Алматинский институт энергетики и связи

**Кафедра телекоммуникационных систем**

IP-телефония и видеосвязь

Г.С. Казиева

**Конспект лекций**

для студентов – бакалавров всех видов обучения,

для специальности 050719 – Радиотехника, электроника и телекоммуникации

**Алматы  2007**

 СОСТАВИТЕЛЬ: Г.С. Казиева IP-телефония и видеосвязь. Конспект лекций  для студентов всех форм обучения специальности 050719 – Радиотехника, электроника и телекоммуникации. -Алматы: АИЭС, 2007. – 58с.

  Данный конспект лекций освещает тенденции современных информационных технологий, позволяющие создавать, хранить, перерабатывать и обеспечивать эффективные способы представления информации потребителю.

Работа устройств в сети Интернет осуществляется с использованием специального протокола IP (Internet Protocol протокол межсетевого взаимодействия). В настоящее время IP протокол используется не только в сети Интернет, но и в других сетях передачи данных с пакетной коммутацией (локальных, корпоративных, региональных). И во всех этих сетях, имеется возможность передавать речевые сообщения с использованием пакетов данных. Такой способ передачи речи получил название IP-телефония. В лекциях охвачены  вопросы передачи речи в IP-телефонии рассмотрены различные сценарии реализаций IP-телефонии. Охвачены также вопросы реализации видеосвязи.

 Лекции предназначены для студентов, обучающихся по специальности 050719 – Радиотехника, электроника и телекоммуникации.

Содержание

Введение

**1  Лекция 1. Сеть Интернет и протокол IP**

**2 Лекция2. Способы передачи голосовых пакетов по IP-сетям**

3 Лекция3. Построение сети по рекомендации ITU H.323

4 Лекция4 . Установление соединения в сетях IP-телефонии

**5 Лекция 5 . Реализации сценариев IP-телефонии**

6Лекция 6  Обеспечение качества IP-телефонии

**7Лекция7. Процедуры обработки речи и методы кодирования**

8Лекция8. Принципы реализации IP-телефонии

9Лекция 9.Адресация в IP-сетях

10Лекция 10 .Таблицы маршрутизации в IP-сетях

11Лекция 11.Протоколы маршрутизации и маршрутизаторы

12Лекция 12. Видеосвязь

**13 Лекция 13. Цифровое представление телевизионного сигнала**

Список используемой литературы

Введение

В Республике Казахстан уделено особое значение формированию Национальной информационной системы с широким доступом к глобальным информационным системам и технологиям, являющимися решающими для прогресса страны в XXI веке. Создаются необходимый фундамент и условия для дальнейшего устойчивого развития данной отрасли, все большей ее интеграции в мировое информационное телекоммуникационное пространство.

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

Работа устройств в сети Интернет осуществляется с использованием специального протокола IP (Internet Protocol протокол межсетевого взаимодействия). В настоящее время IP протокол используется не только в сети Интернет, но и в других сетях передачи данных с пакетной коммутацией (локальных, корпоративных, региональных). И во всех этих сетях, имеется возможность передавать речевые сообщения с использованием пакетов данных. Такой способ передачи речи получил название IP-телефония.

В широком смысле основная задача IP-телефонии заключается в обеспечении естественного речевого или видео общения как минимум двух лиц, являющихся абонентами различных коммуникационных сетей, посредством сети связи с коммутацией пакетов. IP-телефония позволяет существенно экономить требуемую полосу пропускания каналов, что неизбежно ведёт к снижению тарифов, особенно на междугородние и международные телефонные разговоры.

Продолжает развиваться Национальная сеть передачи данных, осуществляется модернизация и реконструкция телефонной сети общего пользования, формируются информационные ресурсы, расширяется перечень современных и перспективных услуг телекоммуникаций, включающий такие услуги как: электронный документооборот; электронная коммерция; дистанционное обучение; мультимедиа; телеконференции; IP-телефония.

В настоящее время IP-телефония получила достаточно широкое распространение. Многие компании имеют представительства в разных странах мира и им приходиться тратить большие средства на междугородние и международные переговоры, поэтому IP-телефония, позволяющая тратить на это меньше средств, была сразу же востребована потребителем. Также развитие IP-телефонии уже сейчас вынуждает операторов традиционной связи снижать тарифы на междугородние и международные переговоры.

**1 Лекция 1. Сеть Интернет и протокол IP**

Цель лекции: ознакомить студентов с основами технологии Интернет, протоколом IP, с основами IP-телефонии.

Создатели технологии Интернет исходили из двух основополагающих соображений: невозможно создать единую физическую сеть, которая позволит удовлетворить потребности всех пользователей; пользователям нужен универсальный способ для установления соединений друг с другом.

В пределах каждой физической сети подсоединённые компьютеры используют ту или иную технологию (Ethernet, Token Ring, FDDI, ISDN, соединения типа точка-точка, а в последнее время к этому списку добавились сеть АТМ и даже беспроводные технологии).

Между механизмами коммуникаций, зависящими от данных физических сетей, и прикладными системами встраивается новое программное обеспечение, которое обеспечивает соединение различных физических сетей друг с другом. При этом детали этого соединения скрыты от пользователей и им предоставляется возможность работать как бы в одной большой физической сети. Такой способ соединения в единое целое множества физических сетей и получил название технологии Интернет, на базе которой реализована одноимённая сеть Интернет. Основной протокол, на базе которого строится сеть Интернет, называется Интернет протоколом или протоколом IP.

Для соединения двух и более сетей в сети Интернет используются маршрутизаторы - устройства, которые физически соединяют сети друг с другом и с помощью специального программного обеспечения передают пакеты из одной сети в другую.

Технология Интернет не навязывает какой-то определённой топологии межсетевых соединений. Добавление новой сети к сети Интернет не влечёт за собой её подсоединения к некоторой центральной точке коммутации или установке непосредственных физических соединений со всеми уже входящими в сеть Интернет сетями. Маршрутизатор знает топологию сети Интернет за пределами тех физических сетей, которые он соединяет, и, основываясь на адресе сети назначения, передаёт пакет по тому или иному маршруту. В сети Интернет используются универсальные идентификаторы подсоединённых к ней компьютеров (адреса), поэтому любые две машины имеют возможность взаимодействовать друг с другом. В Интернет должен также быть реализован принцип независимости пользовательского интерфейса от физической сети, то есть должно существовать множество способов установления соединений и передачи данных (см. рисунок 1), одинаковых для всех физических сетевых технологий.



Рисунок 1 – Внутренняя структура сети Интернет

Фундаментальным принципом Интернет является равнозначность всех объединённых с её помощью физических сетей: любая система коммуникаций рассматривается как компонент Интернет, независимо от её физических параметров, размеров передаваемых пакетов данных и географического масштаба. На рисунке 1 использованы одинаковые обозначения для любых физических сетей, объединённых в сеть Интернет.

Универсальная сеть Интернет строится на основе семейства протоколов TCP/IP и включает в себя протоколы четырех уровней коммуникаций (см. рисунок 2).

|  |
| --- |
| **Прикладной Telnet, FTP, E mail** |
| Транспортный TCP, UDP |
| Сетевой IP, ICMP, IGMP |
| Сетевой интерфейс драйвер устройства и сетевая плата |

Рисунок 2 – Четыре уровня стека протоколов TCP/IP

Уровень сетевого интерфейса отвечает за установление сетевого соединения в конкретной физической сети компоненте сети Интернет, к которой подсоединён компьютер. На этом уровне работают драйвер устройства в операционной системе и соответствующая сетевая плата компьютера.

Сетевой уровень основа стека протоколов TCP/IP. Именно на этом уровне реализуется принцип межсетевого соединения, в частности маршрутизация пакетов по сети Интернет. Протокол IP - основной протокол сетевого уровня, позволяющий реализовывать межсетевые соединения. Он используется обоими протоколами транспортного уровня TCP и UDP. Протокол IP определяет базовую единицу передачи данных в сети Интернет IP дейтаграмму, указывая точный формат всей информации, проходящей по сети TCP/IP. Программное обеспечение уровня IP выполняет функции маршрутизации, выбирая путь данных по соединениям физических сетей. Для определения маршрута поддерживаются специальные таблицы; выбор осуществляется на основе адреса сети, к которой подключён компьютер-адресат. Протокол IP определяет маршрут отдельно для каждого пакета данных, не гарантируя надёжной доставки в нужном порядке. Он задаёт непосредственное отображение данных на нижележащий физический уровень передачи и реализует тем самым высокоэффективную доставку пакетов.

На сетевом уровне протокол IP реализует ненадёжную службу доставки пакетов по сети от системы к системе без установления соединения. Это означает, что будет выполнено всё необходимое для доставки пакетов, однако эта доставка не гарантируется. Пакеты могут быть потеряны, переданы в неправильном порядке, продублированы и т.д. Протокол IP не обеспечивает надёжность коммуникации. Нет контроля ошибок для поля данных, а имеется  только контрольная сумма для заголовка. Надежную передачу данных реализует следующий уровень, транспортный, на котором два основных протокола, TCP и UDP, осуществляют связь между машиной-отправителем пакетов и машиной-адресатом.

Прикладной уровень - это приложения типа клиент-сервер, базирующиеся на протоколах нижних уровней. В отличие от протоколов остальных трёх уровней, протоколы прикладного уровня занимаются деталями конкретного приложения и не интересуются способами передачи данных по сети. Среди основных приложений TCP/IP, имеющихся практически в каждой его реализации, протокол эмуляции терминала TELNET, протокол передачи файлов FTP, протокол электронной почты SMTP, протокол управления сетью SNMP, используемый в системе World Wide Web (WWW), протокол передачи гипертекста HTTP и другие.

Между конечными системами может быть несколько десятков маршрутизаторов и множество промежуточных физических сетей различных типов, но приложение будет воспринимать этот конгломерат как единую физическую сеть. Это и обуславливает основную силу и привлекательность технологии Интернет и протокола IP.

 **2 Лекция2. Способы передачи голосовых пакетов по IP-сетям**

Цель лекции: ознакомить студентов с принципами пакетной передачи речи, дать классификацию сетей IP-телефонии.

**2.1 Принципы пакетной передачи речи**

"Классические" телефонные сети основаны на технологии коммутации каналов (см. рисунок 3),  которая для каждого телефонного разговора требует выделенного физического соединения. Следовательно, один телефонный разговор представляет собой одно физическое соединение физических каналов. В этом случае аналоговый сигнал шириной 3,1 кГц передаётся на ближайшую АТС, где мультиплексируется по технологии временного разделения с сигналами, которые поступают от других абонентов, подключённых к этой АТС. Далее групповой сигнал передаётся по сети межстанционных каналов. Достигнув АТС назначения, сигнал демультиплексируется и доходит до адресата. Основным недостатком телефонных сетей с коммутацией каналов является неэффективное использование полосы канала - во время пауз в речи канал не несёт никакой полезной нагрузки.



Рисунок 3 – Соединение в «классической» телефонной сети

 Переход от аналоговых к цифровым технологиям стал важным шагом для возникновения современных цифровых телекоммуникационных сетей. Одним из таких шагов в развитии цифровой телефонии стал переход к пакетной коммутации. В сетях пакетной коммутации по каналам связи передаются единицы информации, которые не зависят от физического носителя. Такими единицами могут быть пакеты, кадры или ячейки (в зависимости от протокола), но в любом случае они передаются по разделяемой сети (см. рисунок 4), более того по отдельным виртуальным каналам, не зависящим от физической среды. Каждый пакет идентифицируется заголовком, который может содержать информацию об используемом им канале, его происхождении и пункте назначения.

В настоящее время в IP-телефонии существует два основных способа передачи голосовых пакетов по IP сети:

-      через глобальную сеть Интернет (Интернет-телефония);

-      используя сети передачи данных на базе выделенных каналов (IP-телефония).



Рисунок 4 – Соединение в сети с коммутацией пакетов

В первом случае полоса пропускания напрямую зависит от загруженности сети Интернет пакетами, содержащими данные, голос, графику и так далее, а значит, задержки при прохождении пакетов могут быть самыми разными. При использовании выделенных каналов исключительно для голосовых пакетов можно гарантировать фиксированную скорость передачи. В виду широкого распространения сети Интернет особый интерес вызывает реализация системы Интернет-телефонии, но в этом случае качество телефонной связи оператором не гарантируется. Для того чтобы осуществить междугородную (международную) связь с помощью телефонных серверов, организация или оператор услуги должны иметь по серверу в тех местах, куда и откуда планируются звонки.

Общий принцип действия телефонных серверов Интернет-телефонии таков: с одной стороны, сервер связан с телефонными линиями и может соединиться с любым телефоном мира. С другой стороны сервер связан с Интернетом и может связываться с любым компьютером в мире. Сервер принимает стандартный телефонный сигнал, оцифровывает его (если он исходно не цифровой), значительно сжимает, разбивает на пакеты и отправляет через Интернет по назначению с использованием протокола IP. Для пакетов приходящих из сети на телефонный сервер и уходящих в телефонную линию, операция происходит в обратном порядке.

 Вход сигнала в телефонную сеть и его выход из телефонной сети происходят практически одновременно, что позволяет обеспечить полнодуплексный разговор. На основе этих базовых операций можно построить много различных конфигураций. Например, звонок телефон - компьютер или компьютер - телефон может обеспечивать один телефонный сервер.

Для организации связи телефон (факс) - телефон (факс) нужно два сервера. Основным сдерживающим фактором на пути масштабного внедрения IP-телефонии является отсутствие в протоколе IP механизмов обеспечения гарантированного качества услуг, что делает его пока не самым надёжным транспортом для передачи голосового трафика. Сам протокол IP не гарантирует доставку пакетов, а также время их доставки, что вызывает такие проблемы, как рваный голос и просто провалы в разговоре.

С точки зрения масштабируемости IP- телефония представляется вполне законченным решением.

 Соединение на базе протокола IP может начинаться и заканчиваться в любой точке сети от абонента до магистрали. Соответственно, IP- телефонию можно вводить участок за участком.

 Для решений IP-телефонии характерна определённая модульность: количество и мощность различных узлов шлюзов, контролеров зоны можно наращивать практически независимо, в соответствии с текущими потребностями. Проблемы наращивания ресурсов сетевой инфраструктуры не учитываются, поскольку узлы самой сети могут быть независимы от системы IP-телефонии, могут и совмещать в себе их функции.

