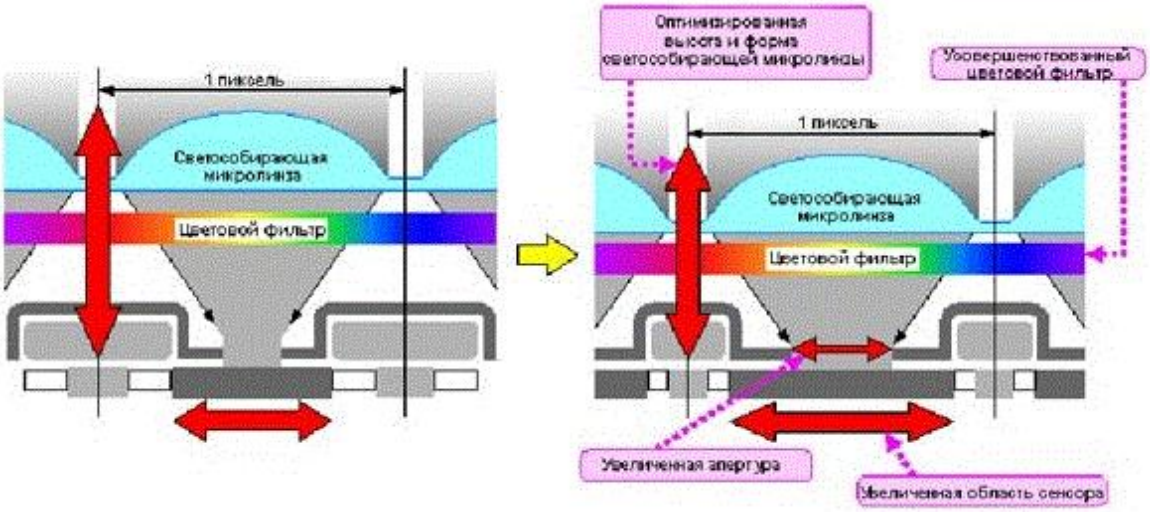

Рис. 6.24. Схематичное решение технологий Super HAD CCD (слева) и Super HAD II CCD (справа).

КМОП-матрица — представляет собой светочувствительную матрицу, выполненную на основе КМОП-технологии (рис. 6.25).

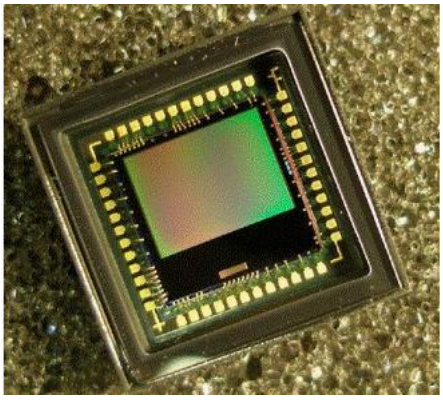

Рис. 6.25. Внешний вид КМОП-матрица под увеличением.

Важным преимуществом КМОП матрицы является единство технологии, т.е. объединение на одном кристалле аналоговой, цифровой и обрабатывающей части. Не только «захват» света, но и процесс преобразования, обработки, очистки сигналов, что послужило основой для миниатюризации камер для самого разного оборудования и снижения их стоимости ввиду отказа от дополнительных

процессорных микросхем. Из миниатюризации вытекает следующий «плюс» – низкое энергопотребление в статическом состоянии. Это позволяет применять такие матрицы в составе энергонезависимых устройств.

Описав особенности каждого из типов фоточувствительных матриц, проведем теперь сравнительный анализ достоинств и недостатков каждого рассмотренного типа матриц:

Преимущества CCD матриц:

1. Высокая чувствительность (динамический диапазон).
2. Высокий коэффициент заполнения пикселов (около 100%).
3. Высокая эффективность (отношение числа зарегистрированных фотонов к их общему числу, попавшему на светочувствительную область матрицы, для CCD — 95%).
4. Низкий уровень шумов.

Недостатки CCD матриц:

1. Сложный принцип считывания сигнала, а следовательно и технология.
2. Высокий уровень энергопотребления (до 2-5Вт).
3. Дороже в производстве.

Преимущества CMOS матриц:

1. Высокое быстродействие (до 500 кадров/с).
2. Низкое энергопотребление (почти в 100 раз по сравнению с CCD).
3. Дешевле и проще в производстве.

Недостатки CMOS матриц:

1. Невысокая чувствительность.
2. Высокий уровень шума (он обусловлен так называемыми темповыми токами — даже в отсутствие освещения через фотодиод течет довольно значительный ток).
3. Низкий коэффициент заполнения пикселов, что снижает чувствительность (эффективная поверхность пиксела ~75%,остальное занимают транзисторы).

6.8.3. Основные технические характеристики видеокамер

При проектировании и эксплуатации сетевых систем видеонаблюдения наиболее важным является выбор, размещение и установка видеокамер, наиболее соответствующих местам их размещения. Естественно, что такой выбор может быть осмысленным и обоснованным только в том случае, если у разработчиков есть достаточно хорошее представление о технических возможностях современных видеокамер. С этой целью рассмотрим основные технические характеристики и параметры выпускаемых в настоящее время видеокамер:

Разрешение видеокамеры

Измеряется в телевизионных линиях (ТВЛ). При этом различают разрешение камеры по горизонтали и по вертикали. Разрешение по горизонтали - это максимальное число вертикальных линий, которое способна передать камера,

например, на видеомониторы. Оно определяется в первую очередь количеством пикселей по горизонтали в ПЗС-матрице, а также электронной схемой камеры.

Как правило, этот параметр не превышает число пикселей в строке, умноженное на 0,75. Разрешение по вертикали ограничено стандартом CIR/PAL до 625 строк и 470 строк в EIA/NTSC. Если принимать во внимание кадровые синхроимпульсы, уравнивающие строки и пр., то максимальная разрешающая способность по вертикали оказывается равной 575 строк в CCIR/PAL и 470 строк в EIA/NTSC.

Для цифровых камер технологии «Высокого Разрешения» (High Definition) обычно используются следующие показатели:

```
 2 Мпкс = 1920 x1080 – Full HD или HD Ready1080p,
1,3Мпкс = 1280 x 1024,
 3 Мпкс = 2048 x 1536,
 5 Мпкс = 2592 x 1944,
10 Мпкс = 3648 x 2752.
```

Качество изображения зависит от показателя разрешения модели камеры. На отечественном рынке наибольшее распространение получили ч/б камеры с разрешением 380-600 ТВЛ и цветные аналоговые с показателем 330-540 ТВЛ. Если оборудование планируется использовать для контроля за удаленными объектами крупных размеров, то можно использовать камеру 380-420 ТВЛ. Но если на охраняемой территории есть мелкие детали (в супермаркетах, банковских учреждениях и т.д.), предпочтительнее устанавливать оборудование высокой четкости – 560-600 ТВЛ. Такие камеры обеспечивают максимально точную и полную картинку.

Чувствительность видеокамеры

Этот параметр определяет качество работы камеры при низкой освещенности. От 0 (полная темнота) до 15 люкс. Типовые значения 0,1Лк (для цветных видеокамер), 0,01-0,0001 Лк (для черно-белых без DSS и DSS), 0 Лк — при использовании ИК-подсветки.

Очень важный параметр при выборе видеокамеры. Нередко картинка с дисплея исчезает уже в сумерках, особенно это касается цветных камер наблюдения. Поэтому для ночной видеозаписи лучше выбирать модели с опцией «день/ночь». Их преимущество состоит в способности автоматически переходить в черно-белый режим, как только степень освещенности снизиться до критического уровня.

Фокусное расстояние объектива

Определяет его угол зрения и степень увеличения предмета в данной точке съёмки. Наиболее востребованные значения — 2,5/ 3.6 / 4,3/ 6 / 8 / 12 / 16 мм. Чем меньше фокусное расстояние, тем больше угол обзора.

