КАЗАНСКИЙ ГОСУДАРСТВЕНЫЙ УНИВЕРСИТЕТ

Ю.А. Гусев

Телекоммуникационные сети

IP-телефония

Часть 2

Учебное пособие

КАЗАНЬ – 2003

Казанский государственный университет

Ю.А.Гусев

Телекоммуникационные сети

IP-телефония

Часть 2

Учебное пособие

Казань - 2003

Печатается по решению редакционно-издательского совета физического факультета Казанского государственного университета.

УДК 538.213

Рецензенты:

Силкин Н.И., к.ф.-м.н., доцент кафедры квантовой электроники и радиоспектроскопии Казанского государственного университета

Димитров Д.М/, профессор, д.т.н. Действительный член РАН, информатика и связь.

Анотация.

В работе представлены Концептуальные основы технологии передачи речи по сетям пакетной документации, работающим по протоколу IP (Internet Protocol). Рассмотрены архитектуры систем IP-телефонии на базе рекомендаций ITU-T H.323 и концепции TIPHON, разработанной ETSI. Описаны вопросы сигнализации, адресации, обеспечения качества в сетях IP-телефонии. Дан анализ принципов построения IP-телефонии, описана практика внедрения услуг пакетной передачи, приведен обзор оборудования для построения сетей IP-телефонии.

Данная работа поддержана грантом BRHE, REC. 007.

Физический факультет Казанского государственного университета, 2003.

Содержание

Предисловие

Интернет-телефония — это технология передачи телефонных речевых сообщений по сети Интернет. Работа устройств в сети Интернет осуществляется с использованием специального Интернет-протокола (Internet Protocol - IP). В настоящее время протокол IP используется не только в сети Интернет, но и в других сетях передачи данных с пакетной коммутацией (локальных, корпоративных, региональных и др.). И во всех этих сетях, в принципе, имеется возможность передавать речевые сообщения с использованием пакетов данных. Такой способ передачи речи и получил название IP-телефония (произносится «Айпи-телефония»). За рубежом обычно употребляется аббревиатура VoIP - Voice over IP, хотя часто используют более узкий термин «Интернет-телефония».

Интерес различных субъектов рынка телекоммуникационных услуг (операторов связи, провайдеров Интернет, производителей оборудования и пользователей) к данному виду связи необычайно возрос в последние годы в связи с разработкой новых стандартов и протоколов, когда IP-телефонный разговор вплотную приблизился по качеству к телефонному разговору по «классическим» телефонным сетям. Этот интерес объясняется тем, что IP-телефония позволяет существенно экономить требуемую полосу пропускания каналов, что неизбежно ведет к снижению тарифов, особенно на междугородные и международные телефонные разговоры. Однако не все так гладко на пути внедрения новой технологии: имеются проблемы с обеспечением сквозного качества телефонной связи, затруднена совместная работа оборудования различных производителей, требуется новое, достаточно дорогое аппаратное и программное обеспечение и др.

IP-телефония - не панацея для решения всех телекоммуникационных проблем. Но в то же время ее использование позволяет предлагать пользователям совершенно новые, невозможные для традиционной телефонии сервисы и приложения. Да и сам фактор экономии затрат на телефонную связь играет не последнюю роль даже с учетом более низкого, но приемлемого, качества передачи разговора. Все это говорит о том, что технология IP-телефонии, по большому счету, выгодна всем: и пользователям, и операторам сетей, и производителям оборудования.

За последние годы редкий номер отечественных телекоммуникационных журналов обходится без статьи, затрагивающих технологию IP телефонии.

В данном учебном пособии нет претензий на абсолютную полноту и глубину представленного материала по IP-телефонии. Но описание основных принципов, основ IP-телефонии (архитектура системы, вопросы стандартизации, сигнализации, обеспечения качества), на мой взгляд будут полезны студентам и аспирантам работающим в данной области телекоммуникаций.

Автор благодарен рецензенту Димитрову Д.М, за ценные замечания и Гафаровой Л.И. за труд и внимание проявленные при подготовке рукописи к печати.

Глава 1

ОБЩИЕ ПРИНЦИПЫ IP-ТЕЛЕФОНИИ

1.1. Сеть Интернет и протокол IP

О технологии и сети Интернет и используемом в ней протоколе IP (Intrnet Protocol] имеется огромное количество информации, как в самом Интернете, так и в печатных изданиях, и желающие могут без труда ее найти. Далее приведены лишь основные концептуальные положения, которые необходимы для понимания возможностей применения сети Интернет и IP-протокола для передачи речевых сообщений.

Точное определение термина «Интернет» было дано в октябре 1995 г. федеральным Сетевым Советом США в следующей форме:

«Интернет - это часть глобальной информационной системы, которая:

- логически связана унитарным адресным пространством, основанном на IP-протоколе или на его перспективных расширениях/последователях;
- может поддерживать коммуникации, используя Transmission Control Protocol (TCP/IP) или его расширения/последователи и/или IP-совместимые протоколы;
- предоставляет, использует или делает доступными (для всех или конфиденциально) сервисы высокого уровня, основанные на коммуникациях и связанной с ними инфраструктуре, здесь определенной».

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 подсоединенные к ней компьютеры используют ту или иную технологию (Ethernet, Token Ring, FDDI, ISDN, соединение типа «точка-точка», а в последнее время к этому списку добавились сеть ATM 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 одноименная 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 (routers) - компьютеры, 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 определенной топологии межсетевых соединений. Добавление новой сети к сети Интернет не влечет за собой ее 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, передает пакет по тому или иному маршруту. В сети Интернет используются универсальные идентификаторы подсоединенных к ней компьютеров (адреса), поэтому любые две машины имеют возможность взаимодействовать друг с другом. В Интернет также должен быть реализован принцип независимости пользовательского интерфейса от

физической сети, то есть должно существовать множество способов установления соединений и передачи данных, одинаковых для всех физических сетевых технологий.

Сеть Интернет скрывает детали соединений сетей между собой, поэтому с точки зрения конечных пользователей и по отношению к прикладным программам сеть Интернет представляет собой **единую виртуальную сеть**, к которой подсоединены все компьютеры -независимо от их реальных физических соединений (рис. 1.1). Каждый компьютер должен иметь программное обеспечение доступа к сети Интернет, которое позволяет прикладным программам использовать сеть Интернет как одну физическую сеть

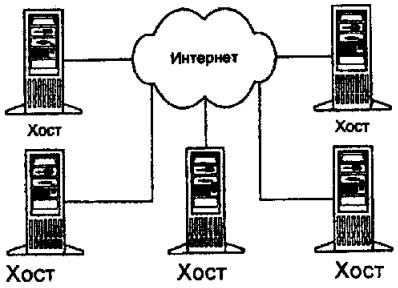

Рис. 1.1. Сеть Интернет с точки зрения пользователя

Фундаментальным принципом Интернет является равнозначность всех объединенных с ее помощью физических сетей: любая система коммуникаций рассматривается как компонент Интернет, независимо от ее физических параметров, размеров передаваемых пакетов данных и географического масштаба. На рис. 1.2 использованы одинаковые обозначения для любых физических сетей, объединенных в сеть Интернет (например, соединений типа «точка-точка», локальных сетей рабочей группы или больших корпоративных сетей).

Универсальная сеть Интернет строится на основе семейства протоколов TCP/IP и включает в себя протоколы 4-х уровней коммуникаций (рис. 1.3).

Уровень сетевого интерфейса отвечает за установление сетевого соединения в конкретной физической сети – компоненте сети Интернет, к которой подсоединен компьютор. 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 подключен компьютер-адресат. Протокол IP определяет маршрут отдельно для каждого пакета данных, не гарантируя надежной доставки в нужном порядке. Он задает непосредственное отображение данных на нижележащий физический уровень передачи и реализует тем самым высокоэффективную доставку пакетов.

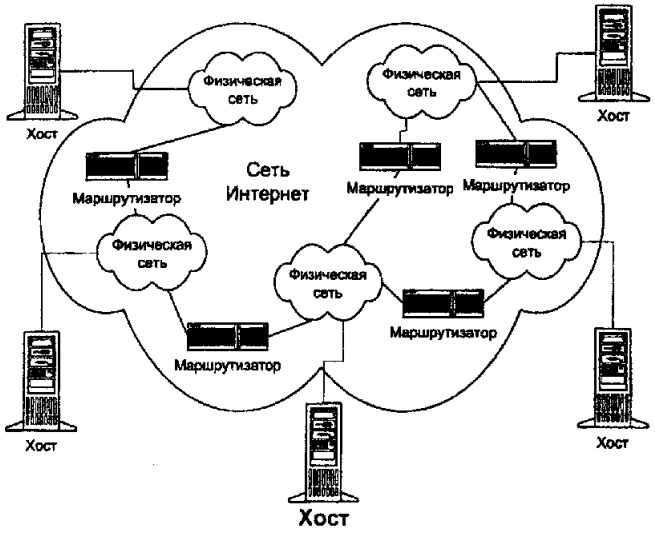

Рис. 1.2. Внутренняя структура сети Интернет

Прикладной:	Telnet, FTP, E-mail и т.д.
Транспортный:	TCP, VDP
Сетевой:	IP, ICMP, IGMP
Сетевой интерфейс:	драйвер устройства и сетевая плата

Рис. 1.3. Четыре уровня стека протоколов TCP/IP

На сетевом уровне протокол IP реализует ненадежную службу доставки пакетов по сети от системы к системе без установления соединения (connectionless packet delivery service). Это означает, что будет выполнено все 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 надежности коммуникации. Не имеется механизма подтверждений ни между отправителем и получателем, ни между хост-компьютерами. Не имеется контроля ошибок для поля данных, только контрольная сумма для заголовка. Не поддерживается повторная передача, нет управления потоком. Обнаруженные ошибки могут быть оглашены посредством протокола ICMP (Internet Control Message Protocol).

Надежную передачу данных реализует следующий уровень, транспортный, на котором два основных протокола, TCP и UDP, осуществляют связь между машиной - отправителем пакетов и машиной-адресатом.

Наконец, прикладной уровень - это приложения типа клиент-сервер, базирующиеся на протоколах нижних уровней. В отличие от протоколов остальных трех 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 др.

Поскольку в Интернет детали физических соединений скрыты от приложений, прикладной уровень совершенно «не заботится» о том, что клиент приложения работает в сети Ethernet, а сервер подключен к сети Token Ring. 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.

На базе протокола IP строится не только сеть Интернет, но и любые другие сети передачи данных (локальные, корпоративные), которые могут иметь или не иметь выход на глобальную сеть Интернет. Универсальность и гибкость сетей на базе протокола IP дает возможность применять их не только для передачи данных, но и другой мультимедийной информации. С недавних пор IP-сети стали использовать для передачи речевых сообщений. А вот как это происходит и будет рассмотрено в данной книге.

1.2. Терминология

В технической литературе используются три основных термина для обозначения технологии передачи речи по сетям с пакетной коммутацией на базе протокола IP (Internet Protocol):

- IP-телефония (IP Telephony);
- голос по IP-сетям (Voice over IP - VoIP);
- Интернет-телефония (Internet Telephony).

Хотя терминология в области IP-телефонии не устоялась окончательно, попробуем все-таки внести некоторую ясность хотя бы в рамках данной книги.

Под **IP-телефонией** будем понимать технологию, позволяющую использовать любую сеть с пакетной коммутацией на базе протокола IP (например, сеть Интернет) в качестве средства организации и ведения международных, междугородных и местных телефонных разговоров и передачи факсов в режиме реального времени.

За рубежом технология передачи голосовой информации с использованием протокола IP имеет устоявшееся название **Voice over IP (VoIP).** В отношении сервисов и технологий между IP-телефонией и VoIP нет никакой разницы. Различные производители могут предпочитать один или другой термин либо использовать их в равной степени. С точки же зрения сетевых решений «IP-телефония», безусловно, - термин более содержательный, так как она реализуется не только на уровне каналов передачи (как глобальных, так и локальных), но и на уровне абонентского оборудования и, что немаловажно, учрежденческих автоматических телефонных станций (УАТС). Последнее действительно означает фактическую интеграцию телефонии в ее привычном понимании и IP-сетей.

Интернет-телефония - это частный случай IP-телефонии, когда в качестве каналов передачи пакетов телефонного графика либо от абонента к оператору, либо на магистрали (либо на обоих названных участках) используются обычные каналы сети Интернет.

Спор о терминах в области IP-телефонии до сих пор не решен на международном уровне. Так организаторы семинара Международного союза электросвязи (ITU), посвященного IP-телефонии (Женева, 14-16 июня 2000 г.), выступили с предложением считать IP-телефонию общим понятием, включающим Интернет-телефонию и VoIP.

Участникам семинара было предложено для обсуждения следующее различие технологий:

- *Интернет-телефония* - передача телефонных сообщений в сетях передачи данных общего пользования, т. е. в мало или неадминистрируемых сетях.
- *VoIP* — передача телефонных сообщений в корпоративных, т.е. в хорошо

администрируемых сетях.

В процессе обсуждения документа выяснилось, что подходы стран-участниц ITU к тому, что есть IP-телефония и как с ней следует поступать, совершенно различны. Существуют два противоположных взгляда на IP-телефонию:

- IP-телефония - явление аналогичное обратному вызову (call-back) и маршрутизации по наименьшей стоимости. В этом смысле она представляет угрозу для операторов традиционной телефонии, так как использует их сетевые ресурсы в обход системы международных расчетов и, следовательно, ее нужно запретить любой ценой;
- IP-телефония - это будущее сети общего пользования и, следовательно, ее нужно всемерно поддерживать и развивать.