  Классификация сетей IP-телефонии

Сеть IP-телефонии представляет собой совокупность оконечного оборудования, каналов связи и узлов коммутации. Сети IP-телефонии строятся по тому же принципу, что и сети Интернет. Однако в отличие от сетей Интернет, к сетям IP-телефонии предъявляются особые требования по обеспечению качества передачи речи. Одним из способов уменьшения времени задержки речевых потоков в узлах коммутации является сокращение количества узлов коммутации, участвующих в соединении. Поэтому при построении крупных транспортных сетей ,в первую очередь ,организуется магистраль, которая обеспечивает транзит трафика между отдельными участками сети, а оконечное оборудование (шлюзы) включается в ближайший узел коммутации (см. рисунок 5).

Оптимизация маршрута позволяет улучшить качество предоставляемых услуг. При подключении к сети других операторов их оборудование также подключается к ближайшему узлу коммутации.

Для связи между устройствами внутри сети и с устройствами других сетей IP-телефонии используются выделенные каналы или сеть Интернет. По способу связи оконечных устройств между собой сети IP- телефонии можно разделить на выделенные, интегрированные и смешанные.

В выделенных сетях (см. рисунок 6) связь между оконечными устройствами осуществляется по выделенным каналам и пропускная способность этих каналов используется только для передачи речевых пакетов. Чаще всего провайдеры IP-телефонии не строят собственную инфраструктуру, а арендуют каналы у провайдеров первичной сети.



Рисунок 5 – Пример построения сети с использованием магистрали



Рисунок 6 – Пример построения сети IP-телефонии

Главное преимущество выделенной сети - это высокое качество передачи речи, так как такие сети предназначены только для передачи речевого трафика. Для обеспечения гарантированного качества предоставляемых услуг в этих сетях, кроме протокола IP, применяются и другие транспортные протоколы ATM и Frame Relay.

**3 Лекция3.** **Построение сети по рекомендации ITU H.323**

Цель лекции: рассмотреть варианты построения сетей IP-телефонии по рекомендации H.323.

 Первый в истории подход к построению сетей IP-телефонии на стандартизированной основе предложен Международным Союзом Электросвязи (ITU) в рекомендации Н.323. Сети на базе протоколов Н.323 ориентированы на интеграцию с телефонными сетями и могут рассматриваться как сети ISDN, наложенные на сети передачи данных.

Рекомендация Н.323 предусматривает довольно сложный набор протоколов, который предназначен не просто для передачи речевой информации по IP сетям с коммутацией пакетов. Его цель обеспечить работу мультимедийных приложений в сетях с негарантированным качеством обслуживания. Речевой трафик это только одно из приложений Н.323 наряду с видеоинформацией и данными.

Вариант построения сетей IP-телефонии по рекомендации Н.323 хорошо подходит тем операторам, которые заинтересованы в использовании IP сети для предоставления услуг междугородней и международной связи.

На рисунке 9 показана архитектура сети на базе рекомендации Н.323. Основными устройствами сети являются: терминал, шлюз, контроллер зоны (привратник) и устройство управления конференциями.



Рисунок 7 – Архитектура сети Н.323

 Терминал Н.323 представляют собой конечную точку в сети способную передавать и принимать трафик в масштабе реального времени, взаимодействуя с другим терминалом Н.323, шлюзом или устройством управления многоточечной конференцией.

Для обеспечения этих функций терминал включает в себя:

-      элементы аудио (микрофон, акустические системы, система акустического эхоподавления);

-      элементы видео (монитор, видеокамера);

-      элементы сетевого интерфейса;

-      интерфейс пользователя.

Технология передачи голоса по IP сети вместо классической сети с коммутацией каналов предусматривает конфигурацию с установкой шлюзов. Шлюз обеспечивает сжатие информации (голоса), конвертирование её в IP пакеты и направление в IP-сеть. С противоположной стороны шлюз осуществляет обратные действия: расшифровку и расформирование пакетов вызовов. В результате обычные телефонные аппараты без проблем принимают эти вызовы.

Такое преобразование информации не должно значительно исказить исходный речевой сигнал, а режим передачи обязан сохранить обмен информацией между абонентами в реальном масштабе времени.

Основные функции, выполняемые шлюзом, состоят в следующем:

-      реализация физического интерфейса с телефонной и IP сетью;

-      детектирование и генерация сигналов абонентской сигнализации;

-      преобразование сигналов абонентской сигнализации в пакеты и обратно;

-      соединение абонентов;

-      передача по сети сигнализационных и речевых пакетов;

-      разъединение связи.

Большая часть функций шлюза в рамках архитектуры TCP/IP реализуются в процессах прикладного уровня. Схема обработки сигналов в шлюзе при подключении аналогового двухпроводного телефонного канала показано на рисунке 8.Телефонный сигнал с двухпроводной абонентской линии поступает на дифференциальную схему, которая разделяет приёмную и передающую части канала. Далее сигнал передачи вместе с просочившейся частью сигнала приёма подаётся на аналого-цифровой преобразователь (АЦП) и превращается в стандартный 12-разрядный сигнал. В последнем случае обработка должна включать соответствующий экспандер. В устройстве эхокомпенсации из сигнала передачи удаляются остатки принимаемого сигнала. Эхокомпенсатор представляет собой фильтр. Для обнаружения и определения сигналов внутриполосной многочастотной телефонной сигнализации (MF сигналов), сигналов частотного (DTMF) или импульсного наборов используются детекторы соответствующих типов. Дальнейшая обработка входного сигнала происходит в речевом кодере. В анализаторе кодера сигнал сегментируется на отдельные фрагменты определённой длительности (в зависимости от метода кодирования) и каждому входному блоку сопоставляется информационный кадр соответствующей длины.

Часть параметров, вычисленная в анализаторе кодера, используется в блоке определения голосовой активности, который решает, является ли текущий анализируемый фрагмент сигнала речью или паузой.



Рисунок 8 – Схема обработки сигналов в шлюзе

 При наличии паузы информационный кадр может не передаваться в службу виртуального канала. На сеансовый уровень передаётся лишь каждый пятый паузный информационный кадр. При отсутствии речи для кодировки текущих спектральных параметров используется более короткий информационный кадр. На приёмной стороне из виртуального канала в логический поступает либо информационный кадр, либо флаг наличия паузы. На паузных кадрах вместо речевого синтезатора включается генератор комфортного шума, который восстанавливает спектральный состав паузного сигнала. Параметры сигнала обновляются при получении паузного информационного кадра. Наличие информационного кадра включает речевой декодер, на выходе которого формируется речевой сигнал. Для эхокомпенсатора этот сигнал является сигналом дальнего абонента, фильтрация которого даёт составляющую электрического эха в передаваемом сигнале. В зависимости от типа цифроаналогового преобразования, сигнал может быть подвергнут дополнительной кодировке.

Можно выделить следующие основные проблемы цифровой обработки сигналов в шлюзе.

При использовании двухпроводных абонентских линий актуальной остаётся задача эхокомпенсации, особенность которой состоит в том, что компенсировать необходимо два различных класса сигналов речи и телефонной сигнализации. Очень важной является задача обнаружения и детектирования телефонной сигнализации. Её сложность состоит в том, что служебные сигналы могут перемешиваться с сигналами речи.

В контроллере зоны (привратнике) сосредоточен весь интеллект сети IP-телефонии. Сеть, построенная в соответствии с рекомендацией Н.323, имеет зонную архитектуру. Контроллер зоны выполняет функции управления одной зоной сети IP-телефонии, в которую входят: терминалы, шлюзы, устройства управления конференциями, зарегистрированные у одного контроллера зоны. Отдельные фрагменты зоны сети Н.323 могут быть территориально разнесены и соединяться друг с другом через маршрутизаторы.

Наиболее важными функциями контроллера зоны являются:

-      регистрация оконечных и других устройств;

-      контроль доступа пользователей системы к услугам IP-телефонии при помощи сигнализации RAS;

-      преобразование alias адреса вызываемого пользователя (объявленного имени абонента, телефонного номера, адреса электронной почты и др.) в транспортный адрес сетей с маршрутизацией пакетов IP (IP адрес -номер порта TCP);

-      контроль, управление и резервирование пропускной способности сети;

-      ретрансляция сигнальных сообщений Н.323 между терминалами.

В одной сети IP-телефонии, отвечающей требованиям ITU H.323, может находиться несколько контроллеров зоны, взаимодействующих друг с другом по протоколу RAS.

Устройство управления конференциями (MCU) обеспечивает возможность организации связи между тремя или более участниками. Рекомендация Н.323 предусматривает три вида конференции: централизованная (то есть управляемая MCU, с которым каждый участник конференции соединяется в режиме точка-точка), децентрализованная (каждый участник конференции соединяется с остальными её участниками в режиме точка группа точек) и смешанная. Устройство управления конференциями состоит из одного обязательного элемента контроллера конференций (MC), и, может включать в себя один или более процессоров для обработки пользовательской информации (МР). МС может быть физически совмещён с контроллером зоны, шлюзом или устройством управления конференциями, а последнее, может быть совмещено со шлюзом или контроллером зоны.

Существует ещё один элемент сети Н.323 – прокси-сервер Н.323, то есть сервер-посредник. Этот сервер функционирует на прикладном уровне и может проверять пакеты с информацией, которой обмениваются два приложения. Прокси-сервер может определять, с каким приложением (Н.323 или другим) ассоциирован вызов, и осуществляет нужное соединение.

Семейство протоколов Н.323 включает в себя три основных протокола: протокол взаимодействия оконечного оборудования с привратником RAS, протокол управления соединениями Н.225 и протокол управления логическими каналами Н.245.

Международный союз электросвязи в рекомендации Н.225.0 определил протокол взаимодействия компонентов сети Н.323: оконечного оборудования (терминалов, шлюзов, устройств управления конференциями) с привратником. Этот протокол получил название RAS (Registration, Admission and Status).

**4. Лекция 4 .Установление соединения в сетях IP-телефонии**

Цель лекции:: ознакомить студентов с принципами установления соединения в сетях IP-телефонии.

 4.1Принципы установления соединения в сетях IP-телефонии

В традиционной телефонии вызывающий пользователь набирает номер нужного ему абонента, а телефонная сеть использует его для маршрутизации вызова. Процедура управления вызовами делится на три фазы: установления соединения, передача речи или данных и разъединение. Сообщения системы сигнализации инициируют и завершают эти фазы, а стандартные контрольные сигналы и записанные голосовые сообщения информируют абонента о характере прохождения его вызова.

В системах IP-телефонии процедуры управления вызовами (см. рисунок 9) выполняются протоколами сигнализации.



Рисунок 9 – Управление вызовами в сети IP-телефонии

 Ещё важный вопрос в IP-телефонии – это контроль за доступом к сети. В сети телекоммуникаций общего пользования (СТОП) абонент подключается к АТС через фиксированный местный шлейф, поэтому идентифицировать его телефонный аппарат очень просто. В сети IP-телефонии всё гораздо сложнее, поскольку существует множество разных способов доступа к ней:

-         с обычного телефона через СТОП;

-         по модемному соединению через сервер удалённого доступа;

-         через ЛВС и территориально распределённую сеть.

В общем случае для установления соединения между вызываемым и вызывающим абонентом шлюзы IP-телефонии должны:

-         найти контроллер зоны, на котором возможна регистрация оконечного устройства;

-         зарегистрировать свой мнемонический адрес на контроллере зоны;

-         указать требуемую полосу пропускания;

-         передать запрос на установление соединения;

-         установить соединение;

-         в процессе вызова управлять параметрами соединения;

-         разъединить соединение.

 Алгоритмы установления, поддержания и разрушения соединения

В общем случае алгоритмы установления, поддержания и разрушения соединений по Н.323 включают в себя следующие фазы:

-         фаза А. Установление соединения;

-         фаза В. Определение ведущего/ведомого оборудования и обмен данными о функциональных возможностях;

-         фаза С. Установление аудиовизуальной связи между вызывающим и вызываемым оборудованием;

-         фаза D. Изменение полосы пропускания, запрос текущего состояния оборудования, создание конференций и обращение к дополнительным услугам;

-         фаза Е. Завершение соединения.

Базовое соединение с участием контроллера зоны осуществляется: вызывающее оборудование передаёт сообщение ARQ с alias адресом вызывающего абонента, в ответ на которое контроллер зоны передаёт сообщение ACF с уведомлением, что именно он будет маршрутизировать сигнальные сообщения, и с указанием транспортного адреса своего сигнального канала. Далее вызывающее оборудование передаёт на этот транспортный адрес запрос соединения Setup (установка). Контроллер зоны пересылает сообщение Setup вызываемому оборудованию и передаёт вызывающему оборудованию сообщение Call Proceeding (переход запроса), означающее, что полученной информации достаточно для обслуживания поступившего вызова. Вызываемое оборудование также отвечает на Setup сообщением Call Proceeding. Если оборудование имеет возможность принять вызов, то оно передаёт запрос допуска к ресурсам сети ARQ, на который контроллер зоны может ответить подтверждением ACF или отказом в допуске к ресурсам сети ARG. В первом случае вызываемое оборудование передаёт сообщение Alerting (приведение в готовность), и контроллер зоны маршрутизирует его к вызывающему оборудованию. Вызываемому пользователю подаётся визуальный или акустический сигнал о входящем вызове, а вызывающему подаётся индикация того, что вызываемый пользователь не занят и ему подаётся вызывной сигнал. При отказе в допуске к ресурсам сети вызываемое оборудование закрывает сигнальный канал путём передачи контроллеру зоны сообщения Release Complete (освобождение).

После того, как вызываемый пользователь примет входящий вызов, контроллеру зоны передаётся сообщение Connect с транспортным адресом управляющего канала Н.245 вызываемого оборудования. Контроллер заменяет этот адрес транспортным адресом своего управляющего канала Н.245 и пересылает Connect вызывающему оборудованию, после чего открывается управляющий канал Н.245.

Чтобы ускорить открытие разговорной сессии, управляющий канал может быть открыт вызываемым оборудованием после получения сообщения Setup c транспортным адресом управляющего канала Н.245 вызывающего оборудования или контроллера зоны, или вызывающим пользователем после получения сообщения Call Proceeding или Alerting, содержащего транспортный адрес управляющего канала Н.245 вызываемого пользователя или контроллера зоны.