Расчёт угла обзора в зависимости от фокусного расстояния и типа матрицы может быть выполнен по следующим формулам:

$$F = v*S/V \quad \text{или} \quad f = h*S/H,$$

```
где
  f — фокусное расстояние
  v — вертикальный размер матрицы
  V — вертикальный размер объекта
  S — расстояние до объекта
  h — горизонтальный размер матрицы
  H — горизонтальный размер объекта
```

Примерные соответствия:

```
  2,5мм — 120 град., дистанция наилучшего качества - 0,7м,
                     дистанция распознавания - 2 м;
  3,6мм —  72 град., дистанция наилучшего качества – 1,5м,
                     дистанция распознавания - 3,5м;
  16 мм —  17 град., дистанция наилучшего качества –   6м,
                     дистанция распознавания - 16 м.
```

Напряжение питания

12VDC, 24VDC, 24VAC, 220VAC. Для питания видеокамер, в зависимости от их назначения и фирмы-изготовителя, как правило, применяются постоянные напряжения 12В, 24В и переменные напряжения 24В, 220 В.

Ток потребления

Типовые значения для: купольной видеокамеры — 120мА, для корпусной видеокамеры — 160мА, уличная видеокамера с ИК — 540мА. Ток потребления камеры – параметр необходимый для выбора источника питания (по мощности), а так же для выбора сечения провода кабеля.

Температурный диапазон

Для внутренних от -10 до +50 град, уличных от -40 до +50 град..

6.8.4. Дополнительные специальные функции видеокамер

*Телевизионные камеры день/ночь.*До недавнего времени в/камеры СОТ разделялись на черно-белые и цветные. По мере увеличения доли цветных камер, все больше проявлялся их главный недостаток - более низкая чувствительность по сравнению с ч/б камерами (в 7 -10 раз). Для решения этой проблемы было предложено в ночное время переводить цветные камеры в ч/б режим. Так появились камеры класса "день/ночь".

*Электронное увеличение чувствительности (DSS) -режим накопления заряда (DSS).*Функция DSS позволяет получать более яркое изображение даже при очень низкой освещенности. При низкой освещенности видеокамера формирует качественное изображение за счет увеличения времени экспозиции, благодаря чему на элементах CCD-матрицы происходит более полное накопление зарядов и тем самым обеспечивается более высокое качество изображения. При этом скорость электронного затвора видеокамеры регулируется автоматически в зависимости от количества света, попадающего на CCD-матрицу.

*Компенсация задней засветки (BLC).*Это функция видеокамеры, которая позволяет управлять автоматической регулировкой усиления и электронным затвором не по всей площади экрана, а по его центральной части, что позволяет

компенсировать излишек освещения, мешающий восприятию. Если свет за объектом яркий и направлен прямо в объектив, то диафрагма сужается, и объект переднего плана выглядит темным и размытым на изображении. Благодаря функции BLC отверстие диафрагмы все равно открывается широко, так что объекты на переднем плане получаются светлыми и четкими даже на фоне яркого света.

Ручной и автоматический баланс белого (AWB) -(Auto White Balance). Видеокамера пытается определить условия внешнего освещения и выставить нужное значение баланса белого. Необходимо заметить, что AWB успешно работает только при наличии источников внешнего освещения одного типа, ATW - автоматическое слежение за балансом белого. Доступны две установки - ручной и фиксированный имеющий 4 предустановки) Баланс белого. ATW (Auto trace white) позволяет автоматически корректировать баланс белого при изменении освещения. Эта функция полезна при съемке в условиях быстро изменяющегося освещения.

Автоматическая регулировка усиления (AGC). При включенном режиме AGC, камера автоматически усиливает видеосигнал при уменьшении освещенности. Максимальное усиление возможно до 28 дБ. Технология AGC - свойство камеры автоматически изменять коэффициент усиления каждого видеотракта в зависимости от уровня сигнала: автоматическая регулировка усиления сглаживает изменения уровня видеосигнала и позволяет получить качественную картинку на видеомониторе при малой освещенности объекта. Как правило, диапазон регулировки усиления ограничивается диапазоном 12-20 дБ (т.е. 4-10 раз), так как большее увеличение усиления видеосигнала приводит к высокому зашумлению и ухудшению изображения.

*Встроенное функциональное меню (OSD) – (On-screen display / Экранные настройки параметров).*Экранное меню-отображение на экране номера программы, установок звука, параметров изображения, таймера и другой информации в виде удобно организованного интерактивного меню. Пользователь может выбирать те или иные функции посредством перемещения курсора в пределах видимой области экрана.

6.9. Основные протоколы сетевого видеонаблюдения

RTSP (Real Time Streaming Protocol, или, по-русски, потоковый протокол реального времени) – это прикладной протокол, в котором описаны команды для управления видеопотоком. С помощью этих команд мы можем «приказать» камере или серверу, например, начать трансляцию видеопотока. Пример запроса на начало воспроизведения выглядит так:

```
PLAY rtsp://192.168.0.200/h264 RTSP/1.0
```

То есть RTSP – это просто набор команд для управления видеопотоком. Проведем эксперимент. Для этого нам понадобится IP-камера с поддержкой RTSP протокола и ее RTSP адрес. Этот адрес выглядит примерно так rtsp:///mpeg. Его можно узнать из руководства по эксплуатации камеры либо из описания API. Для удобства мы приведем RTSP адреса для ряда популярных камер в таблице.

Производитель	IP адреса по умолчанию	Логин	Пароль
Beward	192.168. 0. 99	admin	admin
Dahua	192.168. 1.108	admin	admin
Micro Digital	10. 20.30. 40	root	root
Aircam	192.168. 1. 20	ubnt	ubnt
IPEYE	192.168. 0.123	admin	123456
Hikvision	192. 0. 0. 64	admin	12345

Примеры URL адресов разных типов соединений:

- для IP камер Micro Digital

Модель	Тип соедин.	Пример URL
Unknown	VLC	rtsp://IPADDRESS/cam0_0
Other	JPEG	http://IPADDRESS/image.jpg
Other	VLC	rtsp://IPADDRESS:554/cam0_0

- для IP камер Beward

Модель	Тип соедин.	Пример URL
B1710RV	FFMPEG	rtsp://IPADDRESS:554//av0_0
BD	MJPEG	http://IPADDRESS:8008/
BD Series	JPEG	http://IPADDRESS/cgi-bin/jpg/image.cgi
BD Series	MJPEG	http://IPADDRESS:8008/
BD Series	VLC	rtsp://IPADDRESS:554/live/h264

Более подробную информацию практически по всем камерам большинства производителей можно найти в Интернете на сайте Connecting to IP Cameras. Тип соединения определяется способом и используемым стандартом подключения:

- VLC (VideoLAN Client) — свободный кроссплатформенный медиаплеер. Можно использовать в качестве сервера для трансляции потока аудио/видео по сети. Для воспроизведения мультимедиа не требуется установка дополнительных кодеков. VLC может воспроизводить DVD и потоковое незашифрованное видео.
- MJPEG (Motion JPEG) — покадровый метод видеосжатия, основной особенностью которого является сжатие каждого отдельного кадра видеопотока с помощью алгоритма сжатия изображений JPEG.
- FFmpeg — набор свободных библиотек с открытым исходным кодом, которые позволяют записывать, конвертировать и передавать цифровые аудио- и видеозаписи в различных форматах. Название идет от названия экспертной группы MPEG и FF, означающего fast forward.

После того, как мы узнали RTSP-адрес камеры, открываем стандартный проигрыватель, поддерживающий RTSP. Это может быть одна из следующих программ: Windows Media Player, QuickTime, Media Player Classic, VLC media player, RealPlayer, MPlayer. Если вы выбрали QuickTime, то надо выбрать «Файл -> Открыть URL» и ввести нужный RTSP адрес. После чего QuickTime подключится к камере и воспроизведет «живое видео».

Устройства записи, работающие в системах IP-видеонаблюдения, получают видео от камер либо с помощью протокола HTTP – то есть также, как мы

скачиваем JPEG-картинки с сайтов, либо в виде потока через RTSP – то есть также, как мы получили его с помощью стандартного проигрывателя в последнем примере.

В настройках IP-камер потоковый вариант передачи данных может обозначаться как RTSP over TCP, RTSP over UDP либо просто RTP. Итак, RTSP – это набор команд для управления потоком. Но что означают остальные аббревиатуры: TCP, UDP, и RTP - это транспортные механизмы (протоколы), которые собственно и передают видео.