Но даже при втором подходе возникли противоречия в определениях: IP-телефония - эта услуга реального или нереального времени? В некоторых странах для разделения услуг телефонной сети общего пользования (ТфОП) и IP-телефонии используются понятия: задержка и качество обслуживания. И отсюда возможны два подхода к определению IP-телефонии:

- IP-телефония - это самостоятельная услуга по передаче голоса, представляющая собой более дешевую альтернативу традиционной телефонии;
- IP-телефония - наиболее простая для реализации услуга из пакета услуг, включая передачу данных и видео по протоколу IP. Более того, передача голоса - не самая значительная составляющая этого пакета услуг. IP-телефония будет способствовать повсеместному распространению электронной торговли и добавлять в интерактивные сетевые игры или chat элемент живого общения.

В итоге участники семинара пришли к выводу, что право на жизнь имеет целый ряд терминов и определений, особенно, принимая во внимание быстрое развитие данной технологии.

1.3. Принципы пакетной передачи речи

«Классические» телефонные сети основаны на технологии коммутации каналов (рис.1.4), которая для каждого телефонного разговора требует выделенного физического соединения. Следовательно, один телефонный разговор представляет собой одно физическое соединение телефонных каналов. В этом случае аналоговый сигнал шириной 3,1 кГц передается на ближайшую АТС, где он мультиплексируется по технологии временного разделения с сигналами, которые поступают от других абонентов, подключенных к этой АТС. Далее групповой сигнал передается 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 несет никакой полезной нагрузки.

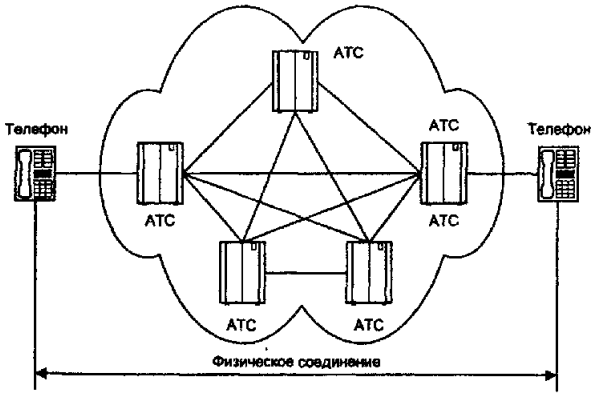

Рис. 1.4. Соединение в «классической» телефонной сети

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 (рис. 1.5), 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 (т.е. об источнике или отправителе) и пункте назначения (о получателе или приемнике).

В сетях на основе протокола IP все данные - голос, текст, видео, компьютерные программы или информация в любой другой форме - передаются в виде пакетов. Любой компьютер и терминал такой сети имеет свой уникальный IP-адрес, и передаваемые пакеты маршрутизируются к получателю в соответствии с этим адресом, указываемом в заголовке. Данные могут передаваться одновременно между многими пользователями и процессами по одной и той же линии. При возникновении проблем IP-сети могут изменять маршрут для обхода неисправных участков. При этом протокол IP не требует выделенного канала для сигнализации. **Процесс передачи голоса по IP-сети состоит из нескольких этапов.** На первом этапе осуществляется оцифровка голоса. Затем оцифрованные данные анализируются и обрабатываются с целью уменьшения физического объема данных, передаваемых получателю. Как правило, на этом этапе происходит подавление ненужных пауз и фонового шума, а также компрессирование.

На следующем этапе полученная последовательность данных разбивается на пакеты и к ней добавляется протокольная информация - адрес получателя, порядковый номер пакета на случай, если они будут доставлены не последовательно, и дополнительные данные для коррекции ошибок. При этом происходит временное накопление необходимого количества данных для образования пакета до его непосредственной отправки в сеть.

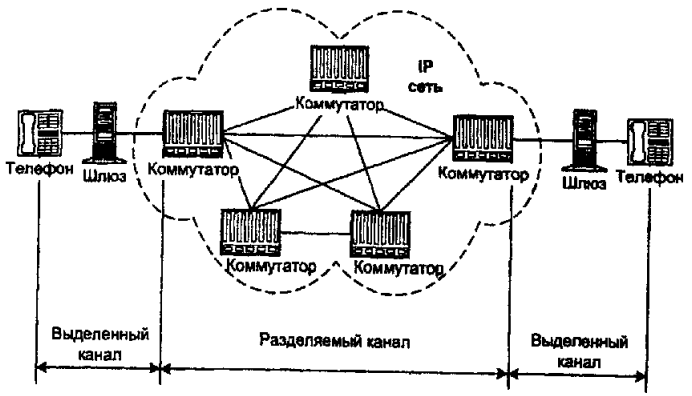

Рис. 1.5. **Соединение в сети с коммутацией пакетов**

Извлечение переданной голосовой информации из полученных пакетов также происходит в несколько этапов. Когда голосовые пакеты приходят на терминал получателя, то сначала проверяется их порядковая последовательность. Поскольку IP-сети не гарантируют время доставки, то пакеты со старшими порядковыми номерами могут прийти раньше, более того, интервал времени получения также может колебаться. Для восстановления исходной последовательности и синхронизации происходит временное накопление пакетов. Однако некоторые пакеты могут быть вообще потеряны при доставке, либо задержка их доставки превышает допустимый разброс. В обычных условиях приемный терминал запрашивает повторную передачу ошибочных или потерянных данных. Но передача голоса слишком критична ко времени доставки, поэтому в этом случае либо включается алгоритм аппроксимации, позволяющий на основе полученных пакетов приблизительно восстановить потерянные, либо эти потери просто игнорируются, а пропуски заполняются данными случайным образом.

Полученная таким образом (не восстановленная!) последовательность данных декомпенсируется и преобразуется непосредственно в аудио-сигнал, несущий голосовую информацию получателю.

Таким образом, с большой степенью вероятности, полученная информация не соответствует исходной (искажена) и задержана (обработка на передающей и приемной сторонах требует промежуточного накопления). Однако в некоторых пределах избыточность голосовой информации позволяет мириться с такими потерями.

Операторы сетей с пакетной коммутацией получают преимущества, присущие разделяемой инфраструктуре электросвязи по самой её природе. Проще говоря, они могут продать больше, чем в действительности имеют, основываясь на статистическом анализе работы сети. Поскольку предполагается, что абоненты не будут круглосуточно и ежедневно задействовать всю оплаченную полосу, можно обслужить больше абонентов, не расширяя магистральную инфраструктуру. Оборот и прибыль при этом увеличиваются.

Иными словами, абонент, оплативший полосу 64 кбит/с, использует канал в среднем лишь на 25%. Следовательно, оператор способен продать имеющийся у него ресурс в четыре раза большему числу пользователей, не перегружая свою сеть. Такой сценарий выгоден обеим сторонам - и клиенту, и продавцу, - поскольку оператор увеличивает свои доходы и уменьшает абонентскую плату за счет снижения издержек. Это выигрышное

решение уже признано в мире передачи данных, а теперь начинает использоваться и на рынке телефонии.

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).

В первом случае полоса пропускания напрямую зависит от загруженности сети Интернет пакетами, содержащими данные, голос, графику и т.д., а значит, задержки при прохождении пакетов могут быть самыми разными. При использовании выделенных каналов исключительно для голосовых пакетов можно гарантировать фиксированную (или почти фиксированную) скорость передачи. Ввиду широкого распространения сети Интернет особый интерес вызывает реализация системы Интернет-телефонии, хотя следует признать, что 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. Стоимость такой связи на порядок меньше стоимости телефонного звонка по обычным телефонным линиям. Особенно велика эта разница для международных переговоров.

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 связаться 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 Интер-ист по назначению с использованием протокола IP. Для пакетов, приходящих из сети на телефонный сервер и уходящих в телефонную линию, операция происходит в обратном порядке. Обе составляющие операции (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 надежным 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. Сегодня эти проблемы решаются: организации по стандартизации разрабатывают новые протоколы, производители выпускают новое оборудование, но на этом уровне дела с совместимостью и стандартизацией обстоят уже не так хорошо, как с «упаковкой» речи в пакеты. Заметим, что если в рамках частной корпоративной сети некоторая потеря качества голосовой связи при сильной загруженности ресурсов вполне терпима при условии, что средний показатель будет вполне удовлетворительным, то в случае сети общего пользования все намного серьезнее.

Поскольку оператор предоставляет некоторый сервис и берет за него деньги, он обязан гарантировать его качество. Даже если клиент согласен (хотя в условиях жесткой конкуренции на рынке телекоммуникаций это маловероятно) время от времени мириться с не очень высоким уровнем качества, он может предъявить претензии в случае серьезных или длительных проблем. Как бы то ни было, оператор вынужден следить за качеством предоставляемых услуг, для чего в случае их масштабного предоставления ему требуется

соответствующая аппаратура и программное обеспечение, которое достаточно дорого и имеется не во всех точках сети.

С точки зрения масштабируемости (если отвлечься от проблем с неконтролируемым ухудшением качества при росте нагрузки на сеть) IP-телефония представляется вполне законченным решением. Во-первых, поскольку соединение на базе протокола IP может начинаться (и заканчиваться) в любой точке сети от абонента до магистрали. Соответственно, IP-телефонию в сети можно вводить участок за участком, что, кстати, на руку и с точки зрения миграции, так как ее можно проводить «сверху вниз», «снизу вверх» или по любой другой схеме. Для решений IP-телефонии характерна определенная модульность: количество и мощность различных узлов - шлюзов, gatekeeper («привратников» - так в терминологии VoIP именуются серверы обработки номерных планов) - можно наращивать практически независимо, в соответствии с текущими потребностями. Естественно, проблемы наращивания ресурсов собственно сетевой инфраструктуры мы сейчас не учитываем, поскольку узлы самой сети могут быть независимы от системы IP-телефонии, а могут и совмещать в себе их функции.

1.4. История и перспективы развития Интернет-телефонии

Существует мнение, что концепция передачи голоса по сети с помощью персонального компьютера зародилась в Университете штата Иллинойс (США). В 1993 г. Чарли Кляйн выпустил в свет первую программу для передачи голоса по сети с помощью персонального компьютера Maven. Одновременно одним из самых популярных мультимедийных приложений в сети стала программа видеоконференций CU-SeeMe для компьютеров Macintosh (Mac), разработанная в Корнельском университете.

В апреле 1994 г. во время полета космического челнока Endeavor Американское агенство по аэронавтике NASA передало на Землю его изображение с помощью программы CU-SeeMe. Одновременно, используя программу Maven, попробовали передавать и звук. Полученный сигнал из Льюисовского исследовательского центра поступал на компьютер Mac, соединенный с Интернет, и любой желающий мог услышать голоса астронавтов. Потом одну программу встроили в другую, и появился вариант CU-SeeMe с полными функциями аудио и видео как для Mac, так и для персональных компьютеров (PC).

В феврале 1995 г. израильская компания VocalTec предложила первую версию программы Internet Phone, разработанную для владельцев мультимедийных PC, работающих под операционной системой Windows. Это стало важной вехой в развитии Интернет-телефонии. VocalTec надеялась использовать очень популярные (текстовые) каналы Internet Relay Chat (IRC) в качестве двустороннего средства общения между людьми, имеющими сходные интересы. Но компании не удалось связаться с Eris Free Network (EFNet), курирующей IRC, и проинформировать о потенциально возможном увеличении трафика, поэтому доступ к этим общественным каналам для Internet Phone был закрыт. Через несколько недель компания VocalTec уладила свои разногласия с EFNet. За это время была создана частная сеть серверов Internet Phone, и уже тысячи людей загрузили эту программу с домашней страницы VocalTec и начали общаться.

В том же 1995 г. другие компании очень быстро оценили перспективы, которые открывала возможность разговаривать, находясь в разных полушариях и не платя при этом за международные звонки. На рынок обрушился поток продукции, предназначенной для телефонии через сеть Интернет.

В сентябре того же года в розничной продаже появилась первая из таких программ - DigiPhone, разработанная небольшой компанией в Далласе (штат Техас), которая предложила «дуплексные» возможности, позволяя говорить и слушать одновременно. Вот в этот момент и родилась привлекательная для абонентов настоящая интерактивная связь.

В марте 1996 г. произошло еще одно памятное событие. Тогда было объявлено о

совместном проекте под названием «Internet Telephone Gateway» двух компаний: уже известной нам VocalTec и крупнейшего производителя программного обеспечения для компьютерной телефонии Dialogic. Целью было научить работать через Интернет обычный телефонный аппарат, для чего между сетью Интернет и ТфОП устанавливался специализированный шлюз. Последний получил название VTG (VocalTec Telephone Gateway) и представлял собой специализированную программу, которая использовала голосовые платы Dialogic как интерфейс с обычными телефонными линиями. Многоканальные голосовые платы позволяли, во-первых, одной системе VTG поддерживать до восьми независимых телефонных разговоров через сеть Интернет, а во-вторых, убрали проблему адресации, взяв на себя преобразование обычных телефонных номеров в IP-адреса (и обратно). Для разговора одного пользователя в том продукте достаточно было ширины полосы канала порядка 11 кбит/с (у современных продуктов она бывает другой). Вот так возможность высокого уплотнения канала и малая стоимость связи создали предпосылки для коренных изменений телекоммуникационного мира.

К настоящему времени уже сотни компаний предложили свои коммерческие решения для IP-телефонии. Одновременно практически все крупные телекоммуникационные компании, использующие традиционные средства для организации телефонных переговоров, почувствовав угрозу рынку предоставляемых ими услуг, начали интенсивные исследования с целью оценки её реальности и масштаба.