После открытия управляющего канала Н.245 начинается обмен данными о функциональных возможностях оборудования. В нашем случае все управляющие сообщения, передаваемые от одного оконечного оборудования к другому, маршрутизируются контроллером зоны. Терминалы обмениваются сообщениями TerminalCapabilitySet (терминальный набор способностей), в которых указываются возможные алгоритмы декодирования принимаемой информации. Следует отметить, что сообщение TerminalCapabilitySet должно быть первым сообщением, передаваемым по управляющему каналу. Оборудование, принявшее сообщение TerminalCapabilitySet от другого оборудования, подтверждает его получение передачей сообщения TerminalCapabilitySetAck.

Затем инициируется процедура определения ведущего/ведомого оборудования, необходимая для разрешения конфликтов, возникающих между двумя устройствами при организации конференции, когда оба они могут быть активными контроллерами конференций, или между двумя устройствами, пытающимися одновременно открыть двунаправленные логические каналы. В ходе процедуры устройства обмениваются сообщениями masterSlaveDetermination (определение главного).

В ответ на полученные сообщения (mSD) оба устройства передают сообщения mSDAck, в которых указывается, какое из этих устройств является для данного соединения ведущим, а какое ведомым. Оборудование, передавшее сообщение mSD и получившее в ответ сообщение mSDAck, передаёт сообщение mSDAck.

После обмена данными о функциональных возможностях и определения ведущего и ведомого оборудования может выполняться процедура открытия однонаправленных логических каналов. В требовании открыть логический канал Open LogicalChannel (открыть логический канал) оборудование указывает вид информации, который будет передаваться по этому каналу, и алгоритм кодирования. Логический канал предназначается для переноса речи, поэтому в сообщении OpenLogicalChannel включается параметр media Control Channel с указанием транспортного адреса канала RTCP, при помощи которого производится контроль передачи RTP пакетов. В ответ на сообщение OpenLogicalChannel оборудование должно передать подтверждение OpenLogicalChannelAck, в котором указывается транспортный адрес, на который передающей стороне следует посылать RTP пакеты, а также транспортный адрес канала RTCP.

Далее открывается разговорная сессия. Оборудование вызывающего пользователя передаёт речевую информацию, упакованную в пакеты RTP/UDP/IP, на транспортный адрес RTP канала оборудования вызванного пользователя, а вызванный пользователь передаёт пакетированную речевую информацию на транспортный адрес RTP канала оборудования вызывающего пользователя. При помощи канала RTCP ведётся контроль передачи информации по RTP каналам.

После окончания разговорной фазы начинается фаза разрушения соединения. Оборудование пользователя, инициирующего разъединение, должно прекратить передачу речевой информации, закрыть логические каналы и передать по управляющему каналу Н.245 сообщение end Session Command (команда об окончании сессии), означающее, что пользователь хочет завершить соединение. Далее от встречного оборудования ожидается сообщение endSessionCommand, после приёма которого управляющий канал Н.245 закрывается. Далее, если сигнальный канал ещё открыт, передаётся сообщение Release Complete.

Пользователь, получивший команду endSessionCommand от пользователя, инициировавшего разрушение соединения, должен прекратить передачу речевой информации, закрыть логические каналы и передать сообщение end Session Command. Далее, если сигнальный канал остался открытым, передаётся сообщение Release Complete, и сигнальный канал закрывается.

После всех этих действий оконечное оборудование извещает контроллер зоны об освобождении зарезервированной полосы пропускания. С этой целью каждый из участников соединения передаёт по каналу RAS запрос выхода из соединения DRQ, на который контроллер зоны должен ответить подтверждением DCF, после чего обслуживание вызова считается завершённым.

**5 Лекция 5.  Реализации сценариев IP-телефонии**

**Цель лекции : рассмотреть со студентами варианты реализации сценариев IP-телефонии.**

**5.1Три основных сценария IP-телефонии**

Рассмотрим три наиболее часто используемых сценария IP-телефонии:

-         "компьютер - компьютер";

-         "компьютер - телефон";

-         "телефон - телефон".

Сценарий "компьютер - компьютер" реализуется на базе стандартных компьютеров, оснащённых средствами мультимедиа и подключённых к сети Интернет. Компоненты модели IP-телефонии по сценарию "компьютер - компьютер" показаны на рисунке 10.

.

Рисунок 10 – Сценарий IP-телефонии "компьютер - компьютер"

 В этом сценарии аналоговые речевые сигналы от микрофона абонента А преобразуются в цифровую форму с помощью аналого-цифрового преобразователя (АЦП), обычно при 8000 отсчётов/с, 8 битов/отсчёт, в итоге 64 Кбит/сек.

Затем отсчёты речевых данных в цифровой форме 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 которым добавляются заголовки протоколов, после чего пакеты передаются через IP- сеть в систему IP- телефонии, обслуживающую абонент Б. Когда пакеты принимаются системой абонента Б, заголовки протокола удаляются, а сжатые речевые данные поступают в устройство, развёртывающие их в первоначальную форму, после чего речевые данные снова преобразуются в аналоговую форму с помощью цифро-аналогового преобразователя (ЦАП) и попадают в телефон абонента Б.

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

Для проведения телефонных разговоров друг с другом абоненты А и Б должны иметь доступ к Интернет или к другой сети с протоколом IP. Рассмотрим алгоритм организации связи между этими абонентами:

-         абонент А запускает своё приложение IP-телефонии, поддерживающее протокол Н.323;

-         абонент Б уже заранее запустил своё приложение IP-телефонии, поддерживающее протокол Н.323,

-         абонент А знает доменное имя абонента Б элемент системы имён доменов(DNS), вводит это имя в раздел "кому позвонить" в своём приложении IP-телефонии и нажимает кнопку Return;

-         приложение IP-телефонии обращается к DNS серверу (который в данном примере реализован в компьютере абонента А) для того, чтобы преобразовать доменное имя абонента Б в Ipадрес;

-         сервер DNS возвращает IP адрес абонента Б;

-         приложение IP-телефонии абонента А получает IPадрес абонента Б и отправляет ему сообщение Н.225 Setup;

-         при получении сообщения Н.225 Setup приложение абонента Б сигнализирует ему о входящем вызове;

-         абонент Б принимает вызов и приложение IP-телефонии отправляет ответное сообщение Н.225 Connect;

-         приложение IP-телефонии у абонента А начинает взаимодействие с приложением у абонента Б в соответствии с рекомендацией Н.245;

-         после окончания взаимодействия по протоколу Н.245 и открытия логических каналов абоненты А и Б могут разговаривать друг с другом через IP сеть.

Сценарий "телефон - компьютер" находит применение в разного рода справочно-информационных службах технической поддержки. Рассмотрим две модификации этого сценария IP-телефонии:

-          от компьютера (пользователя IP сети) к телефону (абоненту СТОП), в частности, в связи с предоставлением пользователям IP сетей доступа к телефонным услугам, в том числе, к справочно-информационным услугам и к услугам Интеллектуальной сети;

-          от абонента СТОП к пользователю IP сети с идентификацией вызываемой стороны на основе нумерации Е.164 или IP адресации.

В первой модификации сценария "компьютер - телефон" соединение устанавливается между пользователем IP сети и пользователем сети коммутации каналов (см. рисунок 11).



Рисунок 11 – Вызов абонента СТОП пользователем IP сети

Предполагается, что установление соединения инициирует пользователь IP сети. Шлюз для взаимодействия сетей СТОП и IP может быть реализован в отдельном устройстве или интегрирован в существующее оборудование СТОП или IP сети.

Рассмотрим несколько подробнее пример упрощённой архитектуры системы IP-телефонии по сценарию "телефон - компьютер" (см. рисунок 12).



Рисунок 12– Пользователя IP сети вызывает абонент СТОП

 При попытке вызвать справочно-информационную службу используя услуги пакетной телефонии и обычный телефон на начальной фазе, абонент А вызывает близлежащий шлюз IP-телефонии. От шлюза к абоненту А поступает запрос ввести номер к которому должен быть направлен вызов и личный идентификационный номер (PIN) для аутентификации и последующего начисления платы ,если это служба, вызов которой оплачивается вызывающим абонентом. Основываясь на вызываемом номере, шлюз определяет наиболее доступный путь к данной службе. Кроме того, шлюз активизирует свои функции кодирования и пакетизации речи, устанавливает контакт со службой, ведёт мониторинг процесса обслуживания вызова и принимает информацию о состояниях этого процесса (занятость посылка вызова разъединение) от исходящей стороны через протокол управления и сигнализации. Разъединение с любой стороны передаётся противоположной стороне по протоколу сигнализации и вызывает завершение установленных соединений и освобождение ресурсов шлюза для обслуживания следующего вызова.

Следующий сценарий "телефон - телефон" отличается от остальных сценариев IP-телефонии, поскольку, целью его применения является предоставление обычным абонентам СТОП альтернативной возможности междугородней и международной телефонной связи. В этом режиме современная технология IP-телефонии предоставляет виртуальную телефонную линию через IP доступ.

Обслуживание вызовов по такому сценарию IP-телефонии выглядит следующим образом. Поставщик услуг IP-телефонии подключает свой шлюз к коммутационному узлу или станции СТОП ,а по сети Интернет или по выделенному каналу соединяется с аналогичным шлюзом находящимся в другом городе или другой стране (см. рисунок 13).



Рисунок 13 – Соединение абонентов СТОП через транзитную IP сеть

 Поставщики услуг IP-телефонии предоставляют услуги "телефон - телефон" путём установки шлюзов IP-телефонии на входе и выходе IP сетей. Абоненты подключаются к шлюзу поставщика через СТОП, набирая специальный номер доступа. Абонент получает доступ к шлюзу, используя персональный идентификационный номер (PIN) или услугу идентификации номера вызывающего абонента. После этого шлюз просит ввести телефонный номер вызываемого абонента, анализирует его 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 сеть.

Для организации соединения через сеть IP, абонент А набирает местный телефонный номер шлюза своего поставщика услуг IP-телефонии. Абоненту А передаётся второй сигнал ответа станции и предлагается ввести телефонный номер вызываемого абонента. Далее устанавливается соединение со стороной вызываемого абонента Б.

Эффективность объединения услуг передачи речи и данных является основным стимулом использования IP-телефонии по сценариям "компьютер - компьютер" и "компьютер - телефон".

**6. Лекция 6 . Обеспечение качества IP-телефонии**

**6.1 Показатели качества IP-телефонии**

Традиционные телефонные сети коммутируют электрические сигналы с гарантированной полосой пропускания, достаточной для передачи сигналов голосового спектра. При фиксированной пропускной способности передаваемого сигнала цена единицы времени связи зависит от удалённости и расположения точек вызова и места ответа.

Сети с коммутацией пакетов не обеспечивают гарантированной пропускной способности, поскольку не обеспечивают гарантированного пути между точками связи.

Для приложений, где не важен порядок и интервал прихода пакетов (например, электронная почта) время задержек между отдельными пакетами не имеет решающего значения. IP-телефония является одной из областей передачи данных, где важна динамика передачи сигнала, которая обеспечивается современными методами кодирования и передачи информации, а также увеличением пропускной способности каналов.

Основными составляющими качества IP-телефонии являются качество речи и сигнализации (см. рисунок 14). Качество речи включает:

-         диалог или возможность пользователя связываться и разговаривать с другим пользователем в реальном времени и полнодуплексном режиме;

-         разборчивость или чистота и тональность речи;

-          эхо слышимость собственной речи;

-         уровень или громкость речи.

Качество сигнализации включает:

-         установление вызова или скорость успешного доступа и время установления соединения;

-         завершение вызова или время отбоя и скорость разъединения;

-         DTMF или определение и фиксация сигналов многочастотного набора номера.



Рисунок 14 – Факторы, влияющие на качество IP-телефонии

 Факторы, которые влияют на качество IP-телефонии, могут быть разделены на две категории: качества IP сети и шлюза.

Факторы качества IP сети:

-         максимальная пропускная способность или максимальное количество полезных и избыточных данных, которая она передаёт;

-         задержка или промежуток времени, требуемый для передачи пакета через сеть;

-         джиттер или задержка между двумя последовательными пакетами.

-         потеря пакета или пакеты, потерянные при передаче через сеть.

Факторы качества шлюза:

-         требуемая полоса пропускания или различные вокодеры требуют различную полосу;

-         задержка или время, необходимое цифровому процессору или другим устройствам обработки для кодирования или декодирования речевого сигнала;

-         буфер джиттера или сохранение пакетов данных до тех пор , пока все пакеты не будут получены и можно будет передать в требуемой последовательности для минимизации джиттера;

-         потеря пакетов или потеря пакетов при сжатии или передаче в оборудовании IP-телефонии;

-         подавление эха или механизм для подавления эха, возникающего при передаче по сети;

-         управление уровнем или возможность регулировать громкость речи.

**6.2 Влияние сети на показатели качества IP-телефонии**

Задержка создаёт неудобство при ведении диалога, приводит к перекрытию разговоров и возникновению эха. Эхо возникает, когда отражённый речевой сигнал вместе с сигналом от удалённого конца возвращается опять к говорящему. Эхо становится трудной проблемой, когда задержка в петле передачи больше, чем 50 мс.

Затруднение диалога и перекрытие разговоров становится серьёзным вопросом качества, когда задержка в одном направлении превышает 250 мс.

Можно выделить следующие источники задержки при передаче речи из конца в конец (см. рисунок 15):

-         задержка накопления (алгоритмическая задержка): эта задержка обусловлена необходимостью сбора кадра речевых отсчётов, выполняемая в речевом кодере;

-         задержка обработки: определённые задержки создаются в процессе кодирования и сбора закодированных отсчётов в пакеты для передачи через пакетную сеть;

-         сетевая задержка: задержка обусловлена физической средой и протоколами, а также буферами, используемыми для удаления джиттера на приёмном конце. Сетевая задержка зависит от ёмкости сети и процессов передачи в сети.



Рисунок 15 – Составляющие задержки в сети IP-телефонии

Время задержки можно отнести к одному из трёх уровней:

-         первый уровень до 200 мс отличное качество связи. Для сравнения, в СТОП допустимы задержки 150, 200 мс;

-         второй уровень до 400 мс хорошее качество связи. Но при сравнении с СТОП разница ощутима;

-         третий уровень до 700 мс приемлемое качество связи для неделовых переговоров. Такое качество связи возможно и в спутниковой связи.