Протокол TCP. Допустим, мы выбрали метод RSTP over TCP и хотим начать передачу видеопотока. Что будет происходить на уровне транспортных механизмов? Предварительно с помощью нескольких команд будет установлено соединение между отправителем и получателем. После этого начнется передача видеоданных.

При этом механизмы TCP будут следить за тем, чтобы все данные дошли до адресата без изменений и в нужной последовательности. Также TCP будет регулировать скорость передачи, чтобы передатчик не посылал данные интенсивнее, чем их может обработать приемник, к примеру, купольная цветная видеокамера высокого разрешения.

Протокол UDP. UDP – это альтернатива транспортному протоколу TCP. В отличие от TCP, UDP не устанавливает предварительного соединения, а вместо этого просто начинает передавать данные. UDP не следит за тем, чтобы данные были получены и не дублирует их, если отдельные части пропали или пришли с ошибками. UDP менее надежен, чем TCP. Но с другой стороны, он обеспечивает более быструю передачу потоков благодаря отсутствию механизма повторения передачи потерянных пакетов.

Вы также можете увидеть различие в протоколах, поставив следующий эксперимент: попробуйте перевести камеру в режим RTSP over TCP и помашите рукой перед объективом - на экране монитора вы увидите задержку. А теперь проведите этот же тест в режиме RTSP over UDP. Задержка будет меньше. На время задержки влияют несколько факторов:

- формат сжатия,
- мощность компьютера,
- протокол передачи
- и особенности ПО, участвующего в декодировании видео.

Протокол RTP. Real-time Transport Protocol, или по-русски транспортный протокол реального времени. Этот протокол специально создан для передачи реалтайм трафика. Он позволяет следить за синхронизацией передаваемых данных, корректировать последовательность доставки пакетов и потому более других подходит для передачи видео- и аудиоданных.

В общем случае для передачи видеопотока предпочтительнее использовать либо RTP либо UDP. Работа через TCP оправдана лишь в том случая, когда вам приходится работать с проблемными сетями, так как протокол TCP сможет корректировать ошибки и сбои, возникающие при передаче данных.

7. ВВЕДЕНИЕ В МУЛЬТИМЕДИЙНЫЕ СЕТИ И ТЕХНОЛОГИИ VOIP И SIP

В настоящее время недостаточно передавать мультимедиа от устройства пользователю, их необходимо передавать на значительные расстояния. Примерами этого являются 1P-телефония, видеоконференции, вебинары, потоковое вещание, передача изображений.

В большинстве случаев создавать специальное решение для передачи мультимедиа слишком дорого, поэтому чаще всего используются имеющиеся каналы связи: телефонные сети, локальные сети, Интернет.

В этом разделе будут идентифицированы и проанализированы требования, которые предъявляет передача мультимедиа к коммуникационной среде. Эти требования условно могут быть разделено на две категории:

- *Требования к трафику*. Они включают в себя ограничения по параметрам реального времени – задержке и джиттеру, ширине полосы пропускания и надежности.
- *Функциональные требования*. Они должны обеспечивать поддержку мультимедийных сервисов, таких как мультикастинг, безопасность, мобильность, управление сессиями.

Такие компоненты мультимедиа, как аудио и видео имеют четкие требования к параметрам реального времени, и коммуникационная среда должна эти требования удовлетворять. Например, аудио- и видеоданные должны проигрываться непрерывно и на той скорости, с которой они записывались.

Если данные не обработать вовремя, то процесс воспроизведения остановится и тогда глаза и уши человека заметят это. В Интернет телефонии человеческие возможности допускают задержку примерно в 200 мс. Если задержка превысит этот порог, то передаваемый голос будет звучать как звонок через спутниковую линию, то есть приводит к снижению качества переговоров.

Таким образом, трафик реального времени обеспечивает строгие ограничения к времени задержки пакета — времени, которое затратил пакет на прохождение пути от источника до приемника, и джиттеру — изменению времени задержки между пакетами на приемнике. Чем меньше эти два параметра, тем выше производительность системы передачи мультимедиа.

Мультимедийные приложения требуют значительно большей полосы пропускания, чем традиционные текстовые приложения. Более того, медиапотоки передаются с использованием RTP (Real-time Transport Protocol) протокола, который не обеспечивает механизма контроля целостности.

Коммуникационная сеть должна обладать возможностью обеспечивать такие высокие требования к полосе пропускания без ущерба для традиционно

существующих потоков данных. Требования к полосе пропускания для некоторых распространенных типов мультимедиа приведены в табл. 7.1 и 7.2.

Таблица 7.1

Пропускная способность канала при передаче звука

Источник звука	Скорость преобразования	Бит в семпле[5]	Битрейт
Телефония (до 3,4 КГц)	8000 семплов/с	12	96 Кбит/с
Широкополосная голосовая связь (до 7 КГц)	16 000 семплов/с	14	224 Кбит/с
Широкополосный двухканальный звук (до 20 КГц)	44 100 семплов/с	16 на канал	1,412 Мбит/с для двух каналов

Таблица 7.2

Пропускная способность канала при передаче изображения

Источник изображения	Количество пикселей	Бит/пиксель	Битрейт
Цветное изображение	512x512	24	6,3 Мбит/с
Обычное телевидение (CCIR)	720x576x30	24	300 Мбит/с
Телевидение высокой четкости (HDTV)	1280x720x60	24	1,327 Гбит/с

Для снижения требуемой полосы пропускания применяются различные алгоритмы сжатия, так называемые кодеки, но их применение не всегда возможно (рентгеновские снимки, телемедицина).

Различные типы данных мультимедиа имеют широкий диапазон требований к наличию ошибок, начиная от полностью не допускающих ошибок. Ошибка

[5] Сэмпл (англ. sample - образец) в цифровом звуке — минимальная часть аудио сигнала, содержащая амплитудное значение звуковой волны. Число сэмплов в секунду называется частотой дискретизации (сэмплирования). Разрядностью сэмпла определяется разрядность цифрового сигнала. Например, если сэмпл содержит 16 бит, то разрядность цифрового сигнала (звука) будет 16 бит. Чем больше частота дискретизации, тем больше сэмплов в единице времени, а следовательно цифровое представление звука более точное

получается, когда пакет данных теряется или повреждается. Большинство допускающих ошибки мультимедийных приложений имеют свои технологии контроля ошибок и средства восстановления данных, использующие правильно полученные пакеты.

Большинство популярных мультимедийных приложений требуют мультикастинга, то есть возможности одновременного получения данных на многих приемниках с одного источника. К примеру, многопользовательские аудио- и видео конференции наиболее широко используемые сервисы в Интернет телефонии. Мультикастинг довольно легко реализуется для однонаправленных видов коммуникации (Интернет-радио). Для двунаправленных его организовать гораздо сложнее. Но в любом случае использование мультикастинга значительно снижает требования к полосе пропускания в отличие от видов связи, когда между каждым из членов конференции устанавливается отдельный канал.

Функционал управления сессиями включает:

- Описание среды

  Позволяет распределенным приложениям распространять информацию о сессии как тип данных (аудио, видео, двоичные данные), время начала сессии, время конца сессии, IP-адреса вовлеченных устройств и т.д. Часто бывает необходимо описать параметры сессии до ее установки, так как большинство участников, вовлеченных в сессию, будут иметь различные мультимедийные возможности;

- Анонсирование сессии

  Позволяет участникам анонсировать будущие сессии. К примеру, есть сотни радиостанций в Интернете, которые в ходе анносирования распространяют информацию о планируемых трансляциях, что облегчает пользователю настройку на предпочитаемое радио-шоу;

- Идентификация сессии.

  Мультимедийная сессия часто состоит из множества потоков данных (включая непрерывные – звук, видео и дискретные –текст, изображения), которые надо идентифицировать раздельно. Например, отправитель может выбрать отправку звука и видео как двух отдельных потоков через одно сетевое соединение, которые получатель должен декодировать синхронно.

  Другой пример: отправитель может поместить аудио- и видеопотоки вместе, но разделить качество на базовый и несколько улучшенных уровней таким образом, что получатели с низкой пропускной способностью канала смогут получить только базовый уровень, в то время как получатели с широким каналом смогут получить и улучшенные уровни;

- Контроль сессии.