Прогресс внедрения технологии IP-телефонии характеризуют следующие цифры. В 1996 году IP-телефония за один год выросла на 997% (от оцененного в 1.8 миллионов долл. рынка), но в 1997 г. объем рынка оборудования, программного обеспечения и услуг IP-телефонии оценен уже в 210 млн. долл. Доходы от предоставления услуг телефонной и факсимильной связи в IP-сетях составили 123 млн. дол. Хотя голосовой график IP-телефонии составляет менее 1% от всех междугородных и международных звонков, рынок Интернет-телефонии в 1999 году достиг 560 миллионов долл.

Стоит упомянуть о некоторых прогнозах развития рынка IP-телефонии. Их делают многие известные аналитические компании. Прогнозы по большей части оптимистические, но звучат и голоса пессимистов.

Так, эксперты компании Killen&Associates предполагают 138% ежегодного прирост рынка до 2002 г., а эксперты Frost&Sullivan ориентируются на 149%. Аналитики Philipt Group-InfoTech прогнозируют в 2004 г. достижение этим сегментом рынка уровня 1,9 млрд долл. (при общем объеме рынка оборудования телефонных систем в 16 млрд. долл.)

По прогнозам компании Yankie Group, доля междугородных и международных звонков (по времени), осуществляемых по IP-сетям, имеет большую тенденцию роста и достигнет, например, в США к 2005 г. 15% (рис. 1.6).

В то же время, по оценкам компании TeleChoice, сотрудничающей с фирмой Lucet Technologies в области VoIP, сейчас рынок IP-телефонии составляет всего 0,1% от общего рынка речевых услуг. По прогнозам этой компании, через пять лет доля рынка IP-телефощ возрастет всего лишь до 2%. По прогнозу экспертов исследовательской компании Insigl Research даже североамериканский рынок пакетной телефонии в 2004 г. составит лишь 10% оборота рынка услуг телефонной связи. Следует подчеркнуть, что под пакетной телефонией эксперты Insight Research понимали не только технологию IP-телефонии, но транспортировку голоса с помощью фреймов Frame Relay (VoFR) и ячеек ATM (VoATM).

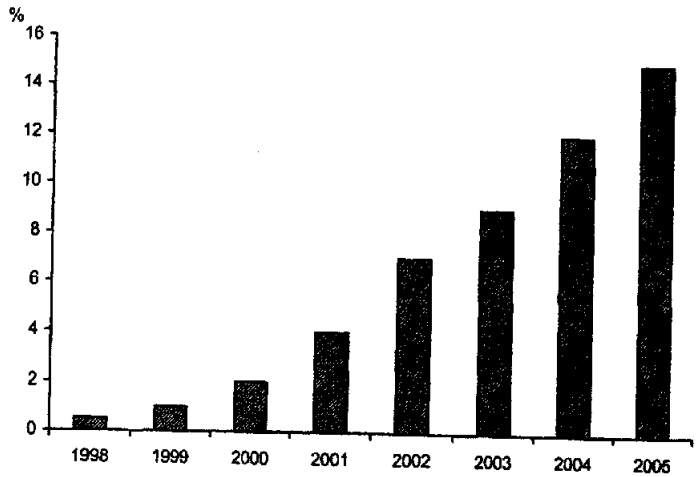

Рис. 1.6. Состояние и прогноз доли трафика IP-телефонии в США (по данным фирмы Yankie Group)

По данным фирмы Killen & Associates, голосовой трафик IP-телефонии в 1998 году в компаниях, входящих в список Fortune 1000, составлял менее 1% от всех междугородных и международных звонков. Кроме того, по оценкам фирм IDC, Link Research даже в 2001 году объем передачи голоса в сетях с коммутацией пакетов составит в США: международные звонки с территории США - 4 млрд. минут; звонки в пределах США - 8,5 млрд. минут. Это будет составлять 0,98% (менее одного процента) общего объема внутреннего (в пределах США) и международного трафика. Согласно данным Datamonitor, доля IP-телефонии в общих доходах телефонных компаний в США и Европе пока еще очень мала и даже в перспективе не превысит 1% (рис. 1.7).

Независимо от приведенных прогнозов с уверенностью можно сказать, что IP-телефония в ближайшее время не станет полноценной альтернативой традиционной телефонии, но сможет занять определенное место особенно в корпоративном сегменте, где в полной мере проявит свое истинное преимущество - возможность сопровождения телефонными переговорами потока данных в едином канале связи. Сеансы одновременной работы с одной и той же информацией в корпоративных сетях, видеоконференции, Интернет-коммерция в режиме «он-лайн» - вот где IP-телефония несомненно займет достойное положение даже с пониженным качеством речи, поскольку основную смысловую нагрузку в этих случаях будет нести информация на дисплее компьютера или видеоэкране. При этом полностью используются преимущества мульти-медийной связи: оперативность и эффективность делового общения, экономия канальных ресурсов и времени. При этом IP-телефония выступает в качестве вспомогательного средства коммуникации, дополняющего передачу данных, видеоизображений, WEB-страниц.

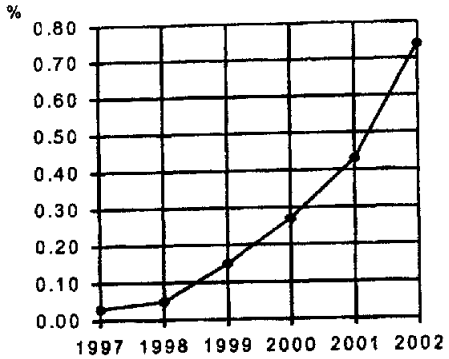

Рис. 1.7. Доля IP-телефонии в общих доходах телефонных компаний в США и Европе, % (по данным Datamonitor)

1.5. Виды соединений в сети IP-телефонии

Сети IP-телефонии предоставляют возможности для вызовов четырех основных типов:

1. «От телефона к телефону» (рис. 1.8). Вызов идет с обычного телефонного аппарата к АТС, на один из выходов которой подключен шлюз IP-телефонии, и через IP-сеть доходит до другого шлюза, который осуществляет обратные преобразования.

2. «От компьютера к телефону» (рис. 1.9). Мультимедийный компьютер, имеющий программное обеспечение IP-телефонии, звуковую плату (адаптер), микрофон и акустические системы, подключается к IP-сети или к сети Интернет, и с другой стороны шлюз IP-телефонии имеет соединение через АТС с обычным телефонным аппаратом.

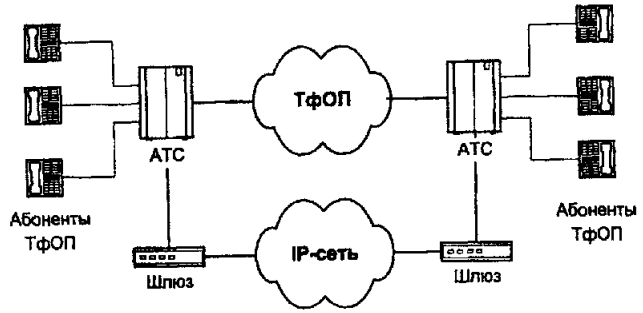

Рис. 1.8. **Схема связи «телефон-телефон»**

Следует отметить, что в соединениях 1 и 2 типов вместо телефонных аппаратов могут быть включены факсимильные аппараты, и в этом случае сеть IP-телефонии должна обеспечивать передачу факсимильных сообщений.

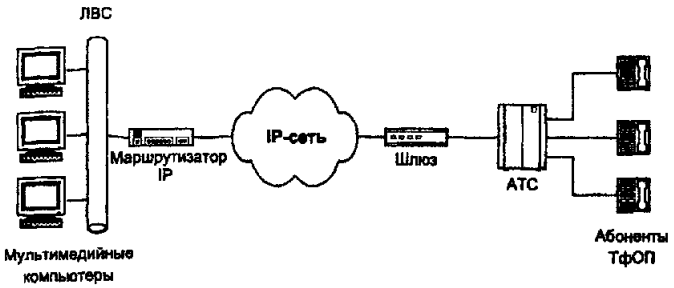

Рис.1.8. Схема связи «телефон-телефон»

3. «От компьютера к компьютеру» (рис. 1.10). В этом случае соединение устанавливается через IP-сеть между двумя мультимедийными компьютерами, оборудованными аппаратными и программными средствами для работы с IP-телефонией.

4. «От WEB браузера к телефону» (рис. 1.11). С развитием сети Интернет стал возможен доступ и к речевым услугам. Например, на WEB-странице некоторой компании в разделе «Контакты» размещается кнопка «Вызов», нажав на которую можно осуществить речевое соединение с представителем данной компании без набора телефонного номера. Стоимость такого звонка для вызывающего пользователя входит в стоимость работы в сети Интернет.

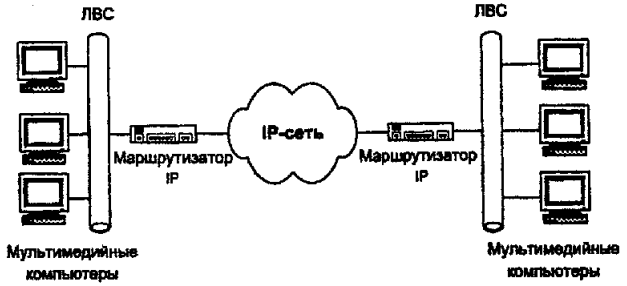

Рис. 1.10. Схема связи «компьютер-компьютер»

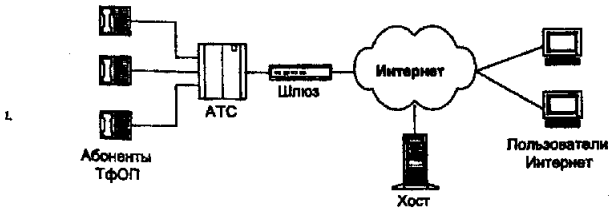

Рис. 1.11. Схема связи «WEB-браузер - телефон»

1.6. Преимущества использования IP-телефонии

Конечный пользователь IP-телефонии не только сохранит имеющиеся преимущества телефонной сети общего пользования, которые включают широкий диапазон услуг, простоту использования, надежность и качество голоса, но и получит следующие дополнительные преимущества:

•более низкие цены на традиционные услуги телефонной связи;

•IP-телефония одновременно поддерживает голос и данные, удовлетворяя требованиям конвергенции. Это означает, что клиенты получат дополнительные преимущества от экономии в развитии, возможные за счет использования единой сети, а также за счет того, что объемы графика и шаблоны быстро сменяются от данных к голосу и наоборот и это защищает клиента;

•феноменальная мобильность пользователя, которую обеспечивает сеть IP-телефонии: звонки и факсы автоматически перенаправляются в любую точку мира, пользователи будут иметь доступ к одному и тому же набору услуг вне зависимости от того, где и как они подключаются к сети. Эта распределенная архитектура обеспечивает прекрасную гибкость и делает возможным отсутствие привязки к месту предоставления услуги;

•новый набор устройств доступа, от традиционных телефонов и факсов до компьютеров;

•доступ к новым услугам (голосовая почта, конференцсвязь, передача факса и др.) через открытый интерфейс архитектуры на базе IP, что обеспечивает совместимость широкого спектра разработчиков приложений;

•возможность настройки набора услуг,

•простота оплаты услуг IP-телефонии (обычно с помощью предоплаченных телефонных карточек);

•простота контроля пользователем состояния его расчетного счета (через сеть Интернет).

Наряду с провайдерами IP-телефонии Интернет-провайдеры также могут занять определенную нишу на рынке услуг IP-телефонии, так как существующая у них IP-инфраструктура дает хорошие возможности для внедрения услуг голосовой связи. Необходимые для этого аппаратные и программные средства можно устанавливать поэтапно, интернет-провайдеры уже имеют точки присутствия, связанные с коммутаторами местных провайдеров и операторов сети общего пользования.

Для Интернет-провайдеров услуга Интернет-телефонии обеспечивает следующие имущества.

• сбережение капитальных вложений за счет использования открытых компьютерных платформ,

• снижение эксплуатационных расходов как результат предоставления разнообразия услуг на единой сети;

• открытая среда разработчика услуги означает более конкурентную, а следовательно менее дорогую разработку новых услуг.

• множество услуг может быть доступно через единственный канал с пользователем что означает больше услуг (прибыли) в расчете на одного пользователя.

Операторы «классических» телефонных сетей настороженно отнеслись к появлению IP-телефонии, так как передача речи по IP-сетям неизбежно вынуждает их снижать тарифы на междугородные и международные разговоры, что приведет к прямому сокращению и доходов. Так, финансовые службы США обещают убытки крупнейшего поставщика традиционного телефонного сервиса - компании AT&T от 620 до 950 миллионов долларов на международных звонках от потери доли рынка в пользу средств IP-телефонии.

С появлением IP-телефонии в рядах операторов дальней связи началась легкая

паника, которая вызвала первое и вполне логичное желание вытеснить с рынка появившихся конкурентов с помощью известных лоббистских приемов, позволяющих оказывать давление на национальные администрации связи с целью ограничения лицензирования, а также с помощью повышения платы за доступ в Интернет. Некоторые американские операторы, например, пытались добиться запрета IP-телефонии через Федеральную комиссию связи, однако ввиду потенциального ущемления прав потребителей все это успеха не имело

В результате традиционные телефонисты вынуждены были сами заняться IP-технологиями и, надо отдать им должное, довольно быстро преуспели в этом, используя IP-решения как минимум для создания резервных каналов для пропуска графика на случай перегрузок или аварий, что позволило получать им дополнительную прибыль. Одновременно в настоящее время проектируются универсальные магистральные IP-сети, которые в будущем должны не то чтобы заменить традиционные телефонные сети, но существенно их дополнить услугами передачи данных, видео и мультимедиа.