Когда речь или данные разбиваются на пакеты для передачи через IP сеть, пакеты часто прибывают в различное время и в разной последовательности. Это создаёт разброс времени доставки пакетов (джиттер). Джиттер приводит к нарушениям передачи речи, слышимым как трески и щелчки. Различают три формы джиттера:

-         джиттер, зависимый от данных, происходит в случае ограниченной полосы пропускания или при нарушениях в сети;

-         искажения рабочего цикла обусловлено выдержкой распространения между передачей снизу вверх и сверху вниз;

-         случайный джиттер является результатом теплового шума.

Потерянные пакеты в IP-телефонии нарушают речь и создают искажения тембра. Все голосовые кадры обрабатываются как данные, поэтому при пиковых нагрузках голосовые кадры будут отбрасываться, как и кадры данных. Кадры данных не связаны со временем, и отброшенные пакеты могут быть успешно переданы путём повторения, а потеря голосовых пакетов приведёт к неполной передаче информации. Предполагается, что потеря до 5% пакетов незаметна, а свыше 10 – 15 % недопустима. Можно предположить, что с повышением трафика возрастают задержки и потери в канале.

**7. Лекция7. Процедуры обработки речи и методы кодирования**

 Цель лекции: ознакомить студентов с методами кодирования в IP-телефонии .

 7.1 Процедуры обработки речи

Для обеспечения качественной передачи речевых сигналов в IP-телефонии необходима их следующая обработка:

а) устранение всех нежелательных компонентов из входного аудиосигнала. После оцифровки речи надо удалить эхо из динамика в микрофон, комнатное эхо и непрерывный фоновой шум, а также отфильтровать шумы переменного тока на низких частотах звукового спектра. Эти функции реализуются аудиокомпонентами персонального компьютера, так что сама система IP-телефонии может их и не иметь;

б) подавление пауз в речи; распознавание остаточного фонового шума (внешних шумов) и кодирование для восстановления на дальнем конце. Паузы лучше полностью подавлять на ближнем конце. Сигналы DTMF и другие сигналы можно заменить на короткие коды для восстановления на дальнем конце. Из-за того, что функция подавления пауз активизируется, когда громкость речи становится ниже определённого порога, некоторые системы обрезают начала и концы слов (в периоды нарастания и снижения энергии);

в) сжатие голосовых данных. Сжать оцифрованный голос можно разными способами. В идеале решения, используемые в IP-телефонии, должны быть быстрыми, сохранять качество речи и давать на выходе небольшие массивы данных;

г) нарезание сжатых голосовых данных на короткие сегменты равной длины, их нумерация по порядку, добавление заголовков пакетов и передача;

д) приём и переупорядочивание пакетов в адаптивном буфере ресинхронизации для обеспечения интеллектуальной обработки потерь или задержек пакетов. Главной целью является преодоление влияния переменной задержки между пакетами. Решение этой проблемы состоит в буферизации достаточного числа поступающих пакетов с тем, чтобы воспроизведение было непрерывным, даже если время между поступлением пакетов разное.

Одним из важных факторов эффективного использования пропускной способности IP канала, является выбор оптимального алгоритма кодирования/декодирования речевой информации кодека.

Все типы речевых кодеков по принципу действия можно разделить на три группы:

а) кодеки с ИКМ и адаптивной дифференциальной ИКМ (АДИКМ), появившиеся в 50х годах и использующиеся сегодня в системах традиционной телефонии. В большинстве случаев представляют собой сочетание АЦП/ЦАП;

б) кодеки с вокодерным преобразованием речевого сигнала возникли в системах мобильной связи для снижения требований к пропускной способности радиотракта. Эта группа кодеков использует гармонический синтез сигнала на основании информации о его вокальных составляющих фонемах. Обычно такие кодеки реализованы как аналоговые устройства;

в) комбинированные (гибридные) кодеки сочетают в себе технологию вокодерного преобразования/синтеза речи, но оперируют уже с цифровым сигналом посредством специализированных процессоров. Кодеки этого типа содержат в себе ИКМ или АДИКМ кодек и реализованный цифровым способом вокодер.

В голосовых шлюзах IP-телефонии понятие кодека подразумевает не только алгоритмы кодирования/декодирования, но и их аппаратную реализацию. Большинство кодеков, используемых в IP-телефонии, описаны рекомендациями семейства «G» стандарта Н.323 (см. рисунок 16).



Рисунок 16– Стандарты для кодирования речевых сигналов

 Рекомендация G.711, утверждённая МККТТ в 1984 году, описывает кодек, использующий ИКМ преобразование аналогового сигнала с точностью 8 кГц и простейшей компрессией амплитуды сигнала. Скорость потока данных на выходе преобразователя составляет 64 кбит/с (8 бит х 8 кГц). Для снижения шума квантования и улучшения преобразования сигналов с небольшой амплитудой при кодировании используется нелинейное квантование по уровню. Кодек G.711 широко распространён в системах традиционной телефонии. Несмотря на то, что рекомендация G.711 в стандарте Н.323 является основной и первичной, в шлюзах IP-телефонии данный кодек применяется редко из-за высоких требований к полосе пропускания и задержкам в канале передачи. Использование G.711 в системах IP-телефонии обосновано лишь в тех случаях, когда требуется обеспечить максимальное качество кодирования речевой информации при небольшом числе одновременных разговоров.

Один из старейших алгоритмов сжатия речи АДИКМ адаптивная дифференциальная ИКМ (стандарт G.726 был принят в 1984 году). Этот алгоритм даёт практически такое же качество воспроизведения речи, как и ИКМ, однако для передачи информации при его использовании требуется полоса всего 16 32 кбит/с. Метод основан на том, что в аналоговом сигнале, передающем речь, невозможны резкие скачки интенсивности. Поэтому, если кодировать не саму амплитуду сигнала, а её изменение по сравнению с предыдущим значением, то можно обойтись меньшим числом разрядов. Кодек предназначен для использования в системах видеоконференций.

Рекомендация G.723.1 описывает гибридные кодеки, использующие технологию кодирования речевой информации MP MLQ (MultyPulse Multy Level Quantization множественная импульсная, многоуровневая квантизация), данные кодеки можно охарактеризовать, как комбинацию АЦП/ЦАП и вокодера. Кодек G.723.1 осуществляет преобразование аналогового сигнала в поток данных со скоростью 64 кбит/c (ИКМ), а затем при помощи многополосного цифрового фильтра/вокодера выделяет частотные фонемы, анализирует их и передаёт по IP каналу информацию только о текущем состоянии фонем в речевом сигнале. Данный алгоритм позволяет снизить скорость до 5,3 6,3 кбит/с без видимого ухудшения качества речи. Процесс преобразования вносит задержку 37 мс. Кодек G.723.1 широко применяется в голосовых шлюзах и прочих устройствах IP-телефонии. Кодек уступает по качеству кодирования G.729, но менее требователен к ресурсам процессора и пропускной способности канала.

Кодеки G.729 сокращённо называют CSACELP (Conjugate Structure Algebraic Code Excited Linear Prediction сопряжённая структура с управляемым алгебраическим кодом линейным предсказанием). Скорость кодирования речевого сигнала составляет 8 кбит/с. В устройствах VoIP этот кодек занимает лидирующее положение, обеспечивая наилучшее качество кодирования речевой информации при достаточно высокой компрессии.

Гибридный кодек, описанный в рекомендации G.728 в 1992 году относится к категории LDCELP Lowe DelayCode Excited Linear Prediction кодек с управляемым кодом линейным предсказанием и малой задержкой. Кодек обеспечивает скорость преобразования 16 кбит/с, вносит задержку при кодировании 35мс и для реализации необходим процессор с быстродействием более 40 MIPS. Кодек предназначен для использования в системах видеоконференций. В устройствах IP-телефонии данный кодек применяется достаточно редко.

**7.2 Обеспечение качества на базе протоколов RSVP, RTP и RTCP**

Одним из средств обеспечения качества IP-телефонии является использование протокола резервирования ресурсов (Resourse Reservation Protocol, RSVP), рекомендованного комитетом IETF. С помощью RSVP мультимедиа программы могут потребовать специального качества обслуживания (QoS) посредством любого из сетевых протоколов IP, а также UDP, чтобы обеспечить качественную передачу видео и аудиосигналов. Протокол RSVP предусматривает гарантированное QoS благодаря тому, что через каждый компьютер, или узел, может передаваться определённое количество данных.

Протокол RSVP предназначен только для резервирования части пропускной способности. Используя RSVP, отправитель периодически информирует получателя о свободном количестве ресурсов сообщением RSVP Path (см. рисунок 17). Транзитные маршрутизаторы по мере прохождения этого сообщения также анализируют имеющееся у них количество свободных ресурсов и подтверждают его соответствующим сообщением RSVP Resv, передаваемых в обратном направлении. Если ресурсов достаточно, то отправитель начинает передачу. Если ресурсов недостаточно, получатель должен снизить требования или прекратить передачу информации.



Рисунок 17 – Применение протокола RSVP

В виду зависимости RSVP от совместимости предела своих возможностей, когда он не может гарантировать запрошенный уровень QoS, все последующие запросы будут игнорироваться и удаляться. При отказе только одного узла обслуживать запрос вся стройная система RSVP распадается на части.

RSVP имеет весьма хорошие перспективы на корпоративном уровне, где администратор имеет возможность определить, какие параметры будет использовать маршрутизатор для обслуживания запросов о предоставлении QoS. В глобальных сетях маршрутизаторы вовсе необязательно находятся под той же юрисдикцией, что и хосты и приложения, производящие запросы, что осложняет гарантированное QoS.

Для уменьшения значений джиттера и задержек на сетевом уровне применяются гарантирующие пользователю заданный уровень качества механизмы RSVP, MPLS, ATM и другие. Они улучшают качество услуг, предоставляемых сетью, но не могут полностью устранить образование очередей в сетевых устройствах, а, следовательно, и совсем убрать джиттер.

**8. Лекция8. Принципы реализации IP-телефонии**

**Цель лекции : рассмотреть вопросы реализации IP-телефонии.**

**8.1 Оборудование IP-телефонии**

 Ниже приведены перечень  целого ряда компаний, преуспевших в разработке программных средств и оборудования IP-телефонии, среди которых-VocalTec, Dialogic, Cisco, Ascend, 3Com, Nortel, Lucent, IBM, Motorola, RAD, Rock-well, Digitcom и др.

Примером практической реализации концепции Nortel Networks является платформа MMCS (MultiMedia Carrier Switch), прошедшая сертификацию для ВСС России и известная по публикациям в журналах. Другими примерами являются семейство Magellan - пакетные коммутаторы серии DPN (протоколы Х.25, FR) и модельный ряд Passport - устройства доступа с компрессией речи по протоколу FR - Passport 4400, мультипротокольные маршрутизаторы серии Passport 7000/6000, пограничные устройства Passport Voice Gateway, сопрягающие телефонные сети и сети ATM, а также высокоскоростные АТМ-коммутаторы Passport 15000. Все это оборудование позволяет полностью интегрировать речь, факсимильные сообщения, видеоинформацию, данные по протоколам IP, FR, SNA, X.25, HDLC, и обеспечивать мультимедийные услуги, оптимизируя использование имеющихся ресурсов (например, при передаче речи применяется технология передачи пакетов с переменной скоростью).

Еще одним примером оборудования IP-телефонии может служить универсальный маршрутизатор 1Р45/951 с функциями передачи речи и мультимедийной информации по IP-сетям, входящий в гамму продуктов корпорации NEC, Япония. Маршрутизатор 1Р45/951 реализует функции шлюза и привратника. Маршрутизатор поддерживает большое количество алгоритмов кодирования речи, в том числе, ITU-T G.729, G.729a, G.729b, G.729ab, G.723.1, G.729.1a, G.711, G.711VAD, G.728 и G.728VAD. Это позволяет маршрутизатору 1Р45/951 соединяться практически со всеми шлюзами, поддерживающими протокол Н.323, в то время как возможности многих шлюзов ограничены небольшим количеством поддерживаемых алгоритмов кодирования. Маршрутизатор 1Р45/951 обеспечивает хорошее качество передачи речи благодаря следующим особенностям: применение современных алгоритмов кодирования; подавление эха (64 мс); сглаживание джиттера; подавление пауз в разговоре; генерация комфортного шума; поддержка протокола RSVP; сжатие заголовков IP/UDP/RTP; поддержка приоритетов для различных видов трафика.

За последнее время появились следующие виды оборудования IP-телефонии для всех этих сценариев.

1. Автономные шлюзы IP-телефонии, подключаемые к АТС через цифровые и аналоговые интерфейсы и осуществляющие предварительную обработку речевых сигналов, компрессию, упаковку в IP-пакеты и передачу их по сети.

2. Магистральные речевые платы с интерфейсом 10/100BaseT (ЛВС Ethernet) для подключения учрежденческих АТС существующих моделей к корпоративной IP-сети. После установки в АТС такой платы речевой трафик в виде IP-пакетов может быть направлен по локальной или глобальной пакетной сети подобно тому, как он сейчас передается от АТС по телефонной сети.

3. Телефонные аппараты, упаковывающие речевую информацию в IP-пакеты (IP-телефоны) и подключаемые не к телефонной сети, а непосредственно к ЛВС Ethernet. Как правило, такие аппараты требуют от сетевого администратора минимальных настроек, используя протокол динамической конфигурации -Dynamic Host Configuration Protocol (DHCP).

4. Специализированные коммутаторы речевых пакетов, предназначенные для выполнения функций традиционной АТС на базе протокола IP. В литературе такие устройства часто называют IP-АТС, но это название не совсем корректно, поскольку в данном случае осуществляется не автоматическая коммутация каналов, а коммутация пакетов.

В ранних моделях цифровая обработка сигнала производилась программными средствами. Позднее программную обработку сменила аппаратная, основную роль стали выполнять платы DSP (Digital Signal Processing), что разгрузило основной процессор и оперативную память, увеличило число портов оборудования и уменьшило время задержки речевой информации. Наиболее известны платы DSP фирм Texas Instrument, Dialogic (DM3 IP Link) и Natural MicroSystems (Quad E1).

Другим, не менее важным аспектом внедрения IP-телефонии являются шлюзы, обеспечивающие взаимодействие сетей с коммутацией каналов и с коммутацией пакетов.