  Мультимедиа сессия включает множество медиапотоков. Информация, содержащаяся в этих потоках данных часто взаимосвязана,

и коммуникационная мультимедийная сеть должна синхронизировать информационные потоки при передаче и предоставлении пользователю.

Синхронизация может быть реализована при помощи помещения штампов времени в каждый пакет данных. Более того, многие пользователи хотят контролировать процесс воспроизведения, использовать функции, аналогичные функциям DVD-плеера (пауза, перемотка и т. д.).

С точки зрения безопасности, коммутационная мультимедиа среда должна обеспечивать три основных аспекта: целостность, достоверность и конфиденциальность. Также не стоит забывать об авторских правах. Если контент оплачен для одного пользователя, не стоит допускать возможности его нелегальной продажи (цифровые водяные знаки).

7.1. Технология Voice over IP (VoIP)

Эта технология, называемая также IP-телефонией, предусматривает взаимодействие сети TDM[6] с коммутацией каналов и сети IP с коммутацией пакетов, а также обеспечивает эволюционное движение телекоммуникационных сетей TDM к сетям IP. Появившись немногим более 10 лет назад, она считается самой перспективной телекоммуникационной технологией, а группу протоколов VoIP можно назвать ключевой среди других телекоммуникационных протоколов.

Согласно принятому определению, IP-телефония — это передача речевого сигнала по сети с пакетной коммутацией в режиме реального времени. При этом телефонный номер преобразуется в IP-адрес, а аналоговый речевой сигнал — в цифровую форму.

Годом рождения Интернет-телефонии считают 1995, когда компания Vocaltec опубликовала программное обеспечение Internet Phone для системы телефонной передачи с использованием протокола IP. Для сетевой реализации Internet Phone до середины 1990-х гг. были доступны только телефонные модемы, поэтому передача речи посредством Internet Phone значительно уступала по качеству традиционной телефонной связи. Однако первый камень в основание здания VoIP был, тем не менее, заложен.

Между тем события стали развиваться столь стремительно, что сейчас реальные возможности технологии VoIP значительно шире ее формального названия. По существу эта технология представляет собой средство для передачи не только речи, но и произвольной информации с использованием протокола IP, а обобщающим термином стало определение «мультимедийная». Соответствующая структура данных может включать речь, изображение и данные в любых комбинациях. Эту триаду обычно называют Triple Play.

Архитектура сети VoIP может быть представлена в виде двух плоскостей. Нижняя – отображает транспортный механизм негарантированной доставки мультимедийного трафика в виде иерархии протоколов RTP/UDP/IP, а верхняя — механизм управления обслуживанием вызовов. Ее ключевыми протоколами

[6] Мультиплексирование с разделением по времени (Time Division Multiplexing, TDM)

являются H.323 ITU-T, SIP, MGCP и MEGACO, представляющие собой различные реализации обслуживания вызовов в сетях 1P-телефонии.

Транспортный протокол реального времени (Real-time Transport Protocol, RTP) предоставляет транспортные услуги мультимедийным приложениям. Он не гарантирует доставку и правильный порядок пакетов, но позволяет приложениям обнаружить потерю или нарушение порядка следования пакетов за счет присвоения каждому из них номера. Протокол предназначен для работы в режимах передачи «точка—точка» или «точка—множество точек» и не зависит от транспортного механизма. Однако в качестве такового обычно используется протокол U DP.

RTP работает совместно с протоколом управления реального времени (Real Time Control Protocol, RTCP), обеспечивающим управление потоком данных и контроль перегрузки канала. Участники сеанса RTP периодически обмениваются пакетами RTCP со статистическими данными (количество отправленных пакетов, число потерянных и т. д.), которые могут быть использованы отправителем мультимедиа, например, для динамической коррекции скорости передачи и даже изменения типа нагрузки.

Среди мультимедийных стандартов наиболее освоен стандарт H.323 ITU-T, к тому же он постоянно совершенствуется и имеет пять версий. Рекомендация H.323, исторически первый способ осуществления вызовов в сети IP, предусматривает следующие виды информационного обмена:

- оцифрованное аудио;
- оцифрованное видео;
- данные (обмен файлами или изображениями);
- управление соединением (обмен информацией о поддерживаемых функциях, управление логическими каналами и т.д.);
- управление установлением и разъединением соединений и сеансов связи.

Основными элементами сети стандарта H.323 являются терминалы (terminal), шлюзы (gateway), привратники (gatekeeper) и устройства управления конференциями (Multipoint Control Units, MCU).

- Терминал обеспечивает двухстороннюю связь в реальном времени с другим терминалом H.323, шлюзом или MCU.
- Шлюзы устанавливают соединение между терминалами сети H.323 и терминалами, находящимися в сетях, где используются другие протоколы. Главная задача шлюзов заключается во взаимном преобразовании информации между сетями разных протоколов (например, IP и протоколом телефонной сети общего пользования, ТфОП).
- Привратники участвуют в управлении соединением, отвечая за взаимное преобразование телефонных номеров и IP-адресов.

Еще один элемент сети H.323, называемый ргоху-сервером (т.е. посредником), работает на прикладном уровне, он определяет тип приложения и выполняет нужное соединение.

Плоскость обслуживания вызовов стандарта H.323 включает три основных протокола (рис. 7.1): протокол взаимодействия оконечного оборудования с привратником RAS (Registration, Admission and Status), протокол управления соединениями H.225 и протокол управления логическими каналами H.245. Для передачи сигнальных сообщений RAS используется протокол UDP, а для передачи сигнальных сообщений H.225 и H.245 — протокол TCP с гарантированной доставкой информации. UDP не обеспечивает гарантированной доставки информации, поэтому, если подтверждение не было получено в установленное время, сообщение передается повторно.

Процесс установления соединения состоит из трех этапов. На первом решаются задачи обнаружения привратника, регистрации привратником терминалов, контроля доступа терминалов к сетевым ресурсам, для чего привлекается протокол RAS. На двух следующих этапах выполняются процессы сигнализации H.225 и обмен управляющими сообщениями H.245.

Рекомендация H.225 регламентирует процедуры управления соединением в сетях H.323 с использованием ряда сигнальных сообщений из рекомендации Q.931 ITU-T.

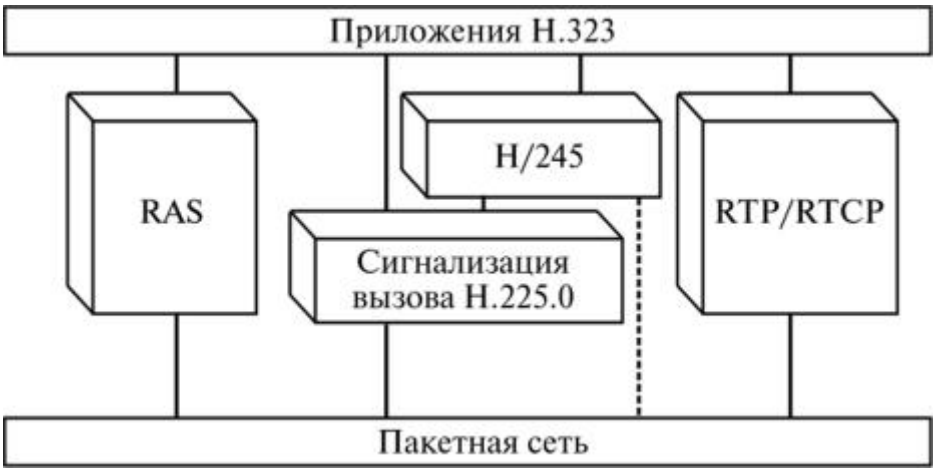

Рис. 7.1. Протоколы обслуживания

Рекомендация H.245 описывает процедуры управления информационными каналами: определение ведущего и ведомого устройств, а также обмен данными о функциональных возможностях терминалов и открытии и закрытии однонаправленных и двунаправленных каналов, вносимой задержке, режиме обработки информации, состоянии информационных каналов путем организации шлейфов.