Тем временем оказалось, что, к сожалению, IP-телефония, не приводит к многократной экономии средств оператора, вкладываемых в передачу голосового графика на дальние расстояния, как это на первый взгляд может показаться при анализе деятельности сегодняшних компаний, предоставляющих эти услуги. И камнем преткновения здесь является все то же качество передачи речи. В результате сегодня IP-технологии успешно применяются для создания выделенных мультисервисных корпоративных сетей связи. Но если речь идет о выходе в общедоступный Интернет, в котором работают миллионы пользователей, - гарантировать высокое качество передачи речевого трафика не не берется никто Ведь передача речи весьма чувствительна к задержкам, а Интернет вовсе не гарантирует не то что задержку, но простую доставку всех посланных IP-пакетов, которые могут приходить в пункт назначения различными путями и совсем не в том порядке, в каком посылались. И то, что обычному пользователю Интернета, бродящему по Web-сайтам, порой незаметно, пользователю Интернет-телефонии очень даже мешает.

Крупные телекоммуникационные операторы, обслуживающие тысячи и сотни тысяч клиентов, вынуждены вкладывать для достижения качества, достойного их имени, такие средства, какие мало уступают инвестициям для создания традиционной сетевой инфраструктуры. Речевой трафик множества абонентов нужно где-то собрать, преобразовать его в пакеты данных, передать в нужный регион по IP сети и, преобразовав обратно в исходный вид, подать в местную телефонную сеть общего пользования. Для гарантии качесгва вместо каналов общедоступного Интернета нужны выделенные магистральные каналы (хотя и уплотненные с помощью технологии IP-телефонии) во все требуемые регионы и страны, нужна более мощная местная телефонная сеть в местах установки шлюза или требуется усгановка нескольких шлюзов (для этого нужно вкладывать в местную ТфОП соответствующие инвестиции) и многое другое. Именно так и работают сегодня серьезные поставщики услуг IP-телефонии. Таким образом, для крупных операторов IP-телефония сегодня - эго способ более эффекгивно использовагь сущесгвующий сетевой ресурс и возможность предоставления своим клиентам современного спектра дополнительных услуг (голосовая почта, конференцсвязь, поиск номеров, контроль за расчетами и многое другое), которые не реализуемы в традиционной телефонной сети, и за счет которых оператор может получить дополнительную прибыль.

Глава 2

СТАНДАРТИЗАЦИЯ IP-ТЕЛЕФОНИИ

2.1. Международные организации по стандартизации IP-телефонии

В настоящий момент времени отсутствуют международные рекомендации или стандарты, разработанные специально для IP-телефонии. В то же время для обеспечения совместимости оконечного оборудования и шлюзов различных поставщиков проблемами стандартизации IP-телефонии занимаются несколько международных организаций:

- Сектор стандартизации телекоммуникаций Международного союза электросвязи МСЭ-Т (International Telecommunications Union - Telecommunications, ITU-T);
- Европейский институт стандартизации по телекоммуникациям (European Telecommunication Standard Institute, ETSI);
- Рабочая группа по инженерным проблемам Интернет (Internet Engineering Task Force - IETF);
- Американский национальный институт стандартов (American National Standards Institute, ANSI);
- Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers, IEEE);
- Форум VoIP (Voice over IP) и другие.

Помимо специальных комиссий официальных международных организаций, например UNO (ITU-T) и EU (ETSI), проблемой стандартизации Voice over IP и Интернет-телефонии озабочены и специалисты по Internet. В IETF созданы две рабочие группы: iptel занимается выработкой стандартов передачи речи по Internet (на базе H.323), тогда как PINT (PSTN and Internet Internetworking) работает над интеграцией телефонных служб с Web.

Фирмы-производители оборудования Интернет-телефонии также уделяют большое внимание вопросам совместимости оборудования. Более 30 ведущих фирм уже обязались поддерживать профиль iNow! Profile, который должен обеспечить совместимость продуктов IP-телефонии на базе стандарта H.323 версии 2.

В рамках International Multimedia Teleconferencing Consortium (IMTC) была создана рабочая группа Voice over IP Forum. В сотрудничестве с ITU-T и ETSI идет работа по улучшению технологий IP-телефонии. При этом основной упор делается на соглашения о кодеках с высоким качеством передачи речи и умеренными требованиями к полосе пропускания. Также рассматривается проблема обеспечения взаимодействия различных H-323-терминалов, соответственно программных реализации H.323.

В табл. 2.1 приведены сведения о международных организациях, участвующих в разработке стандартов, связанных с IP-телефонией, а также о форумах и промышленных инициативах производителей аппаратно-програмного обеспечения IP-телефонии. Далее дается краткое описание наиболле зачимых направлений стандартизации IP-телефонии.

Таблица 2.1. Организации, участвующие в стандартизации IP-телефонии

Организация стандартизации	URL	Стандарты/ Протоколы	Назначение стандартов/протоколов
International Telecommunication Union (ITU)	www.itu.int	T.120	Конференция по передаче данных в реальном времени (аудиографика)
		H.320	Видеоконференция ISDN
		H.323	Видео (аудиовизуальная) связь в локальных сетях
		H.324	Видео и аудио связь через низкоскоростной канал передачи данных, например, через коммутируемое модемное соединение
ETSI/TIPHON	www.etsi.org	OSP	Протокол открытого взаимодействия, обеспечивает передачу IP графика на основе языка XML
Internet Engineering Task Force (IETF)	www.ietf.org	SIP	Протокол инициализации сеансов связи для шлюзов VoIP и оконечного оборудования пользователей
		RSVP	Протокол резервирования ресурсов, обеспечивает приоритезацию пакетного графика пользователей
		RTP/AVT	Протокол реального времени, обеспечивает передачу аудио и видео в реальном времени (но не гарантирует качество)
		MGCP	Протокол управления медиа шлюзом, определяет, как производится управление пакета ми данных от различных служб (например, голоса и видео)
		LDAP	Упрощенный протокол доступа к каталогам, обеспечивает универсальную адресацию баз данных в сетях
Промышленные форумы	URL	Члены форума	Основные направления деятельности
International Multimedia Teleconferencing Consortium (IMTC)	www.imtc.org	Учрежден в 1993 г., более 145 членов	IMTC поддерживает H.323 (и другие стандарты ITU), iNow и другие
Softswitch Consortium	www.soft-switch.org	Учрежден в 1999 г. членов	Основное внимание уделяет протоколу SIP/MGCP и другим технологиям взаимодействия сетей
Internet & Telecoms Convergence Consort	itel.mit.edu	Академии/ корпорации	Выпускает технические, экономические и технологические обзоры
Промышленные инициативы	URL	Учредители	Основные направления деятельности
Interoperability Now!	www.imtc.org /	ITXC, Lucent, VocalTec	Стандартный профиль взаимодействия систем IP-телефонии различных производителей и провайдеров, основанный на H.323

IP Call Detail Record (IPDR)	www.ipdr.org	Jerry Lucas и 19 соучредителей	Цель - определить лучший протокол для передачи IP-трафика и биллинга и предложить его для обсуждения
VON Coalition	www.von.org	JeffPulvern 22 соучр	Определение возможностей нерегулируемого предоставления IP-услуг и информирование пользователей и средств массовой информации о наиболее важных технологиях

2.2. Стандарты ITU-T

Начальное развитие техники IP-телефонии опиралось в большей степени на рекомендации Международного союза электросвязи (ITU-T). В первую очередь, это Рекомендации G.729a и G.723.1, устанавливающие стандарты на компрессию речи до скорости 8 кбит/с и 6,3/5,3 кбит/с, соответственно, и Рекомендация H.323 v.2 (02/98). Последняя рекомендация определяет порядок взаимодействия между системами передачи мультимедийной информации (в том числе в реальном времени) и сетями пакетной коммутации, которые могут не обеспечивать гарантированного качества обслуживания (Quality of Service, QoS). Для передачи речевой информации через IP-сеть Рекомендация H.323 v.2 обязательна, т.е. фактически является стандартом.

Стандарт H.323

Набор рекомендаций МСЭ-Т H.323 определяет сетевые компоненты, протоколы и процедуры, позволяющие организовать мультимедиа-связь в пакетных сетях, в том числе в ЛВС Ethernet. Они определяют порядок функционирования абонентских терминалов в сетях с разделяемым ресурсом, не гарантирующих качества обслуживания QoS. H.323-совместимые устройства могут применяться для телефонной связи, передачи звука и видео (видеотелефония), а тавке звука, видео и данных (мультимедийные конференции).

В связи с появлением множества аппаратно-программных средств организации телефонной связи по протоколу IP потребовалось внести изменения в спецификации H.323, так как эти средства зачастую оказывались несовместимыми друг с другом. В частности, понадобилось обеспечить взаимодействие телефонных устройств на базе ПК и обычных телефонов для сетей, функционирующих по принципу коммутации каналов. Вторая версия H.323, учитывающая новые требования, была принята в январе 1998 г.

В настоящее время готовится следующая версия стандарта. В ней будут описаны создание пакетных сетей факсимильной связи и организация связи между H.323-шлюзами. Речь идет и о функциях, распространенных в современной телефонии, включая уведомление о поступлении второго вызова и режим справки. Некоторые компании добиваются включения в H.323 поддержки мультимедиа-возможностей, основанных на предложенном IETF протоколе Session Initiation Protocol. Помимо «телефонных» функций новая версия будет дополнена средствами, позволяющими учитывать параметры сеансов для целей тарификации, а также поддержкой каталогов - вместо цифровых IP-адресов можно будет пользоваться именами абонентов.

Стандарт H.323 входит в семейство рекомендаций H.32x, описывающих порядок организации мультимедиа-связи в сетях различных типов:

- H.320 - узкополосные цифровые коммутируемые сети, включая ISDN;
- H.321 - широкополосные сети ISDN и ATM;
- H.322 - пакетные сети с гарантированной полосой пропускания;

• H.324 - телефонные сети общего пользования (ТфОП).

Одна из основных целей разработки стандарта H.323 - обеспечение взаимодействия с другими типами сетей мультимедиа-связи (рис. 2.1). Данная задача реализуется с помощью шлюзов, осуществляющих трансляцию сигнализации и форматов данных. Стандарт H.323 позволяет создать надежные решения для организации коммуникаций по ненадежным сетям с переменной задержкой. При условии соответствия стандарту устройства с различными возможностями могут и взаимодействовать друг с другом. Например, терминалы с видеосредствами могут участвовать в аудиоконференции. В совокупности с другими стандартами МСЭ-Т на мультимедийную связь и телеконференции рекомендации H.323 применимы для любых видов соединений - от многоточечных до соединений «точка-точка». Основные компоненты этого стандарта приведены в табл. 2.2.

Стандарт H. 323 определяет также порядок взаимодействия с оконечными устройствами других стандартов. Наиболее часто такая задача возникает при сопряжении телефонных сетей с коммутацией пакетов и коммутацией каналов. Сети стандарта H.323 совместимы и с другими типами H.32x-сетей. Межсетевое взаимодействие различных H.32x-сетей определяет рекоминдация H.246. На следующем этапе развития IP-телефонии к спецификациям H.323, соответствующим нижним уровням эталонной модели взаимодействия открытых систем (ЭМВОС), будут добавлены новые. Они зафиксируют возможности обеспечения классов (class-of-service, CoS) и качества обслуживания (quality-of-service, QoS), т. е. услуг, относящихся, соответственно, ко второму (канальному) и третьему (сетевому) уровням. Разработкой спецификаций CoS/QoS занимается ряд организаций, в том числе рабочие группы IEEE 802.1p и IETF Diff-Serv, а также Европейский институт стандартизации в области электросвязи (ETSI), который включил продукты H.323 в свой проект Telecommunications and internet Protocol Harmonization Over Networks (TIPHON).

Стандарты T.37, T.38

Факсимильная связь на базе IP-сети опирается на два основных стандарта МСЭ-Т. Рекоминдация T.37 описывает преобразование традиционных сигналов факсов в почтовые сообщения SMTP с MIME-совместимыми вложениями в формате TIFF. Эта методика используется обычно поставщиками IP-факсов и сводит передачу факсов к доставке с промежуточным хранением, так как изображения факсов передаются в виде вложений электронной почты. Благодаря Рекомендации T.37 факс-аппараты и факс-серверы на базе IP различных поставщиков могут взаимодействовать друг с другом согласованно, как и традиционные факсы. Однако Рекомендация T.37 описывает всего лишь основные функции для доставки факсов с помощью электронной почты.

Например, он предусматривает применение всего одного метода сжатия - модифицированного метода Хофмана, ограничивая, таким образом, возможности экономии пропускной способности. К тому же, он не делает различий между разными типами факсов, хотя некоторые провайдеры услуг уже давно настраивают доставку факсов в зависимости от конкретного вида передаваемого графика.

Стандарт T.38 описывает передачу факсов в реальном времени либо посредством имитации соединения с факс-аппаратом, или с помощью метода модуляции под названием FaxRelay. Рекомендация T.38 может использоваться для реализации функциональности, более схожей с традиционной факсимильной связью, например для немедленного подтверждения.