В настоящее время несколько десятков компаний выпускают подобные изделия, среди них Cisco Systems, VocalTec, Lucent Technologies и др. Более того, на базе этих шлюзов почти каждая крупная телекоммуникационная компания имеет или заявленное, или уже поставляемое изделие IP-телефонии. Предлагаются АТС, реализованные на основе технологии маршрутизации IP-пакетов. Компания Cisco выпустила интегрированный сервер доступа AS5300 с коммутатором Catalyst 5500. Компания Ascend Communications Inc. объединила модем для коммутируемых каналов TNT с гигабитным маршрутизатором GRF. Компания 3Com добавила передачу речи по IP и факса в свой концентратор Total Control Hub.

При внедрении технологии передачи речевой информации по сетям с маршрутизацией IP-пакетов в единой телефонной сети помимо рассмотренных выше, возникают следующие специфические трудности:

- при подключении оборудования IP-телефонии к АТС телефонной сети общего пользования по двухпроводным аналоговым абонентским линиям препятствием часто становится большое затухание сигналов в этих линиях;

- при подключении оборудования IP-телефонии к коммутационному оборудованию СТОП по межстанционным соединительным линиям затруднения связаны с тем, что декадно-шаговые и координатные АТС имеют специфические системы сигнализации, основная из которых определяется неформальным, но весьма точным термином «R полтора»; присутствующие в СТОП декадно-шаговые АТС создают большие помехи и поддерживают только импульсный набор номера.

Рассмотрим на примере оборудования Протей-ITG построение IP-сети для казахстанских условий. Шлюз IP-телефонии Протей-ITG реализует передачу речевого трафика и факсимильной информации по сетям с маршрутизацией пакетов IP по протоколу Н.323, версия 2. Основным функциональным назначением шлюза является преобразование речевой информации, поступающей от СТОП с постоянной скоростью передачи, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP: кодирование и упаковка речевой информации в пакеты RTP/U DP/IP, а также обратное преобразование. Кроме того, шлюз конвертирует сигнальные сообщения систем сигнализации E-DSS1 и ОКС7 (ISUP-R, российская версия) в сигнальные сообщения Н.323 и производит обратное преобразование по рекомендации ITU H.246.

Шлюз Протей-ITG подключается к СТОП по цифровым линиям со скоростью передачи 2048 Кбит/с (Е1) с использованием сигнализации ISUP-R системы общеканальной сигнализации ОКС7, абонентской сигнализации E-DSS1, а также сигнализации по двум выделенным сигнальным каналам «R1.5», а к сетям с маршрутизацией пакетов IP - при помощи интерфейса 10/100Вазе-Т.

На рисунке 18 изображена обобщенная структура шлюза IP-телефонии Протей-ITG. Следует отметить, что кодирование и пакетирование речевых сигналов, поступающих из СТОП для последующей их передачи по IP-сети, реализованы в Протей-ITG на базе специализированных процессоров обработки цифровых сигналов - Digital Signal Processors (DSP). Остальные функции выполняются программным обеспечением, использующим универсальный процессор.



Рисунок 18 – Структурная схема шлюза Протей-ITC

Модуль обработки телефонной сигнализации взаимодействует с телефонным оборудованием, преобразуя сигналы систем DSS1 и ОКС7 во внутрисистемные примитивы, которые отражают состояния процесса обслуживания вызова (соединения, отбой и т.п.) и используются модулем логики услуг шлюза для установления соединений между СТОП и IP-сетью.

Модуль сигнализации Н.323 обрабатывает сигнальную информацию протоколов RAS, Н.225.0 (Q.931) и Н.245. Информация о состояниях процесса обслуживания вызова в IP-сети передается в модуль логики услуг шлюза.

Модуль логики услуг шлюза IP-телефонии отвечает за маршрутизацию вызова, поступившего из СТОП в IP-сеть. Производятся такие операции, как контроль доступа и анализ телефонного номера вызываемого абонента с последующим определением и предоставлением требуемой услуги. При наличии в сети IP-телефонии привратника многие функции могут быть возложены на него.

Модуль пакетирования речи выполняет функции подготовки речевого сигнала, поступающего из СТОП с постоянной скоростью, для дальнейшей его передачи по сети с маршрутизацией пакетов IP. Основными функциями модуля являются: преобразование речевого сигнала методом импульсно-кодовой модуляции, эхокомпенсация, кодирование речевого сигнала, обнаружение активных периодов и пауз в речи и адаптация воспроизведения. Кроме того, модуль отвечает за детектирование и генерацию сигналов DTMF и за обработку факсимильных и модемных сигналов. Структура модуля пакетирования речи представлена на рисунке 19.

Механизм обнаружения активных периодов речи проверяет получаемый из СТОП сигнал на наличие в нем речевой информации. Если в течение определенного времени речевая информация не обнаружена, передача речевых пакетов в IP-сеть прекращается .



Рисунок 19 – Модуль пакетирования речи

В привратнике сосредоточен весь интеллект сети IP-телефонии. Он выполняет функции управления зоной сети IP-телефонии, в которую входят терминалы, шлюзы и устройства управления конференциями, зарегистрированные в этом привратнике.

В число наиболее важных функций, выполняемых привратником с целью обеспечения нормального функционирования управляемой зоны сети, входят:

- регистрация оконечного оборудования;

- контроль доступа пользователей системы к услугам IP-телефонии при помощи сигнализации RAS (Рекомендация ITU Н.225.0);

- преобразование a/yas-адреса (имени абонента, телефонного номера, адреса электронной почты и др.) в транспортный адрес сети с маршрутизацией пакетов IP (IP адрес  номер порта TCP/UDP);

- контроль, управление и резервирование пропускной способности сети;

- ретрансляция сигнальных сообщений Н.225.0 и Н.245 между терминалами.

В последнем случае привратник в любое время знает состояние конечных пользователей и может предоставлять дополнительные услуги, такие как переключение связи, переадресация, постановка на ожидание, перехват вызова и т.д.

Возможны два варианта организации связи с использованием оборудования IP-телефонии платформы Протей. В первом варианте шлюз IP-телефонии Протей-ITG и привратник Протей-GK подключаются к существующей сети IP-телефонии.

Если сеть построена на базе оборудования VocalTec или, по крайней мере, с наличием привратника, произведенного фирмой VocalTec, который, как правило, занимается начислением платы за разговоры абонентов, то шлюз Протей-ITG общается с привратником по протоколу RAS, входящему в семейство протоколов Н.323.

**9Лекция 9 . Адресация в IP-сетях**

Цель лекции: ознакомить студентов с принципами адресации в IP-сетях.

 Принятый в IP-сетях способ адресации узлов в немалой степени способствует масштабируемости данной технологии, которая позволяет однозначно иденти­фицировать миллионы сетевых интерфейсов (вспомним хотя бы Интернет с его многомиллионной армией пользователей). Однако чтобы обеспечить такую воз­можность в технологию TCP/IP, пришлось включить целый ряд специальных механизмов и протоколов.

**9.1 Типы адресов стека TCP/IP**

В стеке TCP/IP используются три типа адресов:

*-локальные,* или *аппаратные,* адреса, используемые для адресации узлов в пре­делах подсети;

*-сетевые,* или *IP-адреса,* используемые для однозначной идентификации узлов в пределах всей составной сети:

*-доменные имена –* символьные идентификаторы узлов, к которым часто обращаются пользователи.

В общем случае сетевой интерфейс может иметь одновременно один или не­сколько локальных адресов и один или несколько сетевых адресов, а также одно или несколько доменных имен.

Итак, аппаратный (локальный) адрес идентифицирует узел в пределах подсети. Если подсеть использует одну из базовых технологий LAN – Ethernet, FDDI, Token Ring, – то для доставки данных любому узлу такой подсети достаточно указать MAC-адрес. Таким образом, в этом случае аппаратным адресом является MAC-адрес.

В составную сеть TCP/IP могут входить подсети, построенные на основе более сложных технологий, к примеру, технологии IPX/SPX. Эта сеть сама может быть разделена на подсети, и, так же как IP-сеть, она идентифицирует свои узлы аппаратными и сетевыми IPX-адресами. Но поскольку для составной сети TCP/IP составная сеть IPX/SPX является обычной подсетью, в качестве аппаратных адресов узлов этой подсети выступают те адреса, которые однозначно оп­ределяют узлы в данной подсети, а такими адресами являются IPX-адреса. Ана­логично, если в составную сеть включена сеть Х.25, то локальными адресами для протокола IP соответственно будут адреса Х.25.

IP-адреса представляют собой основной тип адресов, на основании которых  сетевой уровень передает пакеты между сетями. Эти адреса состоят из 4 байт, на­пример 109.26.17.100. IP-адрес назначается администратором при конфигуриро­вании компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произ­вольно либо назначен по рекомендации специального подразделения Интернета
(Internet Network Information Center, InterNIС), если сеть должна работать как
составная часть Интернета. Обычно поставщики услуг Интернета получают диапазоны адресов у подразделений InterNIC, а затем распределяют их между свои­ми абонентами. Номер узла в протоколе IP назначается независимо от локально­го адреса узла. Маршрутизатор по определению входит сразу в несколько сетей, поэтому каждый порт маршрутизатора имеет собственный IP-адрес.

 Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер дол­жен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

*Символьные имена* в IP-сетях называются *доменными* и строятся по иерархиче­скому признаку. Составляющие полного символьного имени в IP-сетях разделяются точкой и перечисляются в следующем порядке: сначала простое имя хоста, затем имя группы узлов (например, имя организации), затем имя более крупной группы (поддомена) и так до имени домена самого высокого уровня (например, домена, объединяющего организации по географическому принципу: RU — Россия, UK – Великобритания, SU – США). Поэтому доменные имена называют также DNS-именами.

 9.2Формы записи IP-адреса

IP-адрес имеет длину 4 байта (32 бита) и состоит из двух логических частей – номера сети и номера узла в сети.

Наиболее употребляемой формой представления IP-адреса является запись в виде четырех чисел, представляющих значения каждого байта в десятичной фор­ме и разделенных точками, например:

126.10.2.30.

Этот же адрес может быть представлен в двоичном формате:

10000000 00001010 00000010 00011110.

А также в шестнадцатеричном формате:

 80.0A.02.1D.

Заметим, что запись адреса не предусматривает специального разграничительного знака между номером сети и номером узла. Каким образом маршрутизаторы, на которые поступают пакеты, выделяют из адреса назначения номер сети, чтобы по нему определить дальнейший маршрут? Какая часть из 32 бит, отведенных под IP-адрес, относится к номеру сети, а какая — к номеру узла? Можно предло­жить несколько вариантов решений этой проблемы.

 Простейший вариант состоит
в том, что все 32-битовое поле адреса заранее делится на две части не обязатель­но равной, но фиксированной длины, в одной из которых всегда будет разме­щаться номер сети, а в другой – номер узла. Решение очень простое, но хорошеели? Поскольку поле, которое отводится для хранения номера узла, имеет фиксированную длину, все сети будут иметь одинаковое максимальное число узлов.
Если, например, под номер сети отвести один первый байт, то всё адресное про­странство распадется на сравнительно небольшое (28) число сетей огромного размера (224 узлов). Если границу передвинуть дальше вправо, то сетей станет больше, но все равно все они будут одинакового размера. Очевидно, что такой жесткий подход не позволяет дифференцированно подходить к потребностям отдельных предприятий и организаций. Именно поэтому такой способ структуризации адреса и не нашел применения.

Второй подход основан на использовании маски, которая позволяет максимально гибко  устанавливать границу между номером сети и номером узла. В данном случае *маска –* это число, которое используется в паре с IP-адресом; двоичная запись маски содержит последовательность единиц в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети. Поскольку номер сети является цельной частью адреса, единицы в маске также должны представлять непрерывную последовательность. Граница между последовательностью единиц и последовательностью нулей в маске соответствует границе между номером сети и номером узла в IP-адресе. При таком подходе адресное пространство можно представить как совокупность множества сетей разного размера.

Вводится несколько классов сетей, и для каждого класса определены свои размеры.

Классы IP-адресов

Традиционная схема деления IP-адреса на номер сети и номер узла основана на понятии класса, который определяется значениями нескольких первых битов ад­реса. Именно потому, что первый байт адреса 185.23.44.206 попадает в диапазон 128-191, мы можем сказать, что этот адрес относится к классу B, а значит, номе­ром сети являются первые два байта IP-адреса, дополненные двумя нулевыми байтами – 185.23,0.0, а номером узла – два младшие байта, дополненные с нача­ла двумя нулевыми байтами – 0.0.44.206.

Принадлежность IP-адреса к классу определяется значениями первых битов ад­реса. На рисунке. 20 показана структура IP-адресов разных классов.



Рисунок 20-. Структура IP-адресов

 Если адрес начинается с 0, то этот адрес относится к классу A, в котором под номер сети отводится один байт, а остальные три байта интерпретируются как номер узла в сети. Сети, имеющие номера в диапазоне от 1 (00000001) до 126 (01111110), называются сетями класса А. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже.) Сетей клас­са А немного, зато количество узлов в них может достигать 224, то есть 16777216 узлов.

Если первые два бита адреса равны 10, то адрес относится к классу В. В адресах: класса В под номер сети и под номер узла отводится по два байта. Сети, имеющие номера в диапазоне от 128.0 (1000000000000000) до 191.255 (1011111111111111), называются сетями класса В. Таким образом, сетей класса В больше, чем сетей класса А, но размеры ихменьше, максимальное количество узлов в них составляет 216 (65536).

Если адрес начинается с последовательности битов 110, то это адрес класса С. В этом случае под номер сети отводился 24 бита, а под номер узла – 8 бит. Сети класса C наиболее распространены, но число узлов в них ограничено значением 28 (256) узлов.

Еще два класса адресов D и Е не связаны непосредственно с сетями.

Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, *групповой адрес (multicast).* Групповой адрес идентифицирует группу узлов (сетевых интерфейсов), которые в общем случае могут принадлежать разным сетям. Интерфейс, входящий в группу, получает наряду с обычным индивидуальным IP-адресом еще один групповой адрес. Если при от­правке пакета в качестве адреса назначения указан адрес класса D, то такой па­кет должен быть доставлен всем узлам, которые входят в группу.

Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к классу E. Адреса этого класса зарезервированы для будущих применений.

В табл. 1. приведены диапазоны номеров сетей и максимальное число узлов, соответствующих каждому классу сетей.