Этот обмен сигнальными сообщениями между взаимодействующими устройствами сети H.323 осуществляется по логическим каналам H.245, причем нулевой логический канал, по которому передаются управляющие сообщения, должен быть открыт в течение всего времени существования соединения.

Известный способ обслуживания вызовов в сети VoIP предполагает использование протокола инициирования сеансов (Session Initiation Protocol, SIP),

его спецификации представлены в документе RFC 2543 комитета 1ETF. Как протокол прикладного уровня он предназначен для организации мультимедийных конференций, распределения мультимедийной информации и телефонных соединений. SIP менее приспособлен для взаимодействия с ТфОП, но проще в реализации. Он лучше подходит провайдерам Интернета для организации услуги IP-телефонии в рамках предлагаемого ими пакета услуг.

Ключевыми особенностями протокола SIP являются поддержка персональной мобильности пользователя, обеспечение масштабируемости сети, возможность дополнения новыми функциями, интеграция в стек существующих протоколов Internet, взаимодействие с другими протоколами сигнализации (например, H.323), организация доступа пользователей сетей VoIP к услугам интеллектуальных сетей, независимость от транспортных технологий.

Следует отметить, что поддержка мобильности пользователя уже не является прерогативой исключительно SIP. Теперь это характерно и для H.323 (стандарт H.510 ITU-T «Mobility for H.323 Multimedia Systems and Services»).

Сеть SIP содержит агенты пользователя (User Agents или SIP Clients), proxy-серверы и серверы переадресации.

Агенты пользователя — это приложения терминального оборудования, они включают собственно клиент (User Agent Client, UAC) и сервер (User Agent Server, UAS). UAC инициирует запрос услуги, а UAS выступает в качестве вызывающей стороны.

Proxy-сервер (Proxy Server) объединяет в себе функции UAC и UAS. Он интерпретирует и, если надо, перезаписывает заголовки запросов перед отправкой их другим серверам.

Сервер переадресации (Redirect Server) определяет положение вызываемого абонента и сообщает его вызывающему пользователю.

Еще один способ построения сети IP-телефонии опирается на протокол Media Gateway Control Protocol (MGCP), предложенный рабочей группой MEGACO комитета IETF. Архитектура этого протокола, пожалуй, наиболее проста с точки зрения функциональности. Сеть MGCP содержит шлюз (Media Gateway, MG), выполняющий преобразование речевой информации между сетями ТфОП и IP-телефонии, шлюз сигнализации (Signaling Gateway, SG), обеспечивающий обработку сигнальной информации, а также схожий с привратником сети H.323 контроллер шлюзов (Call Agent), осуществляющий функции управления шлюзами.

Протокол MGCP, подобно H.323, удобен для организации совместимых с ТфОП сетей IP-телефонии. Вместе с тем по своим функциональным возможностям MGCP превосходит H.323. Так, Call Agent сети MGCP поддерживает сигнализацию ОКС-7 и прозрачную передачу сигнальной информации по сети 1P-телефонии. В сети же H.323 любая сигнальная информация должна преобразовываться шлюзом в сигнальные сообщения H.225 (Q.931). Сообщения протокола MGCP передаются в текстовом формате.

Третий способ построения сети IP, представляющий собой усовершенствование MGCP, разработан группой MEGACO комитета IETF вместе

с 16 SG ITU-T, поэтому его называют протоколом MEGACO/H.248. От своего старшего брата он отличается прежде всего иной схемой организации связи. Благодаря ей контроллер MEGACO/H.248 способен изменять топологию связи портов, что позволяет гибко управлять конференциями. Протокол MEGACO поддерживает два способа бинарного кодирования.

Шлюз H.323 поддерживает процедуру альтернативных привратников, которые могут задействоваться в случае неисправности или перегрузки первичных. Непременным условием их использования является получение IP-адреса альтернативного привратника от первичного в рамках процедуры регистрации конечной точки.

Одной из основных новаций последней версии стандарта H.323 стала концепция «назначенного» привратника (Assigned Gatekeeper), представляющая собой расширение концепции альтернативного привратника.

С помощью «назначенного» привратника конечный пункт может регистрироваться без обращения к списку альтернативных привратников, а при его отказе переключается на альтернативный контроллер согласно процедурам выбора последнего. Конечный пункт или «текущий» привратник продолжают контролировать состояние «назначенного», причем после восстановления его работоспособности происходит обратное переключение системы. Это позволяет оператору поддерживать сеть в состоянии предупредительного обслуживания. При значительном разбросе физического местонахождения альтернативных привратников желательно регистрировать конечные пункты на ближайшем из них. В любом случае концепция «назначенного» привратника дает оператору большую свободу в использовании сетевых ресурсов.

7.2. VoIP и Session Initiation Protocol (SIP).

Другое существенное улучшение стандарта H.323 касается процедур безопасности. В прежних версиях стандарта H.323 поддержку безопасности обеспечивал протокол безопасности и шифрования для мультимедийных терминалов H.235 — Security and Encryption for H.323 (and Other H.245-Based) multimedia terminais. Он действителен для любых терминалов, применяемых при организации «двухточечных» и «многоточечных» конференций, которые используют протокол управления H.245. Обеспечивая аутентификацию, секретность и целостность систем H.323, протокол H.235 является, скорее, средством идентификации не терминала, а пользователя.

Профили безопасности H.235 предполагают использование либо пароля пользователя, либо цифровых сертификатов и шифрования открытым ключом, либо комбинации того и другого. Применять указанные профили не обязательно.

Стандарт H.235 позволяет гибко согласовывать услуги и функции, касающиеся выбора криптографических алгоритмов (как стандартных, так и фирменных) и работы с ними. При этом количество алгоритмов, поддерживаемых каждым устройством стандартов H3xx, должно быть достаточным для обеспечения совместимости этих устройств.

В шестой версии стандарта H.323 безопасность значительно усилена за счет полной реконструкции H.235, на смену которому пришло целое семейство рекомендаций H.235.0-H.235.9. Разработчики могут теперь предложить стандартизованную версию RTP — стандарт SRTP, обеспечивающий безопасность медиа-потоков IP.

Кроме того, в новой, шестой, версии стандарта H.323 содержатся следующие изменения: новые документы и приложения для H.245, разрешающие использование различных кодов, в том числе GSM, iLBC и H.264; более подробная детализация отдельных процедур, среди которых процедуры прозрачности вызова, обработки ошибок и т. д.; уточнения в H.225, проясняющие использование отдельных полей, поддержку качества услуг QoS (H.361) и широковещательных сообщений (H.460.21); улучшения, связанные с транспортом комбинации текста и данных в реальном времени для поддержки рекомендации V. 151. Большая часть новых функций была введена в стандарт H.323 в последние два года. Наиболее важными из вновь одобренных документов версии 6 стандарта H.323 являются следующие:

- H.235.0—H.235.9 — определение безопасности систем H.323, включая поддержку протокола SRTP;
- H.239 — управление индикацией типа информационного потока Role Management;
- H.241 — расширенные видеопроцедуры Extended Video Procedures;
- H.249 — расширение индикации ввода пользователя Extended User Input Indications (например, щелчка мыши или движения курсора);
- H.361 — поддержка качества услуг между терминалами End- to-End Quality of Service (вместо Приложения N H.323) и сигнализации приоритета услуги Service Priority Signaling;
- H.460.10 — категория коллективного вызова Call Party Category (транспорт поля IS UP через систему H.323);
- H.460.11 — установление задержанного вызова Delayed Call Establishment (тем самым гарантируется, что медиапоток появится ранее, чем сигнал о входящем вызове);
- H.460.12 — индикатор управления бликами Glare Control Indicator;
- H.460.13 — управление освобождением вызванного пользователя Called User Release Control (при критически важных вызовах; например, при обращении в службы скорой помощи, важно знать, как и когда произошло разъединение);
- H.460.14 — многоуровневый приоритет и прерывание Multi- Level Precedence and Pre-Emption (добавление поддержки MLPP стандартом H.323);
- H.460.15 — сигнализация паузы транспортного канала и перенаправления вызова Call Signalling Transport Channel Suspension and Redirection;

- H.460.16 — гарантия надежного разъединения путем введения механизма квитирования Multiple-Message Release Sequence Capability;
- H.460.17 — туннелирование RAS через H.225.0 Tunneling RAS Through H.225.0;
- H.460.18 — пропуск сигнализации H.323 трансляторами адресов NAT и межсетевых экранов Traversal of H.323 Signaling across Network Address Translators and Firewalls;
- H.460.19 — пропуск мультимедийных потоков H.323 преобразователями адресов NAT и межсетевыми экранами Traversal of H.323 Media Across Network Address Translators and Firewalls;
- H.460.20 — номера дислокации для H.323 Location Number for H.323;
- H.460.21 — широковещательное сообщение для систем H.323 Message Broadcast for H.323 Systems.