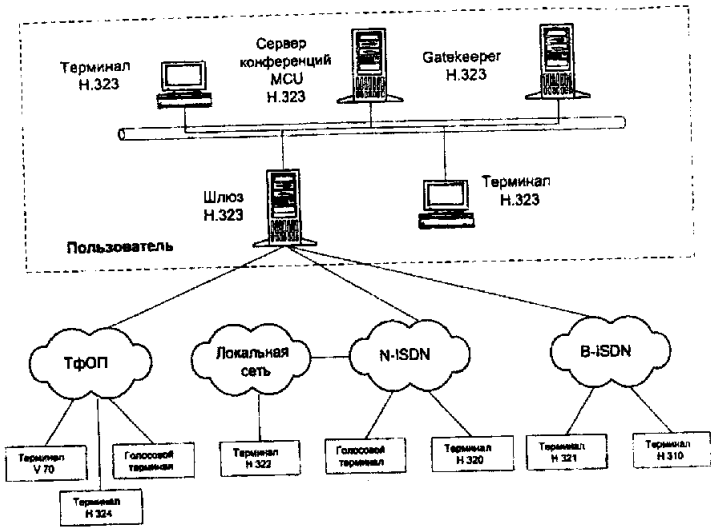

Рис. 2.1. Конфигурация сети на базе стандарта H.323

Таблица 2.2. Основные компоненты стандарта H.323

Рекомендация	Описание
H.225	Определяет сообщения по управлению вызовом, включая сигнализацию и регистрацию, а также пакетизацию и синхронизацию потоков мультимедийных данных
H.245	Определяет сообщения для открытия и закрытия каналов для передачи потоков мультимедийных данных, а также другие команды и запросы
H.261	Видеокодек для аудиовизуальных сервисов на каналах P x 64 кбит/с
H.263	Описывает новый видеокодек для передачи видео по обычным телефонным сетям
G.711	Аудио кодек, 3,1 кГц на 48, 56, и 64 кбит/с
G.722	Аудио кодек, 7 кГц на 48, 56, и 64 кбит/с
G.728	Аудио кодек, 3,1 кГц на 16 кбит/с
G.723	Аудио кодек, для режимов 5,3 и 6,3 кбит/с
G.729	Аудио кодек

2.3. Стандарты ETSI

Европейский институт стандартизации телекоммуникаций ETSI разрабатывает проект, получивший название **TIPHON** (Telecommunications and IP Hannonization ove

Network). Цель проекта - определение глобальных стандартов на Интернет-телефонию, обеспечивающих взаимодействие IP-сетей с телефонными сетями общего пользования, а также сотовыми сетями. При этом для доступа абонентов ТфОП к пользователям услуг IP-телефонии предлагается выделить глобальный код службы в международном плане нумерации, определенном в Рекомендации ITU-T E.I 64. Структура проекта TIPHON и разрабатываемые рабочими группами документы показаны на рис. 2.2.

Задачу реализации проекта TIPHON предполагается решить в четыре этапа. На первых двух этапах стандартизуются процессы установления соединения между H.323-терминалами и пользователями ТфОП (рис. 2.3), а затем между телефонной сетью и H-323-терминалами (рис. 2.4) На третьем этапе предполагается через IP-сети обеспечить соединение между абонентами ТфОП. Наконец, четвертая фаза определит процедуру соединения терминалов-H323 через телефонную сеть (рис. 2.6). В марте 1999 года было официально объявлено о завершении первой фазы, а работа над реализацией второго и третьего этапов продолжается.

2.4. Стандарты IETF

Рабочая группа по инженерным проблемам Интернет (Internet Engineering Task Force -**IETF**) сосредоточила свои усилия на задаче более общего характера - развитии мультимедийных возможностей Интернет.

Первое, что было рекомендовано IETF, - это протокол резервирования ресурсов *(Resource Reservation Protocol, RSVP)*. С помощью PSVP мультимедиа-программы могут потребовать специального качества обслуживания (specific quality of service, QoS) посредством любого из существующих сетевых протоколов - главным образом IP, хотя возможно использовать **UDP** - чтобы обеспечить качественную передачу видео- и аудиосигналов. Протокол **RSVP** предусматривает QoS благодаря тому, что через каждый узел, который связывает между собой участников телефонного разговора, может передаваться определенное количество данных.

Протокол RSVP реализован в маршрутизаторах фирм Cisco, Nortel Networks и многих других производителей.

Хотя протокол RSVP предусматривает решение проблемы QoS, в нем не устранен принципиальный недостаток, присущий протоколам Интернет для программ мультимедиа, - недостаточно развитые средства синхронизации данных. Надежные протоколы, такие, как TCP/IP, располагают многоуровневыми средствами, предотвращающими потерю данных. Однако многоуровневая архитектура может помешать выполнению чувствительных к временной упорядоченности процедур декодирования аудио- и видеосигналов, реагирующих на несвоевременное поступление данных. Кроме того, временные критерии вообще не фигурируют в IP. Из этого следует, что синхронизация может оказаться крайне сложной задачей. Поэтому комитетом IETF был разработан транспортный протокол реального времени *(RTR, Real-time Transport Protocol)*. Протокол описан в документе RFC 1889, а также включен Рекомендацию H.323.

Как правило, протокол RTP используется как надстройка поверх какого-нибудь ненадежного протокола, например UDP. К каждому пакету данных, посылаемых посредством RTP, прилагается информация о времени его посылки и порядковый номер. Благодаря этой дополнительной информации прикладные программы могут относительно несложно смешивать потоки аудио- и видеоданных. Информация о времени посылки,

Рис.2.2. Структура проекта TIPHON

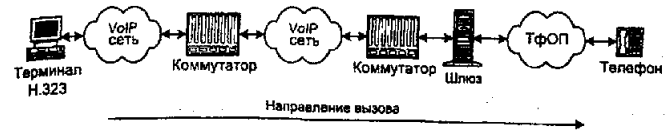

Рис. 2.3. Сценарий 1 проекта TIPHON

Рис. 2.4. Сценарий 2 проекта TIPHON

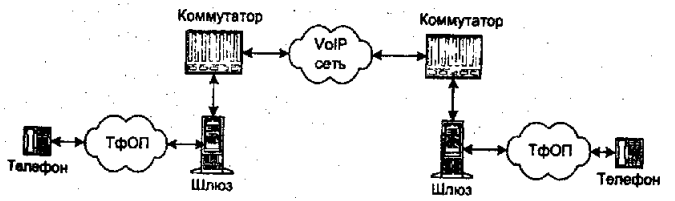

Рис. 2.5. Сценарий 3 проекта TIPHON

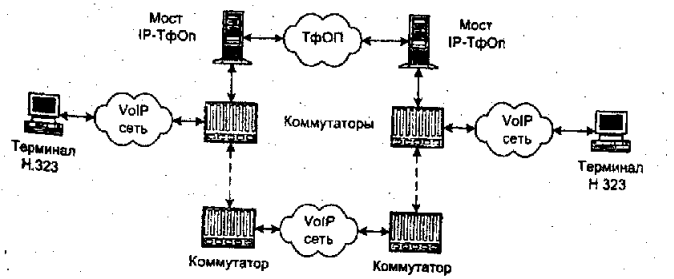

Рис 2.6. Сценарий 4 проекта TIPHON

прилагаемая к каждому пакету, позволяет, кроме того, осуществлять синхронизацию без особых трудностей, так как программа может легко определить порядковый номер кадра, к которому нужно перейти если приходится пропускать некоторые видеокадры. Еще одно преимущество RTP состоит том, что его можно использовать с RSVP для передачи синхронизированной мультимедиа-информации с определенным уровнем качества обслуживания.

Возможности RTP были расширены путем объединения его с еще одним протоколом IETF, а именно с протоколом управления передачей в реальном времени *(Real-time Transpol Control Protocol, RTCP)*. С помощью протокола RTCP программы могут приспосабливаться к изменяющимся нагрузкам на сеть, уведомляя отправителей и получателей о всплеска (spikes) - резких изменениях объемов передаваемой по сети информации. Например, RTCP совместимый телефон может отслеживать пропускную способность сети и мгновенно переключаться на алгоритм кодирования/декодирования

аудиосигнала более низкого качества, если в сети становится слишком много пользователей.

Быстрое развитие IP-телефонии выявило проблему совместимости шлюзов, предназначенных для сопряжения IP-сетей и сетей с коммутацией каналов. Специальная рабоча группа по управлению многоточечными сеансами мультимедиа-связи (MMUSIC) организации IETF разработала собственный протокол прикладного уровня для инициализации сеансов связи *SIP (Session Initiation Protocol)*, который был принят в качестве стандарта RFC 2543 в марте 1999 года. Протокол SIP, не включенный пока ITU-T в стандарт H.323, может оказать огромное влияние на распространение Интернет-телефонии, поскольку он стирает границы пока еще существующие между ней и обычной телефонией.

Этот протокол служит для установления сеансов Интернет-телефонной и мультимедийной связи и использует IP-адреса, а не ISDN-номера как протокол H.323. В него входят также протоколы передачи данных в режиме реального времени RTP и RTCP, а также протокол описания технических параметров сеанса связи *SDP (Session Description Protocol)*. Протоколы RTP и RTCP включены в стандарт H.323, а вот SDP и SIP нет. Последние не могу существовать друг без друга и являются протоколами сигнализации в сетях IP. Протокол SDP описывает параметры (возможности) устройств, необходимые для участия в сеансе мультимедийной связи, протокол SIP служит для установления связи между двумя любыми сетевыми устройствами. Для решения соответствующих задач в стандарт H.323 включены протоколы Q.931, RAS и H.245.

Две рабочие группы IETF работают над стандартом качества обслуживания QoS для Интернет. Одна из этих групп разрабатывает механизм многопротокольного коммутирования меток (Multiprotocol Label Switching, MPLS), а другая - спецификации дифференцированного обслуживания (Differentiated Services, Diff-Serv).

Группа MPLS была создана, чтобы помочь в расширении структурных связей сети Интернет за счет внедрения методов коммутирования цепей в среду коммутации пакетов без установления логических соединений. Для этого в технологии MPLS предусматривается добавление к IP-пакетам специальной метки, указывающей, что трафик будет направляться через Internet по заранее определенным маршрутам. Очевидно, что спецификации MPLS позволяют коммутаторам и маршрутизаторам значительно уменьшить время поиска адресов, по которым должны передаваться пакеты. Кроме того, MPLS обеспечивает более детерминированное и предсказуемое функционирование сети Интернет, что важно для поддержки QoS.

В деятельности группы MPLS принимают активное участие представители крупнейших поставщиков сетевых решений и оборудования. Эта архитектура выросла из системы Tag Switching, предложенной Cisco Systems, однако некоторые идеи были заимствованы у конкурирующей технологии IP-коммутации, созданной компанией Ipsilon, и проекта ARIS корпорации IBM. В архитектуре MPLS собраны наиболее удачные элементы всех упомянутых разработок, и, по прогнозам, она должна превратиться в стандарт Internet благодаря усилиям IETF и компаний, заинтересованных в скорейшем продвижении данной технологии на рынок.

Спецификация Diff-Serv предназначена для присвоения различным приложениям значений параметров, присущих разным уровням QoS. Согласно Diff-Serv, биты типа службы (ToS) в IP-заголовках указывают на класс QoS для различных видов графика и назначаются на основе соглашений об уровне обслуживания, заключаемых между пользователями и поставщиками услуг.

Спецификации Diff-Serv и MPLS используют для обеспечения QoS маркировку пакетов. Но Diff-Serv работает на третьем уровне модели OSI, а MPLS - на втором. MPLS работает как с Diff-Serv, так и без этой спецификации, и наоборот. Однако возможна и их совместная работа - MPLS-устройства могут устанавливать метки для последующей

коммутации после считывания инструкций Diff-Serv из ToS в IP-заголовках.

В настоящее время в IETF реализуется также проект в области управления сетью на основе правил: это исследования, связанные с определением стандартной инфраструктуры для применения данной методологии, а также набора необходимых протоколов и схем работы. Чтобы обеспечить оптимальный процесс хранения и извлечения из хранилища правил, составляющих стратегии, их внутреннее представление должно быть формализовано в структуру данных. Рабочая группа IETF Policy Framework Working Group (PFWG) разработала модель Policy Framework Core Information Model, в которой определен высокоуровневый набор объектно-ориентированных классов, достаточный для представления базовых стратегий управления. Объектные классы могут расширяться производными классами конкретных типов стратегий - например, обеспечения QoS или безопасности.

2.5. Профиль iNow

Есть еще одна проблема, которая присуща всем новым технологиям - несовместимость между собой оборудования разных производителей. Чтобы решить ее, ведущими производителями выдвинута инициатива iNow. Если говорить о технологии Voice over IP в общем, то к ней просматривается интерес и традиционных операторов, например, для предоставления экономичных решений небольшим офисам. Фактически, речь идет о реализации с помощью Voice over IP «последней мили». Естественно, такие решения оказываются сильно дешевле традиционных, которые предусматривают установку определенного количества входящих линий (абонентских или соединительных) и УАТС. Шесть ведущих производителей телефонных IP-шлюзов - Ascend Communications, Siemens, Cisco Systems, Dialogic, Natural MicroSystems и Clarent - намерены добиться полной совместимости своих IP-шлюзов и устройств доступа к ним (gatekeepers). С этой целью названные компании обеспечат в своих устройствах поддержку спецификаций iNow (Interoperability Now), совместно разработанных фирмами Lucent Technologies, ITXC и VocalTec Communications.

Спецификации iNow определяют способы обработки служебной информации при установлении телефонного соединения, меры безопасности и другие функции уровня управления средой передачи, необходимые для установления телефонного соединения между IP-шлюзами. iNow базируются на стандарте H.323 и Приложении G рекомендации H.225.0, которое описывает процедуры организации междоменной связи.

Первыми о совместимости своих шлюзов объявили фирмы Lucent Technologies и VocalTec. В настоящее время их оборудование проходит испытания в коммерческой сети американского оператора ITXC. Остальные производители собираются представить оборудование с поддержкой iNow в ближайшее время.