 Т а б л и ц а 1-. Характеристики адресов разного класса

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Класс | Первые биты  | Наименьшийномер сети  | Наибольший номер сети  | Максимальное число узлов в сети  |
| А  | 0  | 1.0.0.0  | 126.0.0.0  | 224  |
| В  | 10  | 128.0.0.0  | 191.255.0.0  | 216  |
| С  | 110  | 192.0.1.0  | 223.255.255.0  | 28 |
| D  | 1110  | 224.0.0.0  | 239.255.255.255  | Multicast  |
| Е  | 11110  | 240.0.0.0  | 247.255.255.255  | Зарезервирован  |

 Большие сети получают адреса класса A, средние – класса B, а небольшие – класса С:

           -если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом на­значения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется *ограниченным широковещательным сообщением (limited broadcast).* Ограниченность в данном случае означает, что пакет не выйдет за границы маршрутизатора ни при каких усло­виях;.

              -если в поле номера узла назначения стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети. Напри­мер, пакет с адресом 192.190.21.255 доставляется всем узлам сети 192.190.21.0. Такая рассылка называется *широковещательным сообщением (broadcast).*

Специальные адреса, состоящие из последовательностей нулей, могут быть ис­пользованы только в качестве адреса отправителя, а адреса, состоящие из после­довательностей единиц, — только в качестве адреса получателя.

10Лекция 10 .Таблицы маршрутизации в IP-сетях

 Цель лекции: ознакомить студентов с маршрутизациейвIP-сетях.

Программные модули протокола IP устанавливаются на всех конечных станци­ях и маршрутизаторах сети. Для продвижения пакетов они используют таблицы маршрутизации.

10.1Примеры таблиц для маршрутизаторов различных типов

Структура таблицы маршрутизации стека TCP/IP соответствует общим прин­ципам построения таблиц маршрутизации, рассмотренным выше. Однако важно отметить, что вид таблицы IP-маршрутизации зависит от конкретной реали­зации стека TCP/IP. Приведем пример трех вариантов таблицы маршрутиза­ции, с которыми мог бы работать маршрутизатор M1 всети, представленной на рисунке 21.



Рисунок 21 – Пример маршрутизируемой сети

 10.1.1Назначение полей таблицы маршрутизации

Несмотря на достаточно заметные внешние различия, во всех трех таблицах есть все ключевые параметры, необходимые для работы маршрутизатора и рассмот­ренные ранее при обсуждении концепции маршрутизации.

К таким параметрам, во-первых, относится адрес сети назначения (столбцы «Destination» в маршрутизаторах NetBuilder и UNIX или «Network Address» в маршру­тизаторе MPR). Заметим, что в некоторых случаях, когда маршрут к одному из узлов сети отличается от маршрута ко всем остальным узлам данной сети, в этом столбце указывается адрес данного конкретного узла назначения.

Вторым обязательным полем таблицы маршрутизации является адрес следую­щего маршрутизатора (столбцы «Gateway» в маршрутизаторах NetBuilder и UNIX или «Gateway Address» в маршрутизаторе MPR).

Третий ключевой параметр – адрес порта, на который нужно направить пакет, в некоторых таблицах указывается прямо (поле «Interface» в таблице Windows NT), а в некоторых — косвенно. Так, в таблице UNIX-маршрутизатора вместо адреса порта задается его условное наименование – lе0 для порта с адресом 198.21.17.5, le1 для порта с адресом 213.34.12.3 и lo0 для внутреннего порта с ад­ресом 127.0.0.1.

В маршрутизаторе NetBuilder II поле, обозначающее выходной порт в какой-ли­бо форме, вообще отсутствует. Это объясняется тем, что адрес выходного порта всегда можно косвенно определить по адресу следующего маршрутизатора.

Наличие или отсутствие поля маски в таблице говорит о том, насколько современен данный маршрутизатор. Стандартным решением сегодня является исполь­зование поля маски в каждой записи таблицы, как это сделано в таблицах мар­шрутизаторов MPR Windows NT (поле «Netmask») и NetBuilder (поле «Mask»). Обработка масок при принятии решения маршрутизаторами будет рассмотрена ниже. Отсутствие поля маски говорит о том, что либо маршрутизатор рассчитан на работу только с тремя стандартными классами адресов, либо он использует для всех записей одну и ту же маску, что снижает гибкость маршрутизации.

 10.1.2Маршрутизация без использования масок

 Рассмотрим на примере IP-сети алгоритм работы средств сетевого уровня по продвижению пакета в составной сети (рисунок 22). При этом будем считать, что все узлы сети, рассматриваемой в примере, имеют адреса, основанные на клас­сах, а маски не используются. Особое внимание будет уделено взаимодействию протокола IP с протоколами разрешения адресов ARP и DNS.



Рисунок 22 – Пример взаимодействия компьютеров через сеть

 1. Итак, пусть пользователь компьютера cit.dol.ru, находящегося в сети Ethernet и имеющего IP-адрес 194.87.23.17 (адрес класса С), обращается по протоколу FTP к компьютеру s1.msk.su, принадлежащему другой сети Ethernet и имею­щему IP-адрес 142.06.13.14 (адрес класса В):

> ftp s1.msk.su.

2.      Модуль FTP упаковывает свое сообщение в сегмент транспортного протокола TCP который, в cвою очередь, помещает свой сегмент в пакет протокола IP. В заголовке IP-пакета должен быть указан IP-адрес узла назначения. Так как пользователь компьютера cit.dol.ru указывает символьное имя компьюте­ра s1.msk.su, то стек TCP/IP должен определить IP-адрес узла назначения са­мостоятельно.

3.      При конфигурировании стека TCP/IP в компьютере cit.dol.fu был задан его собственный IP-адрес, IP-адрес маршрутизатора по умолчанию и IP-адрес DNS-сервера. Модуль IP может сделать запрос к серверу DNS, но обычно сначала просматривается локальная таблица соответствия символьных имен и IP-адресов. Такая таблица хранится чаще всего в виде, текстового файла простой структуры – каждая его строка содержит запись об одном символьном имени и его IP-адресе. В ОС UNIX такой файл традиционно носит имя hosts и находится в каталоге /etc.

4.  Будем считать, что компьютер cit.dol.ru имеет файл hosts, а в нем есть строка:

142.06.13.14          s1.msk.su.

5.      Таким образом, разрешение имени выполняется локально, и протокол IP мо­жет теперь формировать IP-пакеты с адресом назначения 142,06,13.14 для взаимодействия с компьютеров s1.msk.su.

6.      Модуль IP компьютера cit.dol.ru проверяет, нужно ли маршрутизировать па­кеты с адресом 142.06.13.14. Так как адрес сети назначения (142.06.0.0) не совпадает с адресом (194.87.23.0) сети, которой принадлежит компьютер-от­правитель, то маршрутизация необходима.

7.       Компьютер cit.dol.ru начинает формировать кадр Ethernet для отправки IP-пакета  маршрутизатору  по  умолчанию,  IP-адрес  которого  известен   – 194.87.23.1, но неизвестен MAC-адрес, необходимый для перемещения кадра в локальной сети. Для определения MAC-адреса маршрутизатора протокол IP обращается к протоколу ARP, который просматривает ARP-таблицу. Если в последнее время компьютер cit.dol.ru выполнял какие-либо межсетевые об­мены, то  скорее всего искомая запись, содержащая соответствие между IP- и MAC-адресами маршрутизатора по умолчанию, уже находится в кэш-таблице протокола ARP. Пусть в данном случае нужная запись была найдена именно в кэш-таблице:

194.87.23.1 008048ЕВ7Е60.

8.     Обозначим найденный MAC-адрес 008048ЕВ7Е60 в соответствии сномером маршрутизатора и его порты через MAC11.

9.     В результате компьютер cit.dol.ru отправляет по локальной сети пакет, упако­ванный в кадр Ethernet.

10. Кадр принимается портом 1 маршрутизатора 1 в соответствии с протоколом Ethernet, так как MAC-узел этого порта распознает свой адрес МАС11. Прото­кол Ethernet извлекает из этого кадра IP-пакет и передает его программному обеспечению маршрутизатора, реализующему протокол IP. Протокол IP из­влекает из пакета адрес назначения 142.06.13.14 и просматривает записи сво­ей таблицы маршрутизации. Пусть маршрутизатор 1 имеет в своей таблице маршрутизации следующую запись:

142.06.0.0                     135.12.0.11      2.

11. Эта запись говорит о том, что пакеты для сети 142.06.0.0 нужно передавать маршрутизатору 135.12.0.11, находящемуся в сети, подключенной к порту 2 маршрутизатора 1.

12.  Маршрутизатор 1 просматривает параметры порта 2 и находит, что к нему подключена сеть FDDI. Так как сеть FDDI имеет значение MTU большее,

чем сеть Ethernet, то фрагментация IP-пакета не требуется.

Поэтому маршру­тизатор 1 формирует кадр формата FDDI. На этом этапе модуль IP должен определить MAC-адрес следующего маршрутизатора по известному IP-адресу 135.12.0.11. Для этого он обращается к протоколу ARP. Допустим, что нуж­ной записи в кэш-таблице не оказалось, тогда в сеть FDDI отправляется широковещательный ARP-запрос, содержащий наряду с прочей следующую информацию:

-порт 1 маршрутизатора 2 распознает свой IP-адрес и посылает ARP-ответ по адресу запросившего узла;

-теперь, зная MAC-адрес следующего маршрутизатора 00E0F77F51A0, маршрутизатор 1, отсылает кадр FDDI  по направлению к маршрутизатору 2.

13. Аналогично действует модуль IP на маршрутизаторе 2. Получив кадр FDDI, он отбрасывает его заголовок, а из заголовка IP извлекает IP-адрес сети назначения и просматривает свою таблицу маршрутизации. Там он может найти запись о конкретной сети назначения:

142.06.0.0         203.21.4.12       216.

14. При отсутствии такой записи будет использована запись о маршрутизаторе   по умолчанию:

                 default  203.21.4.12   2.

15.      Определив IP-адрес следующего маршрутизатора 203.21.4.12, модуль IP формирует кадр Ethernet для передачи пакета маршрутизатору 3 по сети Ethernet. С помощью протокола АКР он находит МАС-адрес этого маршрутизатора и помещает его в заголовок кадра. IP-адрес узла назначения, естественно, оста­ется неизменным.:

 16. Наконец, после того, как пакет поступит в маршрутизатор сети назначения (маршрутизатор 3), появляется возможность передачи этого пакета компью­теру назначения. Маршрутизатор 3 определяет, что пакет нужно передать в сеть 142.06.0.0, которая непосредственно подключена к его первому порту. Поэтому он посылает ARP-запрос по сети Ethernet с IP-адресом компьютера s1.msk.su. ARP-ответ содержит MAC-адрес конечного узла, который модуль IP передает канальному протоколу для формирования кадра Ethernet.

 17. Сетевой адаптер компьютера s1.msk.su захватывает кадр Ethernet, обнаружи­вает совпадение MAC-адреса, содержащегося в заголовке, со своим собствен­ным адресом и направляет его модулю IP. После анализа полей IP-заголовка из пакета извлекаются данные, которые в свою очередь, содержат сообщение вышележащего протокола. Поскольку в данном примере рассматривается об­мен данными по протоколу FTP, который использует в качестве транспорт­ного протокола TCP, то в поле данных IP-пакета находится TCP-сегмент, определив из TCP-заголовка номерпорта, модуль IP переправляет сегмент в соответствующую очередь, из которой данный сегмент попадет программно­му модулю FTP-сервера.

 11Лекция 11.Протоколы маршрутизации и маршрутизаторы

  Цель лекции: рассмотреть протоколы маршрутизации.

 Протоколы маршрутизации предназначены для автоматического построения таблиц маршрутизации, на основе которых происходит продвижение пакетов сетевого уровня. Протоколы маршрутизации, в отличие от сетевых протоколов, таких как IP и IPX, не являются обязательными, так как таблица маршрутиза­ции может быть построена администратором сети вручную. Однако в крупных сетях со сложной топологией и большим количеством альтернативных маршру­тов протоколы маршрутизации выполняют очень важную и полезную работу, автоматизируя построение таблиц маршрутизации, динамически адаптируя те­кущий набор рабочих маршрутов к состоянию сети и повышая тем самым ее производительность и надежность.

 11.1 Классификация протоколов маршрутизации

*Назначение протоколов маршрутизации*

Продвижение пакетов в составных сетях осуществляется на основе таблиц мар­шрутизации. Общим в таблицах маршрутизации является то, что в них содержится информация, дос­таточная для принятия решения о продвижении любого поступающего в мар­шрутизатор пакета. Как правило, каждая запись такой таблицы связывает адрес сети назначения с адресом или номером выходного интерфейса, на который нужно передать пакет с этим адресом. Каждый маршрутизатор сети имеет собст­венную таблицу маршрутизации, определяющую один шаг многошагового про­цесса перемещения пакета по сети.

Нетрудно заметить, что задача продвижения пакета от сети источника до сети назначения в каждом маршрутизаторе естественно распадается на две задачи:

           -обработка пакета с помощью имеющейся таблицы маршрутизации;

 -построение таблицы маршрутизации.

Назначение протоколов маршрутизации состоит в автоматическом решении вто­рой задачи. Для этого маршрутизаторы сети обмениваются специальной служеб­ной информацией о топологии составной сети, на основе которой каждый мар­шрутизатор выбирает маршруты к узлам назначения. Создаваемые таблицы маршрутизации обеспечивают рациональность маршрутов следования пакетов через сеть, при этом критерии выбора маршрутов могут быть различными. Напомним, что обычно выбирается «кратчайший» маршрут, где под расстоянием, проходимым пакетом, понимается либо количество промежуточных маршрути­заторов (хопов), либо комплексный показатель, учитывающий также номиналь­ную пропускную способность каналов между маршрутизаторами, надежность каналов или вносимые ими задержки. Протокол маршрутизации должен созда­вать в маршрутизаторах согласованные друг с другом таблицы маршрутизации, то есть такие, которые обеспечат доставку пакета от исходной сети в сеть назна­чения за конечное число шагов. Современные протоколы маршрутизации обеспечивают со­гласованность таблиц, однако это их свойство не абсолютно – при изменениях в сети, например при отказе каналов связи или самих маршрутизаторов, сущест­вуют периоды нестабильной работы сети, вызванной временной несогласованно­стью таблиц разных маршрутизаторов. Протоколу маршрутизации обычно нуж­но некоторое время, чтобы после нескольких итераций обмена служебной информацией все маршрутизаторы сети внесли измерения в свои таблицы и в результате таблицы снова стали согласованными.