Несколько более подробно рассмотрим еще два стандарта семейства H.323 — протоколы видеокодирования и семейство протоколов конференций T. 120.

Стандартизация в области видеокодирования прошла долгий путь — от первых H.261 и MPEG-1 до современных H.264/MPEG-4 AVC, причем последние продолжают совершенствоваться. Новейшим стандартом видеокодирования является H.264/AVC, где аббревиатура AVC обозначает Advanced Video Coding, т. е. усовершенствованное видеокодирование. Его основными особенностями стала повышенная эффективность сжатия и транспорта интерактивных и вещательных видеоприложений.

Стандарт T.120 представляет собой совокупность телекоммуникационных и прикладных протоколов для организации и проведения многоточечной конференции в реальном времени. В зависимости от конкретной реализации продукты T.120 могут устанавливать соединения, выполнять передачу и прием данных и работать совместно, используя программное разделение, передачу файлов и т. п.

Главные особенности стандарта T.120 заключаются в организации и поддержании конференций на любой платформе, управлении множеством участников и программ, безошибочном и безопасном обмене данными при всем многообразии возможных сетевых сценариев.

Семейство T. 120 включает следующие протоколы:

- T.121 — представляет основу для разработки прикладных протоколов;
- T.122 — совместно с T.125 определяет доступные многоточечные услуги;
- T.123 — специфицирует транспортные профили ТфОП, ISDN, цифровых сетей с коммутацией каналов CSDN, цифровых сетей с коммутацией пакетов PSDN, сети Novell NetWare IPX и сети TCP/IP;
- T.124 — регламентирует общий процесс управления конференцией Generic Conference Control (GCC), обеспечивая полный набор инструмента для ее организации и управления;

- T.125 — описывает многоточечный протокол связи (Multipoint Communication Service Protocol, MCS), задающий процедуры для передачи сигнальной информации и данных между провайдерами MCS;
- T.126 — определяет процедуры просмотра и аннотирования неподвижных изображений между двумя или несколькими приложениями;
- T.127 — предусматривает средства файлового обмена между участниками конференции, в том числе их одновременную приоритетную передачу, а также опции для сжатия файлов перед их транспортированием.4

Архитектура T.120 — это двухуровневая архитектура с предопределенными протоколами взаимодействия уровней. Протоколы нижнего уровня T.122, T.123, T.124 и T.125 описывают независимый от приложений механизм для организации многоточечной связи, а протоколы верхнего уровня T.126 и T.127 являются прикладными протоколами, причем в рамках одной конференции могут сосуществовать как стандартизованные, так и нестандарти- зованные приложения.

По степени распространенности следующим после H.323 является протокол инициирования сеансов (Session Initiation Protocol, SIP).

Протокол SIP решает, по существу, те же задачи, что и H.323 (рис. 7.2).

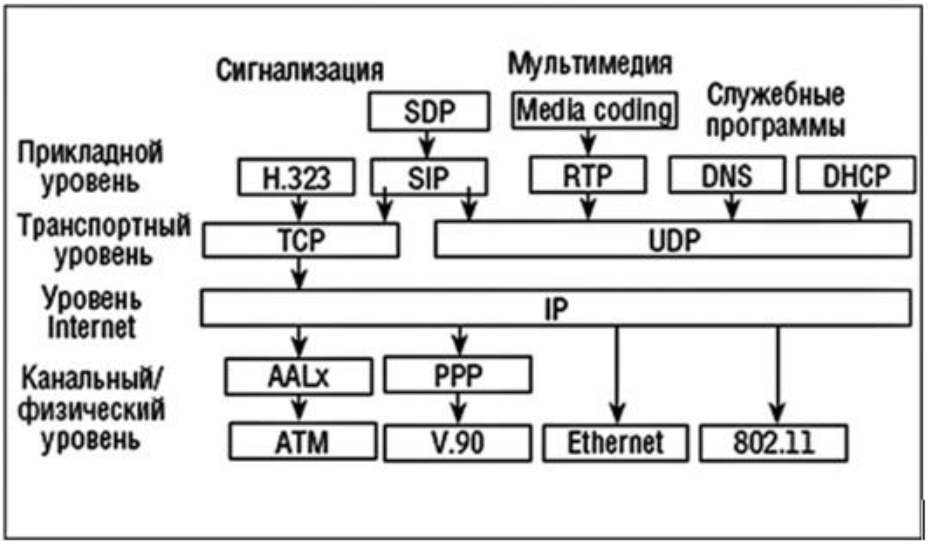

Рис. 7.2. Положение SIP в стеке протоколов TCP/IP

Оба протокола могут рассматриваться в качестве примера разного подхода к решению одной и той же задачи. Если H.323 опирается на традиционные системы телефонной сигнализации на основе протокола Q.931, то SIP реализует более современный, ориентированный на интернет-подход на базе протокола HTTP.

Протокол SIP способен устанавливать, модифицировать и завершать сеансы мультимедиа, подобные VoIP. Он разработан рабочей группой по управлению многоточечными сеансами мультимедиасвязи (MMUSIC) организации IETF, а его последняя версия изложена в документе RFC 3261 IETF.

SIP поддерживает несколько основных функций установления и завершения мультимедийных сеансов, включая определение местонахождения вызванного пользователя, его готовности участвовать в сеансе, его возможностей (параметры используемой среды, оборудования и др.), посылку вызова, задание параметров сеанса на вызывающей и вызываемой сторонах, управление сеансом (включая процессы передачи и завершения сеанса, модификации параметров сеанса и предложение услуг).

SIP поддерживает приглашение участников к текущим сеансам наподобие многоточечных конференций, добавление к текущему сеансу или удаление из него мультимедийных данных, прозрачное распределение имен и перенаправление услуг, включая персональную мобильность пользователя.

SIP совместим с обоими протоколами адресации IPv4 и IPv6.

Для построения законченной мультимедийной архитектуры SIP используется вместе с другими протоколами IETF — уже обсуждавшимися ранее транспортным протоколом реального времени RTP и протоколом управления потоком данных RTCP.

Протокол описания сеанса (Session Description Protocol, SDP) входит в семейство протоколов SIP в виде документа RFC 2327 IETF и содержит механизм описания характеристик сеанса: время проведения, требуемые ресурсы и т. д. В SDP предусмотрена возможность изменения параметров сеансов в оперативном режиме.

Протокол инициирования сеансов для телефонов (Session Initiation Protocol for Telephones, SIP-T), приведенный в документе RFC 3372, содержит алгоритм взаимодействия SIP с ТфОП. Он предусматривает как прямое взаимное преобразование сообщений SIP и ТфОП, так и их инкапсуляцию.

При взаимном преобразовании вызов SIP, исходящий от шлюза ТфОП, нельзя отличить от вызова, который посылает устройство SIP, поэтому оба вызова будут обрабатываться одинаково. Однако не каждый параметр сигнального сообщения ТфОП имеет соответствие в SIP, а значит, если вызов адресован абоненту ТфОП, часть сигнального сообщения будет потеряна.

К недостаткам инкапсуляции относятся возможность использования этого подхода в сети только с одним протоколом телефонной сигнализации, необходимость шифрования сообщений ТфОП при передаче через общедоступную сеть Интернет или использование в сети только с SIP-совместимыми устройствами.

Стек протоколов транспорта сигнализации (Signaling Transport Protocol Stack, SIGTRAN, а также Signaling Transport) обеспечивает транспорт протоколов сигнализации «Общеканальная сигнализация № 7», ОКС-7, через сеть IP и может рассматриваться как эволюция этих протоколов, где учтены их особенности и особенности пакетных протоколов. Приложения SIGTRAN включают удаленный коммутируемый доступ, взаимодействие 1P-телефонии с ТфОП и др.