Глава 3

БАЗОВАЯ АРХИТЕКТУРА СИСТЕМ IP-ТЕЛЕФОНИИ

3.1. Архитектура системы на базе стандарта H.323

Рекомендация H.323 разработана Сектором стандартизации телекоммуникаций Международного союза электросвязи (МСЭ-Т) и содержит описания терминальных устройств, оборудования и сетевых служб, предназначенных для осуществления мультимедийной связи в сетях с коммутацией пакетов (например, в корпоративной интрасети или Интернет). Терминальные устройства и сетевое оборудование стандарта H.323 могут передавать данные, речь и видеоинформацию в масштабе реального времени. В Рекомендации H.323 не определены: сетевой интерфейс, физическая среда передачи информации и транспортный протокол, используемый в сети. Сеть, через которую осуществляется связь между терминалами H.323, может представлять собой сегмент или множество сегментов со сложной топологией. Терминалы H.323 могут быть интегрированы в персональные компьютеры или реализованы как автономные устройства. Поддержка речевого обмена - обязательная функция для устройства стандарта H.323.

В рекомендации H.323 описываются четыре основных компонента (рис. 3.1):

- терминал;
- gatekeeper (контроллер зоны);
- шлюз;
- устройство управления многоточечной конференцией (MCU).

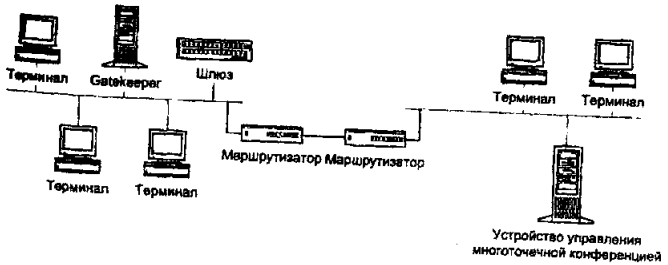

Рис. 3.1. Зона H.323

Все перечисленные компоненты организованы в так называемые зоны H.323. Одна зона состоит из gatekeeper и нескольких конечных точек, причем gatekeeper управляет всеми конечными точками своей зоны. Зоной может быть и вся сеть поставщика услуг IP-телефонии или ее часть, охватывающая отдельный регион. Деление на зоны H.323 не зависит от топологии пакетной сети, но может быть использовано для организации наложенной сети H.323 поверх пакетной сети, используемой исключительно в качестве транспорта.

Терминалы H.323

Терминал H.323 представляет собой конечную точку в сети, способную передавать и принимать трафик в масштабе реального времени, взаимодействуя с другим терминалом H.323, шлюзом или устройством управления многоточечной конференцией (MCU).

Для обеспечения этих функций терминал включает в себя:

- элементы аудио (микрофон, акустические системы, телефонный микшер, система акустического эхоподавления);
- элементы видео (монитор, видеокамера);
- элементы сетевого интерфейса;
- интерфейс пользователя.

H.323-терминал должен поддерживать протоколы H.245, Q.931, RAS, RTP/RTCP и семейство протоколов H.450, а также включать в себя аудиокодек G.711. Также немаловажна поддержка протокола совместной работы над документами T. 120.

Примером терминала, поддерживающим стандарт H.323, является аппарат фирмы Seisms Systems (приобретена компанией Cisco Systems). Он выглядит как обычный цифровой системный телефон, только оснащенный интерфейсом Ethernet вместо порта RJ-11. Такой терминал, используя собственные процессоры, микропрограммные кодеки и стек TCP/IP, обеспечивает высокие качество звука и уровень надежности.

Шлюзы H.323

Технология передачи голоса по IP-сети вместо классической сети с коммутацией каналов предусматривает конфигурацию с установкой шлюзов. Шлюз обеспечивает сжатие информации (голоса), конвертирование ее 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.

Более полно 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 данных и обратно.
- Преобразование речевого сигнала в пакеты данных и обратно.
- Соединение абонентов.
- Передача по сети сигнализационных и речевых пакетов.
- Разъединение связи.

1

Большая часть функций шлюза в рамках архитектуры TCP/IP реализуются в процессах прикладного уровня.

Наличие разноплановых с вычислительной точки зрения функций, выполняемых системой, порождает проблему ее программной и аппаратной реализации. Рациональное решение этой проблемы основано на использовании распределенной системы, в которой управленческие задачи и связь с сетью осуществляется с помощью универсального процессора, а решения задач сигнальной обработки и телефонного интерфейса выполняются на цифровом процессоре обработки сигналов.

Схема обработки сигналов в шлюзе при подключении аналогового двухпроводного телефонного канала PSTN показана на рис. 3.2.

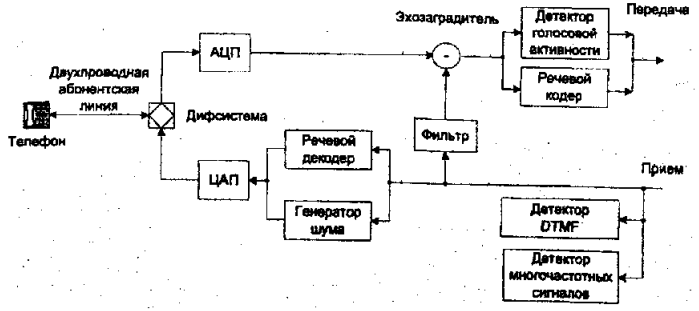

Рис. 3.2. Схема обработки сигналов в шлюзе

Телефонный сигнал с двухпроводной абонентской линии поступает на дифференциальную систему, которая разделяет приемную и передающую части канала. Далее сигнал передачи вместе с "просочившейся" частью сигнала приема подается на аналого-цифровой преобразователь (ADC) и превращается либо в стандартный 12-разрядный сигнал, либо в 8-разрядный сигнал, закодированный по μ- или А-закону. В последнем случае обработка должна также включать соответствующий экспандер. В устройстве эхо-компенсации (Echo canceller) из сигнала передачи удаляются остатки принимаемого сигнала. Эхо-компенсатор представляет собой адаптивный нерекурсивный фильтр, длина памяти (порядок) которого и механизм адаптации выбираются такими, чтобы удовлетворить требованиям рекомендации МСЭ-Т G.I 65. 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 (Speech Coder). В анализаторе кодера сигнал сегментируется на отдельные фрагменты определенной 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 (VAD - voice activity detector), который решает, является ли текущий анализируемый фрагмент сигнала речью или паузой. При наличии паузы информационный кадр может не передаваться в службу виртуального канала. На сеансовый уровень передается лишь каждый пятый «паузный» информационный кадр. Кроме того, при отсутствии речи для кодировки текущих спектральных параметров используется более короткий информационный кадр. На приемной стороне из виртуального канала в логический поступает либо в информационный кадр, либо флаг наличия паузы. На паузных кадрах вместо речевого ситезатора включается генератор комфортного шума (Noise Generator), который восстанавливает спектральный состав паузного сигнала. Параметры генератора обновляются при получении паузного информационного кадра. Наличие информационного кадра включает речевой декодёр, на выходе которого формируется речевой сигнал. Для эхо-компенсатора этот сигнал является сигналом дальнего абонента, фильтрация которого дает составляющую электрического эха в передаваемом сигнале. В зависимости от типа цифро-аналогового преобразования (DAC) сигнал может быть подвергнут дополнительной кодировке по А - или μ-закону.

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.

С построением кодеков тесно связана задача синтеза VAD. Основная трудность состоит в правильном детектировании пауз речи на фоне достаточно интенсивного акустическо| шума (шум офиса, улицы, автомобиля и т.д.)

Gatekeeper H.323

Функцию управления вызовами выполняет gatekeeper (контроллер зоны). Gatekeeper выполняет следующие функции:

- преобразовывает адреса-псевдонимы в транспортные адреса;
- контролирует доступ в сеть на основании авторизации вызовов, наличия необходимой для связи полосы частот и других критериев, определяемых производителем;
- контролирует полосу пропускания;
- управляет зонами.

Причем gatekeeper осуществляет вышеперечисленные функции в отношении терминалов, шлюзов и устройств управления, зарегистрированных в нем. Идентификация узла можно осуществляться по его текущему IP-адресу, телефонному номеру E.164 или подстановочному имени - строке символов, наподобие адреса электронной почты. Gatekeeper упрощает процесс вызова, позволяя использовать легко запоминающееся подстановочное имя.

Функции gatekeeper могут быть встроены в шлюзы, элементы распределенных УПАТС, блоки управления многоточечными конференциями, а также в конечные узлы H.323 (терминалы). С помощью механизмов RAS (Registration/Admissions/Status) терминалы могут находить gatekeeper и регистрироваться в них.

Сервер управления конференциями (MCU)

Сервер управления конференциями (MCU - Multipoint Control Unit) обеспечивает связь трех и более H.323-терминалов. Все терминалы, участвующие в конференции, устанавливают соединение с MCU. Сервер управляет ресурсами конференции, согласовывает возможности терминалов по обработке звука и видео, определяет аудио- и видеопотоки, которые необходимо направлять по многим адресам.

В рамках архитектуры H.323 может быть использовано два подхода для построения системы управления многоточечными конференциями:

- децентрализованное управление многоточечной конференцией;
- централизованное управление многоточечной конференцией.

Первый тип требует, чтобы все участники конференции пересылали многоадресные (групповые) сообщения всем остальным. Это позволяет избежать концентрации трафика в некоторых сегментах сети, но управлять такой конференцией не очень удобно. Но большинство производителей предлагают централизованные системы MCU. При их использовании конечные узлы передают сигнал системе MCU, которая и обеспечивает его рассылку. Чтобы связывать группы участников конференции, централизованные системы MCU могут каскадироваться.

Подавляющее большинство производителей систем MCU стандарта H.323 предлагают использовать стандартные браузеры для администрирования и планирования конференций, и для прямого контроля и мониторинга gatekeeper и систем MCU. Это позволяет поместить сервер MCU в коммуникационный шкаф и управлять им из любой точки сети.

По архитектуре MCU подразделяются на системы на базе стандартных серверов (Windows NT) и автономные программно-аппаратные комплексы, устанавливаемые в стойку.

Примерами MCU первого типа являются - Encounter Netserver 1.2.1 фирмы VideoServer, MeetingPoint 4.0 фирмы White Pine Software, PictureTel330 NetConference Multipoint Video Server фирмы PictureTel.

Продукты MultiMedia Communications Exchange (MMCX) компании Eucent Technologies и MCU-323 фирмы RADVision представляют собой устройства второго типа. Такие системы, будучи однажды сконфигурированными, могут круглосуточно работать в коммутационных шкафах и управляться дистанционно. MMCX компании Eucent представляет собой универсальную коммуникационную систему, поддерживающую любые H.323-совместимые устройства и IP-телефоны.

3.2. Характеристики шлюзов IP-телефонии

В общем случае IP-телефония опирается на две основных операции: преобразование двунаправленной аналоговой речи в цифровую форму внутри кодирующего/декодирующего устройства (кодека) и упаковку в пакеты для передачи по IP. Эти функции чаще всего выполняют автономные шлюзовые устройства, которые имеют несколько разновидностей. Это могут быть выделенные устройства или совмещенные маршрутизаторы/коммутаторы со встроенным аппаратным и программным обеспечением шлюза. Другой тип автономных устройств представляют пограничные устройства, где шлюз объединен с удаленным доступом и пулом модемов. Положение шлюзов в сети IP-телефонии показано на рис. 3.3. Независимо от способа аппаратной реализации шлюзы IP-телефонии могут иметь ряд характеристик, которые приведены ниже.

Совместимость со стандартом H.323

Базовым протоколом для работы IP-оборудования подавляющим большинством производителей был принят протокол, описанный МСЭ-Т в рекомендации H.323v2, стандартизирующей мультимедийную связь в сетях с коммутацией пакетов.

Пользователи мультимедийных персональных компьютеров с программным обеспечением H.323 могут подключиться к такой системе шлюзов. Вызовы при этом могут быть направлены на поддерживающие H.323 шлюзы других производителей. В результате данная система будет обеспечивать интеграцию речи, видео и данных в реальном времени для приложений по организации совместной работы в рабочих группах, например Microsoft NetMeeting.

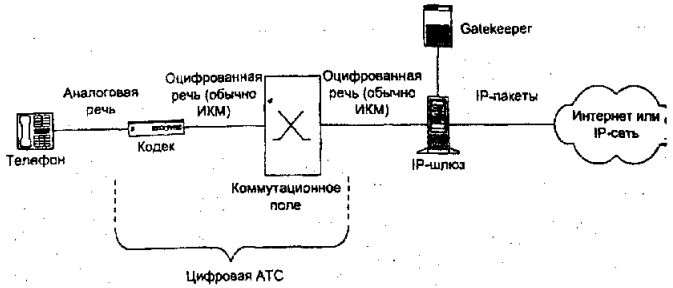

Рис. 3.3. Положение шлюза в сети IP-телефонии

Стандарты, отличные от H.323, используют в своей работе шлюзы CX950 Access Switch компании Memotec Comminications Inc., F-50 IP и F-200 IP компании Neura Communications Inc., VIP Gateway от Nortel Networks, сетевые станции Network Exchange 2201/2210 фирмы Netrix Corp.

Наличие механизмов резервирования ресурсов

Поддержка какой-либо схемы приоритезации (протокол резервирования RSVP или байт дифференциации услуг - DS byte) для осуществления возможности выбора приоритета между передаваемой речью или данными является важной характеристикой шлюза. При этом протокол RSVP позволяет маршрутизаторам придерживать часть полосы пропускания д организации голосового графика. У шлюзов IPT (Ericsson Inc.), Netblazer 8500 (Digi International), Packetstar IP Gateway 1000 (Lucent Technologies Inc.), Vocaltec Telephony Gateway (Vocaltec Communications Ltd.), Webphone Gateway Exchange (Netspeak Corp.) эта возможность отсутствует.