 11.1.1Маршрутизация без таблиц

Прежде чем перейти к классификации протоколов маршрутизации, необходимо отметить, что существуют такие способы продвижения пакетов в составных се­тях, которые вообще не требуют наличия таблиц маршрутизации в маршрутиза­торах, а значит, и протоколов маршрутизации.

Наиболее простым способом передачи пакетов по сети является так называемая *лавинная маршрутизация,* когда каждый маршрутизатор передает пакет всем своим непосредственным соседям, кроме того, от которого его получил. Понят­но, что это не самый рациональный способ, так как пропускная способность сети используется крайне расточительно, но он работоспособен (именно так мосты и коммутаторы локальных сетей поступают с кадрами, имеющими неизвестные ад­реса).

Другой вариант маршрутизации без таблицы — это *маршрутизация, управляемая событиями* (Event Dependent Routing), когда пакет к определенной сети на­значения посылается по маршруту, который уже приводил ранее к успеху (для данного адреса назначения). Это достаточно эффективный метод маршрутиза­ции, но он требует наличия обратной связи, чтобы маршрутизатор-отправитель мог фиксировать факт успеха доставки пакета.

Маршрутизация, управляемая событиями, может сочетаться с таблицей маршру­тизации. В такой таблице для каждой сети назначения указывается несколько возможных соседей, которым целесообразно направлять запрос на установление соединения (или тестирующий эхо-запрос). Подобный подход применяется в те­лефонных сетях, в которых указывается несколько возможных «направлений» передачи запроса на установление соединения, и эти запросы передаются снача­ла по первому из указанных направлений, пока не будет исчерпана его коммутационная емкость, затем по следующему и т. д.

Еще одним видом маршрутизации; не требующим наличия таблиц маршрутиза­ции, является *маршрутизация от источника (Source Routing).* В этом случае от­правитель помещает в пакет информацию о том, какие промежуточные маршру­тизаторы должны участвовать в передаче пакета к сети назначения. На основе этой информации каждый маршрутизатор считывает адрес следующего мар­шрутизатора и, если он действительно является адресом его непосредственного соседа, передает ему пакет для дальнейшей обработки. Вопрос о том, как отпра­витель узнает точный маршрут следования пакета через сеть, остается открытым. Маршрут может прокладывать либо администратор вручную, либо узел-отправитель автоматически, но в этом случае ему нужно поддерживать тот или иной протокол маршрутизации, который сообщит узлу о топологии и состоянии сети.

*Адаптивная маршрутизация*

В тех случаях, когда маршрутизация осуществляется на основании таблиц, раз­личают *статическую* и *адаптивную (динамическую)* маршрутизацию. В первом случае таблицы составляются и вводятся в память каждого маршрутизатора вручную администратором сети, все записи в таблице имеют статус «статиче­ских» (static), что подразумевает бесконечный срок их жизни. При изменении состояния какого-нибудь элемента сети администратору необходимо срочно вне­сти изменения в таблицы маршрутизации тех маршрутизаторов, для которых та­кое изменение требует смены маршрута (или маршрутов) следования пакетов – иначе сеть будет работать некорректно, и пакеты либо вообще перестанут дохо­дить до сети назначения, либо их маршрут окажется не рациональным. Таким образом, при статической маршрутизации протоколы маршрутизации оказываются невостребованными, так как всю их работу выполняет один или несколько администраторов.

Адаптивная маршрутизация обеспечивает автоматическое обновление таблиц маршрутизации после изменения конфигурации сети. Для адаптации таблиц как раз и нужны протоколы маршрутизации. Эти протоколы работают на основе ал­горитмов, позволяющих всем маршрутизаторам собирать информацию о топологии связей в сети, оперативно отрабатывая все изменения конфигурации связей. В таблицах маршрутизации при адаптивной маршрутизации обычно имеется информация об интервале времени, в течение которого данный маршрут будет ос­таваться действительным. Это время называют *временем жизни маршрута (Time То Live, TTL).* Если истечении времени жизни существование маршрута не подтверждается протоколом маршрутизации, то он считается нерабочим, пакеты по нему больше не посылаются.

Протоколы маршрутизации могут быть *распределенными* и *централизованными.* При распределенном подходе в сети отсутствуют какие-либо выделенные маршру­тизаторы, которые собирали бы и обобщали топологическую информацию: эта работа распределяется между всеми маршрутизаторами сети. Каждый маршру­тизатор строит свою собственную таблицу маршрутизации, основываясь на данных, получаемых по протоколу маршрутизации от остальных маршрутизаторов сети.

При централизованном подходе в сети существует один маршрутизатор, кото­рый собирает всю информацию о топологии и состоянии сети от других маршру­тизаторов. Затем этот выделенный маршрутизатор (который иногда называют сервером маршрутов) может выбрать несколько вариантов поведения. Он может построить таблицы маршрутизации для всех остальных маршрутизаторов сети, а затем распространить их по сети, чтобы каждый маршрутизатор получил соб­ственную таблицу и в дальнейшем самостоятельно принимал решение о продви­жении каждого пакета. Центральный маршрутизатор может также сообщить о выбранных маршрутах только конечным узлам (или пограничным маршрути­заторам), чтобы они направляли пакеты в сеть в соответствии с техникой мар­шрутизации от источника. В сети может быть не один, а несколько выделенных маршрутизаторов, каждый из которых обслуживает определенную группу под­чиненных ему маршрутизаторов.

Адаптивные протоколы обмена маршрутной информацией, применяемые в на­стоящее время в вычислительных сетях, в свою очередь, делятся на две группы, каждая из которых связана с одним из следующих типов алгоритмов:

     -дистанционно-векторные алгоритмы (Distance Vector Algorithms, DVA);

           -алгоритмы состояния связей (Link State Algorithms, LSA).

12Лекция 12 .Видеосвязь

         Цель лекции: рассмотреть вопросы развития видеосвязи

 Видеоконференции по каналам Интернет и ISDN

Расширение международных контактов и реализация проектов с "удаленными" отечественными партнерами делает актуальной проблему экономии командировочных расходов особенно в случае коротких поездок (1-7 дней). Одним из средств решения проблемы является использование видеоконференций. Видеоконференции по каналам Интернет могут быть привлекательны для дистанционного обучения и медицинской диагностики. В отличие от телевизионных программ обучение с использованием Интернет предполагает диалог между преподавателем и обучаемым, что делает процесс более эффективным (эта техника может успешно дополнить WWW-методику, широко используемую в университетах США и Европы). Медицинские приложения еще более многообещающи. Видеоконференции позволят проконсультироваться в клинике, отстоящей на тысячи километров, устроить консилиум с участием врачей из разных городов, оперативно передать томограмму или многоканальную кардиограмму пациента с целью ее интерпретации и т.д. В более отдаленной перспективе технология видеоконференций может быть применена для целей телевидения.

Для проведения видеоконференции необходимо иметь цифровой канал с пропускной способностью не менее 56-128 кбит/с. Если канал не позволяет, можно ограничиться аудиоконференцией. Помимо стандартного оборудования рабочей станции требуется интерфейс для подключения видеокамеры и микрофонов. Этот интерфейс обычно снабжается аппаратной схемой сжатия видео и аудио данных. Многие современные мультимедиа интерфейсы снабжены входами для видеокамеры. Полезным дополнением может служить сканер, который позволит с высоким разрешением передать изображения документов или чертежей, видеомагнитофон, а также видеопроектор для отображений принятого изображения на экране или телевизор с большим экраном.

Видеоконференции обеспечивают не только "живое" общение партнеров, но также оперативное обсуждение и редактирование чертежей и документов. При этом разрешающая способность может превышать в 10-100 раз ту, которая доступна для факсов.

Реализовать видеоконференцию можно разными путями, из них два наиболее реальны:

а) использование оборудования, каналов и программного обеспечения ISDN; полоса и качество здесь гарантируются, но стоимость весьма высока;

б) применение каналов Интернет, соответствующего (обычно общедоступного) программного обеспечения и оборудования общего применения; вариант относительно дешев, но качество здесь пока не гарантируется, ведь информационный поток при проведении сеанса конкурирует с потоками от других процессов в Интернет.

При видеоконференциях используется технология codec (coder/decoder) для выделенных и телефонных коммутируемых линий (>56 Кбит/с, интерфейс V35), применим и режим коммутации пакетов (multicast backbone, >256 Кбит/с).  Базовым протоколом для работы в локальных сетях является H.323. Этот стандарт обеспечивает видеоконференции для соединений точка-точка и для многоточечных топологий в рамках стека протоколов TCP/IP, он регламентирует также принципы сжатия видео и аудио информации. Привлекательность стандарта заключается в том, что он применим к уже существующей инфраструктуре телекоммуникаций с широкими вариациями задержек отклика. Способствует этому возрастающая пропускная способность локальных (fast ethernet и gigabit ethernet) и региональных сетей (SDH, ATM, FDDI, Fibre Channel и т.д.)

H.323 определяет четыре главных составляющих коммуникационной системы:

-  терминалы;

-  шлюзы;

-  блоки многоточечного управления;

-  системы управления доступом (gatekeepers).

Терминалы служат для предоставления пользователям определенных услуг и обеспечивают двухсторонний обмен данными в реальном масштабе времени. Все терминалы H.323 должны также поддерживать стандарт H.245, который служит для выбора параметров канала.

Интерфейс RAS (registration/admission/status) служит для взаимодействия с блоком доступа (gatekeeper) и поддерживает протоколы RTP/RTCP. Опционными частями H.323 являются видео кодеки, протоколы для проведения информационных конференций (T.120) и возможности поддержания многоточечной связи (mcu). Внешний шлюз также является опционным элементом конференций H.323. Шлюз может выполнять функции интерфейса для согласования с требованиями других форматов, например, H.225 – H.221 или других коммуникационных процедур, например, H.245 – H.242. Типичным шлюзом можно считать соединитель H.323 с коммутируемой телефонной сетью (GSTN). Данный шлюз устанавливает аналоговую связь с терминалами GSTN, с терминалами H.320 по каналам ISDN и с терминалами H.324 по сети GSTN. Терминалы взаимодействуют со шлюзом через протоколы H.245 и Q.931. Применяя соответствующую перекодировку, можно обеспечить работу шлюза H.323 с терминалами, поддерживающими протоколы V.70, H.322, H.310 и H.321. Многие функции шлюза не стандартизованы, к их числу, например, относится нумерация подключенных терминалов.

Узел управления доступом (gatekeeper) является центральным блоком сети H.323. Через него проходят все запросы обслуживания, при этом он выполняет функцию виртуального переключателя. Узел управления доступом осуществляет преобразование имен терминалов и шлюзов в их IP и IPX-адреса в соответствии со спецификацией RAS. Например, если администратор сети установил верхний предел на число участников конференции, при достижении этого порога узел управления доступом может отказать в установлении соединения. К числу обязательных функций узла управления доступом относится:

-  преобразование адресов (например, из стандарта E.164 в транспортный формат);

-  осуществление контроля доступа к локальной сети с использованием сообщений Admission Request, Confirm и Reject (возможен режим разрешения доступа для всех запросов) ;

-  управление полосой пропускания (поддержка сообщений Bandwidth Request, Confirm и Reject) ;

-  управление зоной и реализация всех вышеперечисленных функций для MCU, шлюза и терминалов, зарегистрированных в зоне.

Для организации конференций с числом участников три и более используется блок многоточечного доступа (MCU). MCU включает в себя многоточечный контроллер (MC) и многоточечный процессор (MP). MC осуществляет согласование рабочих параметров терминалов для обеспечения совместимости при передаче видео и аудио информации в рамках протокола H.245. Все терминалы посылают аудио, видео и данные MCU в режиме соединения точка-точка. Управляющая канальная информация H.245 передается непосредственно в MC. MP может выполнять перекодировку в случае использования кодеков различного типа. Конференция может быть организована в централизованном (все обмены идут через MCU) и децентрализованном режиме, когда терминалы непосредственно взаимодействуют друг с другом. Терминалы используют протокол H.245, для того ,чтобы сообщить MC, сколько видео- и аудио- потоков они могут обработать одновременно. MP может осуществлять отбор видеосигналов и смешение аудио-каналов при децентрализованной многоточечной конференции. Допускается и смешенный режим, когда одновременно реализуется централизованная и децентрализованная схема обменов.

Звуковой сигнал передается в оцифрованной и сжатой форме. Алгоритмы компрессии, поддерживаемые H.323, соответствуют требованиям стандартов ITU. Терминалы H.323 должны быть способны работать со стандартом компрессии голоса G.711 (56 или 64 Кбит/c). Голосовой кодек должен следовать рекомендациям G.723, а видео кодек должен соответствовать стандарту H.261 (поддержка H.263 является опционной, этот стандарт обеспечивает более высокое качество изображения). В таблице 1 приведены форматы для видео-конференций стандартов ITU.

Пакетная техника обеспечивает удовлетворительное качество изображения и звукового сопровождения при низкой загрузке канала и малой вероятности ошибок при передаче пакетов. Достижимое сжатие видеосигнала - 1000:1, звукового 8:1.

Для экспериментов с передачей звука и изображения группой IETF (Internet Engineering Task Force) была сформирована структура мультикастинг-сети MBONE. MBONE (Multicast Backbone, до 300 Кбит/с) представляет собой виртуальную сеть, построенную из уникаст-туннелей, которые функционируют поверх Интернет. MBONE составляет около 3,5% от всего Интернет. Рабочие станции для доступа к MBONE должны поддерживать IP-мультикастинг. Следует иметь в виду, что не все маршрутизаторы поддерживают мультикастинг.

При работе с MBONE отправитель не должен знать, кто является получателем, а требуемая пропускная способность канала не зависит от того, обслуживается один клиент или 100.

Требуемая полоса канала для видеоконференций определяется необходимой разрешающей способностью и частотой кадров. Требования к каналу для передачи изображения представлены в таблице 3.

Т а б л и ц а 2

|  |  |
| --- | --- |
| Частотакадров/с | Размер экрана (24 цветовых бит) |
| 1280\*1024 | 640\*480 | 320\*240 | 160\*120 |
| 30 | 900 Мбит/с | 211 Мбит/с | 53 Мбит/с | 13 Мбит/с |

 В таблице 3 приведены требования на пропускную способность канала при использовании различных степеней сжатия передаваемых видеоданных для частоты кадров 30/с и 24 бит на пиксель для отображения цвета.