Основу архитектуры SIGTRAN составляют следующие элементы:

- транспортный шлюз (Media Gateway, MG), упаковывающий речевой трафик в пакеты и доставляющий его по назначению;

- шлюз сигнализации (Signaling Gateway, SG), обеспечивающий интерфейс для сети ОКС-7 и передачу сигнальных сообщений к узлам IP;
- контроллер Media Gateway Controller (MGC), отвечающий за управление вызовами (между шлюзом сигнализации и транспортным шлюзом) и доступом между сетями ТфОП и IP;
- точка управления сервисом (IP-enabled Service Control Point, SCP), целиком находящаяся в сети IP, но адресуемая из сети ОКС-7;
- IP-телефон.

Протокол передачи с управлением потоком (Stream Control Transmission Protocol, SCTP) — ключевой протокол семейства протоколов SIGTRAN, который представляет собой улучшенную версию протокола TCP: подобно TCP, он обеспечивает надежный транспорт пакетов, но превосходит TCP с точки зрения транспорта сообщений.

Так, в SCTP предусмотрена встроенная сегментация сообщений, что позволяет выделять их на транспортном уровне. Кроме того, он устраняет проблему протокола TCP, называемую «Head of Line Blocking». Ее суть состоит в том, что при большом окне потеря сегмента ведет к задержке в буфере всего содержимого окна до тех пор, пока он не будет передан повторно. SCTP поддерживает также множественную адресацию коммутируемых пакетов (multihoming), поэтому при нарушении нормальной работы одного из серверов балансировки нагрузки другой продолжает принимать сообщения даже без привлечения услуг сервера DNS.

Протокол маршрутизации телефонии по IP (Telephony Routing over IP, TRIP) поддерживает обмен таблицами маршрутизации телефонных вызовов при взаимодействии разных сетей 1P-телефо- нии или, как определяется в RFC 2871, различных административных доменов IP-телефонии (ITAD). Каждый из них содержит, по крайней мере, один сервер местоположения (Location Server, LS), играющий роль сервера сигнализации. Это может быть контроллер домена H.323, сервер SIP или устройство MGC. Протокол TRIP необходим при объединении таких LS. С его помощью передаются данные о вызываемом абоненте и применяемой им сигнализации внутри ITAD, т. е. на TRIP возлагаются примерно те же обязанности, которые выполняет BGP в случае объединения автономных систем в Интернете.

Приложение 1. Сеть хранения данных

Сеть хранения данных (англ. Storage Area Network, SAN) — представляет собой архитектурное решение для подключения внешних устройств хранения данных, таких как дисковые массивы, ленточные библиотеки, оптические приводы к серверам таким образом, чтобы операционная система распознала подключённые ресурсы как локальные.

SAN характеризуются предоставлением, так называемых, сетевых блочных устройств (обычно посредством протоколов Fibre Channel, iSCSI или AoE), в то время как сетевые хранилища данных (англ. Network Attached Storage, NAS) нацелены на предоставление доступа к хранящимся на их файловой системе данным при помощи сетевой файловой системы (такой как NFS, SMB/CIFS, или Apple Filing Protocol).

При этом категоричное разделение SAN и NAS является искусственным, так как с появлением iSCSI началось взаимное проникновение технологий с целью повышения гибкости и удобства их применения. Например, в 2003 году NetApp уже предоставляли iSCSI на своих NAS, а EMC и HDS — наоборот, предлагали NAS-шлюзы для своих SAN-массивов.

Большинство сетей хранения данных использует протокол SCSI для связи между серверами и устройствами хранения данных на уровне шинной топологии.

Рис..1 SAN-Свитч Qlogic SANbox 5600 с подключёнными к нему оптическими разъёмами Fibre Channel

Так как протокол SCSI не предназначен для формирования сетевых пакетов, в сетях хранения данных используются низкоуровневые протоколы, такие как:

- Fibre Channel Protocol (FCP), транспорт SCSI через Fibre Channel. Наиболее часто используемый на данный момент протокол. Существует в вариантах 1 Gbit/s, 2 Gbit/s, 4 Gbit/s, 8 Gbit/s, 10 Gbit/s, 16 Gbit/s, 20 Gbit/s.
- iSCSI, транспорт SCSI через TCP/IP.
- iSER[en], транспорт iSCSI через InfiniBand / RDMA.

- SRP[en], транспорт SCSI через InfiniBand / RDMA.
- FCoE, транспортировка FCP/SCSI поверх «чистого» Ethernet.
- FCIP и iFCP, инкапсуляция и передача FCP/SCSI в пакетах IP.
- HyperSCSI, транспорт SCSI через Ethernet.
- FICON, транспорт через Fibre Channel (используется только мейнфреймами).
- ATA over Ethernet, транспорт ATA через Ethernet.

Также используется протокол NVMe over Fabrics, обеспечивающий доступ по сетевому расширению протокола NVMe.

7.3. Совместное использование устройств хранения

Движущей силой для развития сетей хранения данных стал взрывной рост объёма деловой информации (такой как электронная почта, базы данных и высоконагруженные файловые серверы), требующей высокоскоростного доступа к дисковым устройствам на блочном уровне. Ранее на предприятии возникали «острова» высокопроизводительных дисковых массивов SCSI. Каждый такой массив был выделен для конкретного приложения и виден ему как некоторое количество томов (LUN).

Сеть хранения данных позволяет объединить эти «острова» средствами высокоскоростной сети. Также без использования технологий SCSI транспорта невозможно организовать отказоустойчивые кластеры, в которых один сервер подключается к двум и более дисковым массивам, находящимся на большом расстоянии друг от друга на случай стихийных бедствий.

Сети хранения помогают повысить эффективность использования ресурсов систем хранения, поскольку дают возможность выделить любой ресурс любому узлу сети.

Не стоит забывать и об устройствах резервного копирования, которые также подключаются к SAN. В данный момент существуют как промышленные ленточные библиотеки (на несколько тысяч лент) от ведущих брендов, так и решения для малого бизнеса. Сети хранения данных позволяют подключить к одному хосту несколько приводов таких библиотек, обеспечив, таким образом, хранилище данных для резервного копирования от сотен терабайт до нескольких петабайт.

7.4. Преимущества

Совместное использование систем хранения, как правило, упрощает администрирование и добавляет изрядную гибкость, поскольку кабели и дисковые массивы не нужно физически транспортировать и перекоммутировать от одного сервера к другому.

Другим преимуществом является возможность загружать сервера прямо из сети хранения. При такой конфигурации можно быстро и легко заменить сбойный сервер, переконфигурировав SAN таким образом, что сервер-замена будет загружаться с LUN'a сбойного сервера. Эта процедура может занять,

например, полчаса. Идея относительно новая, но уже используется в новейших датацентрах.

Дополнительным преимуществом является возможность на хосте собрать RAID-зеркало из LUNов, которые презентованы хосту с двух разных дисковых массивов. В таком случае полный отказ одного из массивов не навредит хосту.

Также сети хранения помогают более эффективно восстанавливать работоспособность после сбоя. В SAN может входить удаленный участок со вторичным устройством хранения. В таком случае можно использовать репликацию — реализованную на уровне контроллеров массивов, либо при помощи специальных аппаратных устройств.

Поскольку каналы WAN на основе протокола IP встречаются часто, были разработаны протоколы Fibre Channel over IP (FCIP) и iSCSI с целью расширить единую SAN средствами сетей на основе протокола IP.

7.5. Сравнение технологий обмена данными

Порой сравнивают SAN и NAS, говоря на самом деле о разнице между сетевым диском и сетевой файловой системой — которая состоит в том, кто обслуживает файловую систему, хранящую данные.