Поддержка основных телефонных интерфейсов J и типов сигнализаций

Важными критериями при оценке характеристик шлюзов является возможно большое разнообразие телефонных интерфейсов, поддерживаемых IP-шлюзом (El, PRI, BRI) и аналогового в частности, а также поддержка основных типов телефонной сигнализации: CAS, DTMF, PRI и ОКС №7. Существенную роль играет поддержка оборудованием механизмов безопасности в соответствии с Рекомендацией H.235.

Транспортные архитектуры

Диапазон транспортных архитектур, с которыми работают современные шлюзы, достаточно широк: выделенные линии, ISDN, Frame Relay, ATM, Ethernet. Шлюзы, поддерживающие передачу речи через Frame Relay, производят компании 3COM (Pathbuilder S200 Voice Access Switch), Cisco (серия 2600, 3600), Motorola (Vanguard

Подавляющее большинство производителей систем MCU стандарта H.323 предлагают использовать стандартные браузеры для администрирования и планирования конференций, и для прямого контроля и мониторинга gatekeeper и систем MCU. Это позволяет поместить сервер MCU в коммуникационный шкаф и управлять им из любой точки сети.

По архитектуре MCU подразделяются на системы на базе стандартных серверов (Windows NT) и автономные программно-аппаратные комплексы, устанавливаемые в стойку.

Примерами MCU первого типа являются - Encounter Netserver 1.2.1 фирмы VideoServer, MeetingPoint 4.0 фирмы White Pine Software, PictureTel330 NetConference Multipoint Video Server фирмы PictureTel.

Продукты MultiMedia Communications Exchange (MMCX) компании Eucent Technologies и MCU-323 фирмы RADVision представляют собой устройства второго типа. Такие системы, будучи однажды сконфигурированными, могут круглосуточно работать в коммутационных шкафах и управляться дистанционно. MMCX компании Eucent представляет собой универсальную коммуникационную систему, поддерживающую любые H.323-совместимые устройства и IP-телефоны.

3.2. Характеристики шлюзов IP-телефонии

В общем случае IP-телефония опирается на две основных операции: преобразование двунаправленной аналоговой речи в цифровую форму внутри кодирующего/декодирующего устройства (кодека) и упаковку в пакеты для передачи по IP. Эти функции чаще всего выполняют автономные шлюзовые устройства, которые имеют несколько разновидностей. Это могут быть выделенные устройства или совмещенные маршрутизаторы/коммутаторы со встроенным аппаратным и программным обеспечением шлюза. Другой тип автономных устройств представляют пограничные устройства, где шлюз объединен с удаленным доступом и пулом модемов. Положение шлюзов в сети IP-телефонии показано на рис. 3.3. Независимо от способа аппаратной реализации шлюзы IP-телефонии могут иметь ряд характеристик, которые приведены ниже.

Совместимость со стандартом H.323

Базовым протоколом для работы IP-оборудования подавляющим большинством производителей был принят протокол, описанный МСЭ-Т в рекомендации H.323v2, стандартизирующей мультимедийную связь в сетях с коммутацией пакетов.

Пользователи мультимедийных персональных компьютеров с программным обеспечением H.323 могут подключиться к такой системе шлюзов. Вызовы при этом могут быть направлены на поддерживающие H.323 шлюзы других производителей. В результате данная система будет обеспечивать интеграцию речи, видео и данных в реальном времени для приложений по организации совместной работы в рабочих группах, например Microsoft NetMeeting.

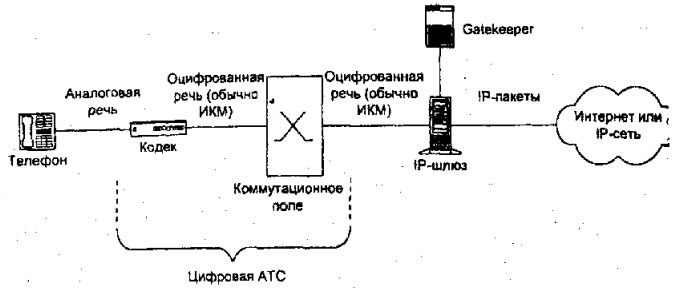

Рис. 3.3. Положение шлюза в сети IP-телефонии

Стандарты, отличные от H.323, используют в своей работе шлюзы CX950 Access Switch компании Memotec Comminications Inc., F-50 IP и F-200 IP компании Neura Communications Inc., VIP Gateway от Nortel Networks, сетевые станции Network Exchange 2201/2210 фирмы Netrix Corp.

Наличие механизмов резервирования ресурсов

Поддержка какой-либо схемы приоритезации (протокол резервирования RSVP или байт дифференциации услуг - DS byte) для осуществления возможности выбора приоритета между передаваемой речью или данными является важной характеристикой шлюза. При этом протокол RSVP позволяет маршрутизаторам придерживать часть полосы пропускания д организации голосового графика. У шлюзов IPT (Ericsson Inc.), Netblazer 8500 (Digi International), Packetstar IP Gateway 1000 (Lucent Technologies Inc.), Vocaltec Telephony Gateway (Vocaltec Communications Ltd.), Webphone Gateway Exchange (Netspeak Corp.) эта возможность отсутствует.

Поддержка основных телефонных интерфейсов J и типов сигнализаций

Важными критериями при оценке характеристик шлюзов является возможно большое разнообразие телефонных интерфейсов, поддерживаемых IP-шлюзом (El, PRI, BRI) и аналогового в частности, а также поддержка основных типов телефонной сигнализации: CAS, DTMF, PRI и ОКС №7. Существенную роль играет поддержка оборудованием механизмов безопасности в соответствии с Рекомендацией H.235.

Транспортные архитектуры

Диапазон транспортных архитектур, с которыми работают современные шлюзы, достаточно широк: выделенные линии, ISDN, Frame Relay, ATM, Ethernet. Шлюзы, поддерживающие передачу речи через Frame Relay, производят компании 3COM (Pathbuilder S200 Voice Access Switch), Cisco (серия 2600, 3600), Motorola (Vanguard

6560/6520), Newbridge Networks Corp. (MainStreetXpress 36100 VoIP Gateway) и другие. Режим ATM поддерживают шлюзы, выпускаемые фирмами Lucent Technologies (Packetstar IP Gateway 1000), Cisco (серия 2600, 3600), Ascend Communications (MultiVoice Gateway), Motorola Vanguard 6560/6520 Multiset-vice Access Device и другие.

Масштабируемость

Важной характеристикой шлюза является его масштабируемость, что обеспечивается модульным построением оборудования. На первом этапе развертывания сети IP-телефонии возможно использование неполного ресурса имеющихся портов при постепенном дальнейшем увеличении числа задействованных голосовых портов. При этом число портов соответствует количеству одновременных вызовов, которые может сделать шлюз, поскольку каждый ее порт оснащен собственным цифровым сигнальным процессором (DSP - Digital Signal Processor) для оцифровки голосовых сигналов.

Обеспечение факс-связью

Подавляющее большинство производимых шлюзов имеют возможность обеспечивать факсимильную связь на базе протокола IP. Она опирается на два основных стандарта, предложенных МСЭ-Т. Стандарт Т.37 сводит передачу факсов к доставке с промежуточным хранением, так как изображения факсов передаются в виде вложений электронной почты. Благодаря Т.37 факс-аппараты и факс-серверы на базе IP различных поставщиков могут взаимодействовать друг с другом так же согласованно, как и традиционные факсы. Еще один стандарт Т. 38 описывает передачу факсов в реальном времени либо посредством имитации соединения с факс-аппаратом, либо с помощью метода модуляции под названием FaxRelay. Т.38 может использоваться для реализации функциональности, более схожей с традиционной факсимильной связью, например для немедленного подтверждения.

Управление шлюзом

Шлюзы могут отличаться предусмотренными средствами управления. Данные средства управления имеют своей функцией маршрутизацию вызовов между шлюзами и перекодировку телефонных номеров в IP-адреса. Такими средствами оснащаются почти все шлюзы. Они конструктивно могут быть интегрированы со шлюзом или представлять собой отдельный мультимедийный менеджер конференций или многоголосовый менеджер доступа. Одним из решений является использование единого пакета, включающего в себя средства биллинга, маршрутизации вызовов и сетевого администрирования. Примером является шлюз компании Clarent (Clarent Carrier Gateway), взаимодействующий с пакетом Clarent Command Center, а также пакет Telephony Packet Network компании Northern Telecom Ltd. (Nortel).

Возможность установки различных алгоритмов кодирования речи

На показатели качества передаваемого голоса по IP-сети существенно влияет схема кодирования, используемая в шлюзе VoIP при сжатии голосовой информации. Наиболее распространена схема, обеспечивающая наибольшую степень сжатия информации и соответствующая спецификации G.723.1 (до 5,3 кбит/с). Применяются и другие схемы -

G.729a, G.711. Ci.726, G.728. При этом чрезвычайно важной является оснащение шлюза дополнительной установкой используемой схемы сжатия голоса. Для различных задач и при разных условиях владелец имеет возможность определить для работы шлюза тот или иной алгоритм кодирования. Такие шлюзы имеют многие компании: Lucent Technologies Inc. (Packetstar IP Gateway 1000), Hypercom Corp. (серия Integrated Enterprise Network), Memotec Communications Inc. (CX950 Access Switch), Netrix Corp. (сетевые станции Network Exchange 2201, 2210), Vocaltec Communications Ltd. (Vocaltec Telephony Gateway).

3.3. Классификация шлюзов IP-телефонии

Классификация шлюзов по области применения

Шлюзы IP-телефонии по масштабности применения можно разделить на два основных типа: шлюзы, ориентированные на корпоративное применение, и шлюзы, предназначенные для операторов и поставщиков услуг связи. Продукты последнего типа отличаются большой емкостью и масштабируемостью, присутствием средств аутентификации и мониторинга, а также дополнительных возможностей биллинга. Примерами таких устройств являются следующие шлюзы: IPTC компании Ericsson, PacketStar IP Gateway 1000 компании Lucent Technologies, MainStreetXpress 36100 от Newbridge, Hi-Gate 1000 компании EC1 Telecom, Clarent Gateway фирмы Clarent. Типовая инсталляция этих шлюзов предусматривает их подключение с одной стороны к IP-сети (например, через Ethernet-интерфейс), а с другой – к традиционной телефонной сети общего пользования (обычно по E 1 -каналам).

Исполнение шлюзов IP-телефонии

1. Автономные IP-шлюзы

Большинство производителей шлюзов предлагает автономные IP-шлюзы, которые обычно состоят из серверов на базе персональных компьютеров с комплектом голосовых плат. Голосовые платы не предназначены для компрессии/декомпрессии звука, поэтому данная операция должна выполняться главным процессором ПК.

Существуют шлюзы на базе ПК-серверов с платами с цифровой обработкой сигналов (Digital Signal Processing, DSP). Фирма Dialogic выпускает плату DM3 IP (с программным обеспечением от VocalTec); Micom - платы IP-телефонии для аналоговых линий, T-1 и E-1;| NMS - платы E-Fusion Inc., используемые многими разработчиками, в том числе Inter- Tel.| Оборудование этого типа производят также компании Vocaltec Communications Ltd., Neura Communications Inc., Netrix Corp. и другие. Автономные устройства могут стать хорошим решением для сетей, уже имеющих маршрутизаторы от различных производителей. Платы-маршрутизаторы, в свою очередь, применимы для дополнительного оснащения работающего оборудования функциями IP-телефонии.

2. Маршрутизаторы-шлюзы

В мире производителей оборудования телекоммуникаций намерилась тенденция к тому, что крупные компании традиционное сетевое оборудование оснащают узлами, отвечающими за IP-телефонию. Одной из первых в этом направлении стала работать компания Cisco Systems (устройства серии 2600 и 3600), за которой последовали другие фирмы (Memotec Comminications Inc. с машиной CX950 Access Switch, Motorola Inc. с устройством Vanguard). Эта продукция - маршрутизаторы и устройства доступа к распределенным сетям со встроенными шлюзами IP-телефонии - занимает отдельную,

важную нишу на рынке сетевого оборудования.

3. RAS-шлюзы

Свою часть рынка оборудования для IP-телефонии занимают шлюзы для VoIP, состоящие из плат, устанавливаемых в серверы дистанционного доступа (RAS). В этом направлении работают компании Ascend Communications и Digi International (устройства Multivoice Gateway и Netblazer 8500 соответственно). Усгановка устройств данного типа при построении IP-сетей оправдана при работе с приложениями с множеством голосовых портов и имеющими предельно важное значение.

4. Шлюзы-модули для УПАТС

В настоящее время получили распространение шлюзы IP-телефонии, предеставляющие собой конструктивно модули для классических учрежденческих АТС. Компании Lucent Technologies и Nortel Networks производят их для своих станций Defmity и Meridian I. Причем такая система перед тем, как установить соединение через IP-сеть, проверяет качество связи. В случае достаточного ее качества (норма устанавливается администратором системы), соединение устанавливается. Иначе, вызов направляется по традиционным линиям связи. Таким образом, налицо стремление фирм-производителей постепенно заменять транспортную среду, не затрагивая при этом телефонный сервис, предоставляемый конечным пользователям.