Т а б л и ц а 3

|  |  |
| --- | --- |
| Степень сжатия данных | Размер экрана |
|   | 1280\*1024 | 640\*480 | 320\*240 | 160\*120  |
| 100:1 | 9 Мбит/с | 2.11 Мбит/с | 0.53 Мбит/с | 0.13 Мбит/с |
| 50:1 | 18 | 4,22 | 1,06 | 0,26 |
| 25:1 | 36 | 8,44 | 2,12 | 0.52 |
| 12:1 | 75 | 17,58 | 4,4 | 1,08 |
| 6:1 | 150 | 35,17 | 8,8 | 2,16 |

 Требования при передаче звука определяются необходимым качеством, так для получения полосы 6 Кгц нужно 64 Кбит/с, а для уровня, сопоставимого с CD - 1,4 Мбит/с. Применение сжатия информации позволяет снизить эти требования в 4-8 раз. Общепринятыми стандартами для сжатия изображения при видеоконференциях являются JPEG, MPEG, H.261. Обычно они реализуются программно, но есть и аппаратные реализации.

Если сегодня базовым транспортным протоколом для мультимедиа является UDP, то в самое ближайшее время его потеснит RTR и дополнят RSVP и ST-II, что заметно повысит качество и надежность.

  13 Лекция 13 Цифровое представление телевизионного сигнала

**Цель лекции : ознакомить студентов с цифровым представлением телевизионного сигнала.**

Цифровая техника стала постепенно проникать в телевидение в семидесятые годы прошлого века. Первыми появились цифровые корректоры временных искажений, затем - кадровые синхронизаторы, генераторы специальных эффектов, микшеры, коммутаторы. Но говорить о возможности полномасштабного перехода к цифровому телевидению стали двадцать лет назад, когда появился первый промышленный цифровой видеомагнитофон, разработанный фирмой Sony. Это - выдающееся событие для телевидения. Прежде всего, надо отметить, что параметры, характеризующие качество воспроизводимого изображения и звука в цифровом аппарате, превосходили те значения, которые были типичными для аналоговых магнитофонов. Но появление цифровой видеозаписи означало не просто значительное улучшение параметров. Эффект накопления искажений, присущий всем аналоговым системам, например, ограничивает предельно допустимое число перезаписей, которые могут быть сделаны на аналоговом магнитофоне. А вот цифровые системы свободны от эффекта накопления искажений.

Но цифровая техника порождает и проблемы. Полоса частот цифровых сигналов значительно шире полосы их аналоговых "предшественников". Например, полоса частот, занимаемая телевизионным видеосигналом в цифровой форме, составляет сотни мегагерц. Так, при передаче полного телевизионного сигнала в цифровой форме требуются каналы связи с пропускной способностью до сотен мегабит в секунду. Использование каналов, не вносящих ошибки в цифровой поток и обладающих столь большой пропускной способностью, может оказаться невозможным или экономически невыгодным.

Принципиальный способ решения проблем передачи и записи с высокой степенью помехозащищенности был обоснован Шенноном. Он заключается в кодировании сигнала. К системам кодирования в цифровой видеотехнике предъявляются весьма многочисленные и часто противоречивые требования. Поэтому на практике кодирование всегда выполняется в несколько приемов. Сейчас принято выделять следующие основные виды:

-  кодирования источника информации с целью преобразования сигнала в цифровую форму и его экономное представление путем сжатия или, как часто говорят, компрессии;

-  кодирования с целью обнаружения и исправления ошибок;

-  канального кодирования с целью согласования параметров цифрового сигнала со свойствами канала связи и обеспечения самосинхронизации.

Для преобразования любого аналогового сигнала (звука, изображения) в цифровую форму необходимо выполнить три основные операции: дискретизацию, квантование и кодирование. Дискретизация - представление непрерывного аналогового сигнала последовательностью его значений (отсчетов). Эти отсчеты берутся в моменты времени, отделенные друг от друга интервалом, который называется интервалом дискретизации. Величину, обратную интервалу между отсчетами, называют частотой дискретизации. На рисунке 23 показаны исходный аналоговый сигнал и его дискретизированная версия. Изображения, приведенные под временными диаграммами, получены в предположении, что сигналы являются телевизионными видеосигналами одной строки, одинаковыми для всего телевизионного растра.



Рисунок 23 – Аналого-цифровое преобразование. Дискретизация

 Чем меньше интервал дискретизации и, соответственно, выше частота дискретизации, тем меньше различия между исходным сигналом и его дискретизированной копией. Ступенчатая структура дискретизированного сигнала может быть сглажена с помощью фильтра нижних частот.

Таким образом и осуществляется восстановление аналогового сигнала из дискретизированного. Но восстановление будет точным только в том случае, если частота дискретизации по крайней мере в 2 раза превышает ширину полосы частот исходного аналогового сигнала (это условие определяется известной теоремой Котельникова). Если это условие не выполняется, то дискретизация сопровождается необратимыми искажениями.

Дело в том, что в результате дискретизации в частотном спектре сигнала появляются дополнительные компоненты, располагающиеся вокруг гармоник частоты дискретизации в диапазоне, равном удвоенной ширине спектра исходного аналогового сигнала. Если максимальная частота в частотном спектре аналогового сигнала превышает половину частоты дискретизации, то дополнительные компоненты попадают в полосу частот исходного аналогового сигнала. В этом случае уже нельзя восстановить исходный сигнал без искажений.

Пример искажений дискретизации приведен на рисунке 24.



Рисунок 24 – Искажение дискретизации

Аналоговый сигнал (предположим опять, что это видеосигнал ТВ строки) содержит волну, частота которой сначала увеличивается от 0,5 МГц до 2,5 МГц, а затем уменьшается до 0,5 МГц. Этот сигнал дискретизируется с частотой 3 МГц. На рисунке 30 последовательно приведены изображения: исходный аналоговый сигнал, дискретизированный сигнал, восстановленный после дискретизации аналоговый сигнал. Восстанавливающий фильтр нижних частот имеет полосу пропускания 1,2 МГц. Как видно, низкочастотные компоненты (меньше 1 МГц) восстанавливаются без искажений. Волна с частотой 1,5 МГц исчезает и превращается в относительно ровное поле. Волна с частотой 2,5 МГц после восстановления превратилась в волну с частотой 0,5 МГц (это разность между частотой дискретизации 3 МГц и частотой исходного сигнала 2,5 МГц).

Эти диаграммы иллюстрируют искажения, связанные с недостаточно высокой частотой пространственной дискретизации изображения. Если объект телевизионной съемки представляет собой очень быстро движущийся или, например, вращающийся предмет, то могут возникать и искажения дискретизации во временной области. Примером искажений, связанных с недостаточно высокой частотой временной дискретизации (а это частота кадров телевизионного разложения), является картина быстро движущегося автомобиля с неподвижными или, например, медленно вращающимися в ту или иную сторону спицами колеса (стробоскопический эффект).

Если частота дискретизации установлена, то искажения дискретизации отсутствуют, когда полоса частот исходного сигнала ограничена сверху и не превышает половины частоты дискретизации. Если потребовать, чтобы в процессе дискретизации не возникало искажений ТВ сигнала с граничной частотой, например, 6 МГц, то частота дискретизации должна быть не меньше 12 Мгц. Однако, чем ближе частота дискретизации к удвоенной граничной частоте сигнала, тем труднее создать фильтр нижних частот, который используется при восстановлении, а также при предварительной фильтрации исходного аналогового сигнала. Это объясняется тем, что при приближении частоты дискретизации к удвоенной граничной частоте дискретизируемого сигнала предъявляются все более жесткие требования к форме частотных характеристик восстанавливающих фильтров - она все точнее должна соответствовать прямоугольной характеристике.

Следует подчеркнуть, что фильтр с прямоугольной характеристикой не может быть реализован физически. Такой фильтр, как показывает теория, должен вносить бесконечно большую задержку в пропускаемый сигнал. Поэтому на практике всегда существует некоторый интервал между удвоенной граничной частотой исходного сигнала и частотой дискретизации.

Квантование представляет собой замену величины отсчета сигнала ближайшим значением из набора фиксированных величин - уровней квантования. Другими словами, квантование - это округление величины отсчета. Уровни квантования делят весь диапазон возможного изменения значений сигнала на конечное число интервалов - шагов квантования. Расположение уровней квантования обусловлено шкалой квантования. Используются как равномерные, так и неравномерные шкалы. На рисунке 31 показаны исходный аналоговый сигнал и его квантованная версия, полученная с использованием равномерной шкалы квантования, а также соответствующие сигналам изображения.

Искажения сигнала, возникающие в процессе квантования, называют шумом квантования. При инструментальной оценке шума квантования вычисляют разность между исходным сигналом и его квантованной копией, а в качестве объективных показателей шума принимают, например, среднеквадратичное значение этой разности. В отличие от флуктуационных шумов, шум квантования коррелирован с сигналом, поэтому шум квантования не может быть устранен последующей фильтрацией. Шум квантования убывает с увеличением числа уровней квантования.



Рисунок 25– Квантование

Еще несколько лет назад вполне достаточным казалось использовать 256 уровней для квантования телевизионного видеосигнала. Сейчас считается нормой квантовать видеосигнал на 1024 уровня. Число уровней квантования при формировании цифрового звукового сигнала намного больше: от десятков тысяч до миллионов.

Квантованный сигнал, в отличие от исходного аналогового, может принимать только конечное число значений. Это позволяет представить его в пределах каждого интервала дискретизации числом, равным порядковому номеру уровня квантования. В свою очередь это число можно выразить комбинацией некоторых знаков или символов. Совокупность знаков (символов) и система правил, при помощи которых данные представляются в виде набора символов, называют кодом. Конечная последовательность кодовых символов называется кодовым словом. Квантованный сигнал можно преобразовать в последовательность кодовых слов. Эта операция и называется кодированием. Каждое кодовое слово передается в пределах одного интервала дискретизации. Для кодирования сигналов звука и изображения широко применяют двоичный код. Если квантованный сигнал может принимать N значений, то число двоичных символов в каждом кодовом слове n ≥ log2N. Один разряд, или символ слова, представленного в двоичном коде, называют битом. Обычно число уровней квантования равно целой степени числа 2, т.е. N = 2n.

Кодовые слова можно передавать в параллельной или последовательной формах (см. рисунок 26). Для передачи в параллельной форме надо использовать n линий связи (в примере, показанном на рисунке 32, n = 4).



Рисунок 26 – Цифровое кодирование

Символы кодового слова одновременно передаются по линиям в пределах интервала дискретизации. Для передачи в последовательной форме интервал дискретизации надо разделить на n подинтервалов - тактов. В этом случае символы слова передаются последовательно по одной линии, причем на передачу одного символа слова отводится один такт.

Каждый символ слова передается с помощью одного или нескольких дискретных сигналов - импульсов. Преобразование аналогового сигнала в последовательность кодовых слов называют импульсно-кодовой модуляцией. Форма представления слов определенными сигналами определяется форматом кода. В параллельном цифровом потоке по каждой линии в пределах интервала дискретизации передается 1 бит 4-разрядного слова. В последовательном потоке интервал дискретизации делится на 4 такта, в которых передаются (начиная со старшего) биты 4-разрядного слова.

Операции, связанные с преобразованием аналогового сигнала в цифровую форму (дискретизация, квантование и кодирование), выполняются одним устройством - аналого-цифровым преобразователем (АЦП). Сейчас АЦП может быть просто интегральной микросхемой. Обратная процедура, т.е. восстановление аналогового сигнала из последовательности кодовых слов, производится в цифро-аналоговом преобразователе (ЦАП). Сейчас существуют технические возможности для реализации всех обработок сигналов звука и изображения, включая запись и излучение в эфир, в цифровой форме. Однако в качестве датчиков сигнала (например, микрофон, передающая ТВ трубка или прибор с зарядовой связью) и устройств воспроизведения звука и изображения (например, громкоговоритель, кинескоп) пока используются аналоговые устройства. Поэтому аналого-цифровые и цифро-аналоговые преобразователи являются неотъемлемой частью цифровых систем.

Цифровые сигналы можно описывать с помощью параметров, типичных для аналоговой техники, например таких, как полоса частот. Но их применимость в цифровой технике является ограниченной. Важным показателем, характеризующим цифровой поток, является скорость передачи данных. Если длина слова равна n, а частота дискретизации FD, то скорость передачи данных, выраженная в числе двоичных символов в единицу времени (бит/с), находится как произведение длины слова на частоту дискретизации:

C = nFD.

Список используемой литературы

1. Кузнецов А.Е., Пинчук А. В., Суховицкий А.Л. Построение сетей IP-телефонии / Компьютерная телефония.- 2000.- №6.

2. Кульгин М. Технологии корпоративных сетей: Изд. «Питер», 1999.

3. Будников В.Ю., Пономарев Б.А. Технологии обеспечения качества обслуживания в мультисервисных сетях / Вестник связи.-, 2000.- №9.

4. Варакин Л. Телекоммуникационный феномен России / Вестник связи International.- 1999.-№4.

5. Варламова Е. IP-телефония в России / Connect! Мир связи.-1999.- №9.

6. Гольдштейн Б.С. Сигнализация в сетях связи. –т. 1.- М.: Радио

и связь, 1998.

7. Гольдштейн Б.С. Протоколы сети доступа. –т. 2.- М.: Радио и связь, 1999.

8. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети.- М.: Радио и связь, 2000.

11. Ломакин Д. Технические решения IP-телефонии / Мобильные системы.-1999.- №8.

12. Мюнх Б., Скворцова С. Сигнализация в сетях IP-телефонии. -ч I, 2/Сети и системы связи.- 1999. - №13(47), 14(48).

13. Уиллис Д. Интеграция речи и данных. В начале долгого пути./Сети и системы связи, 1999.-№16.

14. Шнепс-Шнеппе М.А. Интеллектуальные услуги - это ДВО / Информ - курьер-связь.-2000 - №9.

15. Armitage Grenville. Quality of Service in IP Networks. - Macmillan Technical Publishing, 2000.

16. Anquetil L-P., Bouwen J., Conte A., Van Doorselaer. B. Media Gateway Control Protocol and Voice over IP Gateway. - Alcatel Telecommunications Review, 2nd Quarter 1999.

17. Caputo R. Cisco Packetized Voice and Data Integration. - McGraw-Hill Cisco Technical Expert, 2004.

18. Curtin P., Whyte B. Tigris - A gateway between circuit-switched and IP networks / Ericson Rewiew.- 1999.- №2.

19. DavidsonJ., Peters J. Voice Over IP Fundamentals. - Cisco Press, 2000.