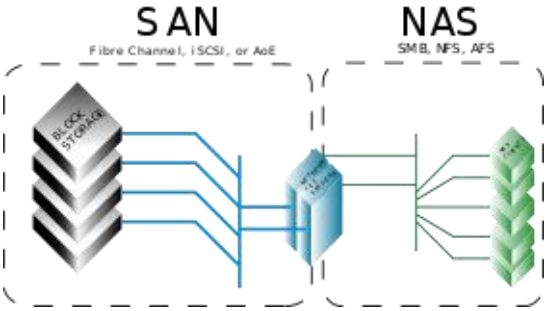

Рис. 2. Различия между NAS и SAN

В случае сетевого диска (также «блочного устройства», англ. block device):

- обмен данными с ним по сети осуществляется блоками подобно тому, как и с локальным SCSI- или SATA-диском;
- файловая система, если нужна, создаётся и управляется клиентом и, как правило, используется им одним.

В случае сетевой файловой системы («ресурс с совместным/разделяемым доступом» — не хранит, а только передаёт данные):

- обмен данными по сети происходит с применением более высокоуровневых понятий «файл» и «каталог», соответствующих объектам подлежащей «настоящей» ФС на физических дисках (либо логических поверх них в случае применения RAID, LVM);
- эта файловая система создаётся и обслуживается в рамках удалённой системы, при этом может одновременно использоваться на чтение и запись множеством клиентов.

7.6. Топологии сетей хранения данных

Для организации сетей хранения данных используются такие топологии, как:.

Однокоммутаторная структура (англ. single-switch fabric) состоит из одного коммутатора Fibre Channel, сервера и системы хранения данных. Обычно эта топология является базовой для всех стандартных решений — другие топологии создаются объединением однокоммутаторных ячеек.

Решётка (англ. meshed fabric) — набор ячеек, коммутатор каждой из которых соединен со всеми другими. При отказе одного (а в ряде сочетаний — и более) ISL-соединения связность сети не нарушается. Недостаток — большая избыточность соединений.

Центрально-распределённая топология (англ. core-edge fabric) практически повторяет схему топологии решётки. Среди преимуществ — меньшая избыточность соединений и высокая степень отказоустойчивости.

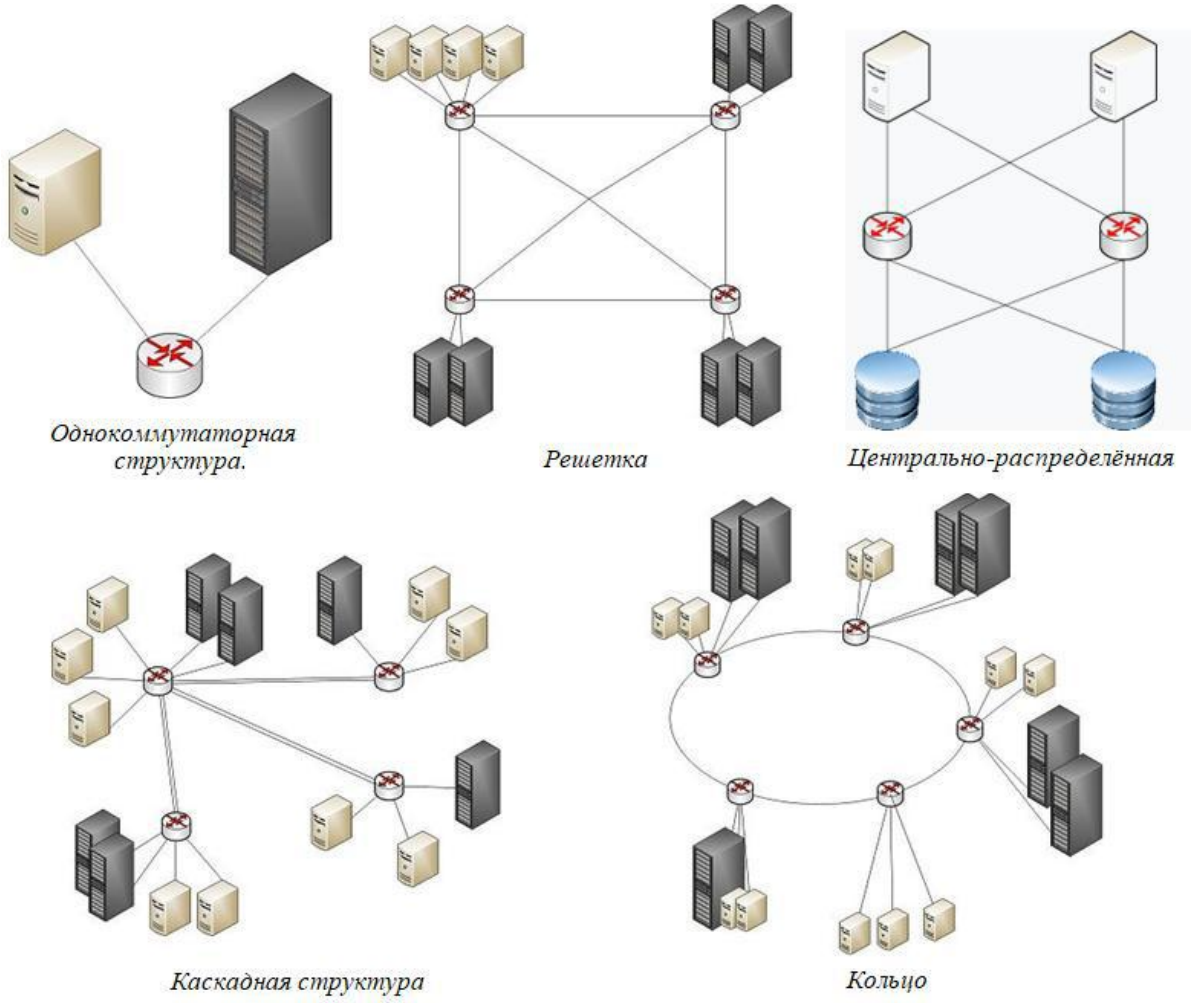

Рис. 3. Топологии сетей хранения данных

Каскадная структура (англ. cascaded fabric) — набор ячеек, коммутаторы которых соединены в дерево с помощью межкоммутаторных соединений (англ. Inter-Switch link, ISL). Во время инициализации сети коммутаторы выбирают «верхушку дерева» (англ. principal switch, главный коммутатор) и присваивают ISL'ам статус «upstream» (вверх) или «downstream» (вниз) в зависимости от того, ведет этот линк в сторону главного свитча или на периферию.

Кольцо (англ. ring fabric) практически повторяет схему топологии решётки. Среди преимуществ — использование меньшего количества ISL-соединений.

Приложение 2. RTP (Real-time Transport Protocol)

RTP (Real-time Transport Protocol) — протокол передачи данных, работает на прикладном уровне и используется при передаче трафика реального времени. Впервые опубликован в 1996 году, выведен из употребления в 2003 году.

Описание протокола

RTP был разработан как протокол для передачи потоковых данных в режиме реального времени по технологии end-to-end. Рассматривался как основной стандарт для передачи голоса и видео в IP-сетях. В протокол заложена возможность компенсации джиттера и обнаружения нарушения последовательности пакетов данных — типичных событий при передаче через IP-сети. RTP поддерживает передачу данных для нескольких адресатов через Multicast.

Основное отличие RTP от TCP состоит в том, что TCP позволяет себе временную задержку ради полной достоверности передаваемых данных, в то время как RTP допускает некоторую потерю пакетов ради оперативной доставки информации в режиме реального времени. Поэтому большинство реализаций RTP базируются на UDP.

Компоненты протокола

Спецификация RTP описывает два подпротокола:

- Протокол передачи данных, RTP, который взаимодействует с передачей данных реального времени. Информация, предоставляемая посредством этого протокола, включает в себя отметку времени(для синхронизации), последовательный номер (для детектирования потери и дублирования пакетов) и формат полезной нагрузки, который определяет формат кодирования данных.
- Протокол контроля, RTCP, используемый для определения качества обслуживания (QOS), обратной связи и синхронизации между медиа-потоками. Занимаемая полоса пропускания RTCP мала в сравнении с RTP, обычно около 5 %.
- Управляющий сигнальный протокол, такой как SIP, H.323, MGCP или H.248. Сигнальные протоколы управляют открытием, модификацией и закрытием RTP-сессий между устройствами и приложениями реального времени.

Управляющий протокол описания медиа, такой как Session Description Protocol.