5. Шлюзы с интеграцией бизнес-приложений

По мере развития систем IP-телефонии на ведущие роли выходят сервис-функции. При этом оборудование должно ориентироваться не только на интеграцию трафика, но и на интеграцию бизнес-приложений, позволяющую повысить продуктивность работы предприятий. К таким продуктам следует отнести систему eBridge Interactive Web Responce компании eFusion, обеспечивающую интеграцию Web-служб и центров по обработке вызовов. Она позволяет реализовать службу типа "щелкни и говори" для установления телефонной связи между посетителями Web-узла компании и ее сотрудниками.

6. Учрежденческие АТС на базе шлюзов

Еще одно направление развития оборудования IP-телефонии - построение учрежденческих телефонных систем на базе инфраструктур ЛВС. Примерами такого оборудования могут послужить продукты фирм NBX (приобретена компанией 3COM) и Selsius (приобретена компанией Cisco Systems).

В случае, когда нецелесообразна установка отдельного сервера для преобразования телефонных сигналов в IP-пакеты, используются сетевые устройства, подключаемые напрямую к сети lOBaseT (по типу концентраторов Ethernet). При этом каждый концентратор представляет, по сути, небольшую УАТС с голосовой почтой и автоматическим секретарем, подключаемую через разъем RJ-14 к внешним и внутренним телефонным линиям и через гоединители RJ-45 к локальной сети Ethernet.

Обладая простотой управления и наличием встроенных средств компьютерно-телефонной интеграции эти системы в состоянии составить конкуренцию обычным учрежденческим АТС.

7. Сетевые платы с функциями телефонии

Одним из решений IP-телефонии являются многоцелевые сетевые платы с функциями телефонии (небольшие устройства типа Internet PhoneJACK от Quicknet Technologies, EtherPhone фирмы PhoNet Communications или крупные устройства типа

плат ATM от SphereCommunications). Такие устройства оборудованы портами RJ-11 для подключения обычног телефонного аппарата.

8. Автономные IP-телефоны

Представляют собой решение "все в одном" для одной линии. По внешнему виду и базовым сервисным возможностям аппаратные реализации IP-телефонов ничем особо не отличаются от обычных телефонов, но их электронная «начинка» позволяет существенно уменьшить нагрузку на персонал, отвечающий за телефонную связь. Такой тип продуктов предлагает компания Cisco Systems.

Помимо аппаратной существуют и программные реализации IP-телефонов. В этом случае персональный компьютер (ПК), оборудованный телефонной гарнитурой или микрофоном и акустическими системами, превращается в многофункциональный коммуникационный центр. Пользователь ПК, кроме доступа к обычному телефонному сервису, получает набор дополнительных возможностей: получение информации о звонящем клиенте (благодаря наличию стандартного интерфейса TAPI к другим программам), контроль за телефонными вызовами и работой с речевой почтой. Примером могут послужить программные продукты NetMeeting от Microsoft и IntemetPhone фирмы Vocaltec Communications. Недостатками систем является неполная совместимость с H.323 версии 2, а также отсутствие поддержки функций по обеспечению безопасности в работе с gatekeeper.

3.4. Архитектура системы на базе проекта TIPHOI

Недостатки архитектуры H.323

Основной недостаток архитектуры на базе стандарта H.323 заключается в сложности разработки и использования систем IP-телефонии. Охватывая несколько уровней модели OSI, H.323 структурно является довольно сложной рекомендацией, а некоторые ее места допускают неоднозначную трактовку.

Так, функции безопасности (согласно рекомендации H.235) определены в H.323 версии 2 как необязательные. Наличие механизмов аутентификации, шифрования и обеспечения целостности информации не исключается, но и не является необходимым условием чтобы считать продукт соответствующим H.323.

Согласно H.323, необязательной является и поддержка серии рекомендаций H.450, в которой определены механизмы предоставления дополнительных видов обслуживания, например, перевод и переадресация телефонных вызовов. Без поддержки H.450 подобные виды обслуживания будут невозможны в инфраструктуре IP-телефонии, построенной на базе продуктов разных производителей.

Упростить процесс внедрения технологии IP-телефонии призван проект TIPHON реализация которого позволит успешно решить задачи установления, модификации и завершения телефонных соединений, включая процессы межсетевого взаимодействия, управления безопасностью вызова, запроса качества обслуживания, шифрования, аутентификации и другие.

Функциональная модель TIPHON также состоит из трех компонентов – gatekeeper, шлюза и терминала, но шлюз разделен на три функциональных объекта. Это шлюз сигнализации (SG), транспортный шлюз (MG) и контроллер транспортного шлюза (MGC).

Шлюз сигнализации служит промежуточным звеном сигнализации между сетями IP и сетями на основе коммутации каналов (СКК). В задачи транспортного шлюза входят:

- преобразование и/или перекодирование передаваемой информации;
- обеспечение терминирования ИКМ-трафика, СКК и пакетного трафика;

• трансляция адресов;
• эхоподавление;
• воспроизведение различных сообщений для абонентов;
• прием и передача цифр кодом DTMF.

Контроллер MGC выполняет процедуры сигнализации H.323, которые определены в рекомендациях H.323, H.225 (RAS и Q.931) и H.245, и преобразует сообщения сигнализации СКК в сообщения сигнализации H.323. Основная его задача - управлять работой транспортного шлюза, т.е. осуществлять контроль за соединениями, использованием ресурсов, трансляцией протоколов.

Главная функция транспортного шлюза (MG) - преобразование ИКМ-трафика в IP-пакеты и наоборот. В качестве этого элемента могут использоваться разные устройства:

• шлюзы;
• серверы доступа;
• системы передачи ATM;
• серверы интерактивных речевых сообщений.

Смоделированный на основе трех описанных элементов шлюз воспринимается внешними элементами как единая система. Причем эти три элемента могут не быть физически разделены, однако такое разделение дает определенные преимущества.

Решение с тремя шлюзами позволяет обрабатывать большее количество вызовов, так как при этом функции разделены по отдельным процессорам.

Gatekeeper отвечает за контроль и управление объектами сеги: выполняет преобразование адресов (например, телефонных номеров в соответствующие IP-адреса H.323 и обратно) и маршрутизацию вызовов.

Gatekeeper в модели TIPHON поддерживает все те функции, которые определены для него в стандарте H.323. Но, помимо этого, gatekeeper отвечает за:

• тарификацию;
• взаиморасчеты;
• составление отчетов по использованию ресурсов;
• управление.

Разработанная в рамках проекта TIPHON модель сеги, состоящая из функциональных элементов и интерфейсов между ними, показана на рис. 3.4.

Чтобы соответствовать рекомендациям TIPHON, продукты должны поддерживать следующие интерфейсы:

• интерфейс D - предназначен для маршрутизации вызовов между контроллерами зоны (gatekeeper);
• интерфейс C - для взаимодействия между шлюзом (MGC) и контроллером зоны;
• интерфейс N - определяет особенности взаимодействия между объектами MGC и MG.

Контроллер и шлюз обмениваются информацией при создании, модификации и разрыве соединений; определении требуемого формата информации; включении в поток тональных сигналов и различных речевых уведомлений; запросе ответов но событиям, связанным с прохождением информационного потока. Показанные на рис 3.4 службы поддержки могут быть использованы для аутентификации, биллинга, преобразования адресов и других задач.

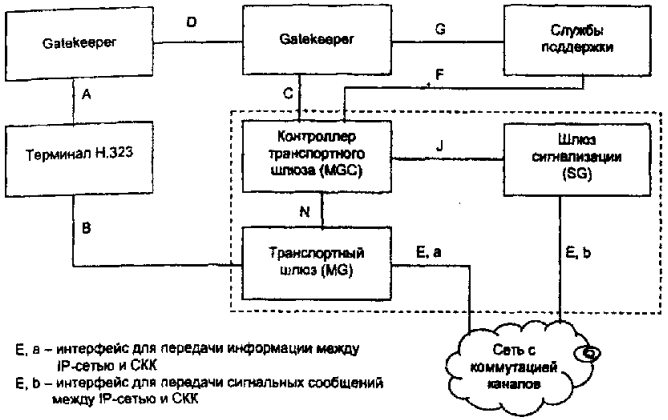

Рис. 3.4. Функциональная архитектура, предложенная в рамках проекта TIPHON

Глава 4

СИГНАЛИЗАЦИЯ В СЕТЯХ IP-ТЕЛЕФОНИИ

4.1. Общие принципы сигнализации в сетях IP-телефонии

Для обеспечения широкомасштабного внедрения IP-телефонии одним из самых важных факторов является обеспечение совместимости систем разных фирм. Достижение совместимости возможно только на базе стандартных протоколов сигнализации. Протоколы сигнализации обеспечивают установление, администрирование и завершение сеанса связи между конечными точками (пользователями), однозначно идентифицируемыми заданной схемой адресации. Понятие «сигнализация» относится ко всей информации, связанной с вызовами и необходимой для их установления, маршрутизации, мониторинга и завершения как на физическом, так и на логическом уровне.

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: установление соединения, передача речи или данных и разъединение. Сообщения системы сигнализации инициируют и завершают эти фазы, а стандартные контрольные сигналы и (или) записанные голосовые сообщения информируют абонента о характере прохождения его вызова.

Во всех современных сетях с коммутацией каналов система сигнализации основана на семействе ОКС №7. Они обеспечивают обмен сообщениями, которые необходимы для маршрутизации вызовов, резервирования ресурсов, трансляции адресов, установления соединений, управления ими, выставления счетов. Кроме того, на взаимоувязанной сети связи Российской Федерации используется еще много других систем сигнализации (аналоговых и цифровых).

По сравнению с сигнализацией в обычных телефонных сетях сигнализация IP-телефонии должна обладать более широкими возможностями в силу специфики конечных узлов. Они могут иметь самые разные характеристики в части требуемой полосы пропускания, кодирования/декодирования аудиосигналов, передачи данных и т.д., и для установления сеанса связи между ними необходимо убедиться в совместимости этих характеристик.

В системах IP-телефонии процедуры управления вызовами выполняются протоколами сигнализации, а непосредственная маршрутизация трафика через IP-сеть обеспечивается протоколами: OSPF или BGP (резервирование сетевых ресурсов возможно, например, при помощи протокола RSVP). Таким образом, архитектура сети IP-телефонии предусматривает Разделение плоскостей управления и передачи пользовательской информации, что является наиболее благоприятным условием для внедрения новых услуг (рис. 4.1).

В настоящее время еще окончательно не решен вопрос выбора оптимальной архитектуры управления вызовами особенно для Интернет-телефонии: должна ли она быть интегрирована с существующими службами Интернет или развернута отдельно для обеспечения управления в режиме реального времени. Первый подход привлекает Интернет-провайдеров, которые рассматривают услуги Интернет-телефонии лишь как небольшую часть своего сервисного пакета. Они планируют предлагать эти услуги по фиксированным тарифам, используя максимально упрощенную схему управления услугами. За второй подход ратуют операторы, для которых Интернет-телефония является основной или даже единственной предлагаемой услугой. Им необходимы системы, способные обеспечить высокий уровень контроля за использованием сетевых ресурсов и

мощные средства биллинга.

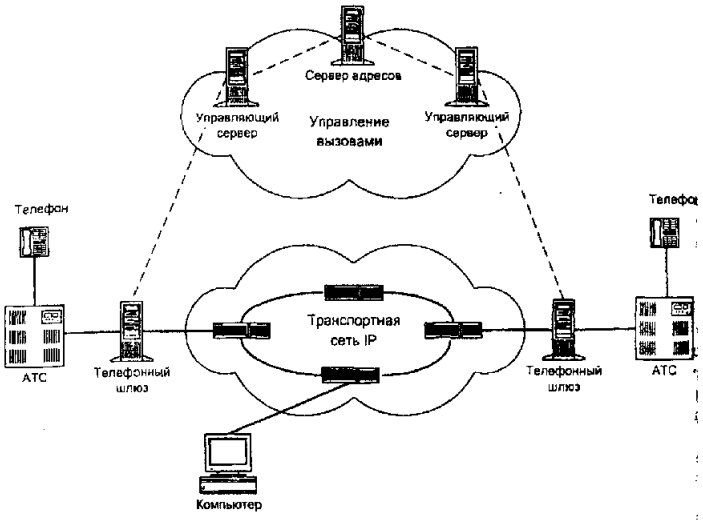

Рис. 4.1. Управление вызовами в сети IP-телефонии

Еще один важный вопрос, связанный с сигнализацией в IP-телефонии - контроль за доступом к сети. В обычной телефонной сети общего пользования (ТфОП) абонент подключается к АТС через фиксированный местный шлейф, поэтому идентифицировать его телефонный аппарат очень просто. В сети IP-телефонии все гораздо сложнее, поскольку существует множество разных способов доступа к ней: с обычного телефона через ТфОП, по модемному соединению через сервер удаленного доступа, через ЛВС и территориально распределенную сеть и т.д. Кроме этого, пользователи могут перемещаться между различными сетями, таким образом, абонента нельзя идентифицировать по используемой им линии доступа.

Для эффективного контроля за доступом оператор должен аутентифицировать каждого пользователя, запрашивающего услугу. С увеличением числа операторов IP-телефонии требуются также средства контроля за трафиком на границе между их сетями.ё Такие средства должны осуществлять контроль за доступом и использованием сетевых ресурсов и выполнением соглашений по качеству обслуживания. При их отсутствии оператору может оказаться проблематичным гарантировать пользователю определенный класс обслуживания, если его график частично проходит через сеть другого оператора.

На рис. 4.2 показано место механизмов сигнализации IP-телефонии в протокольном стеке: над ними находятся приложения, под ними - транспортные службы IP. Приложение может представлять собой телефонный шлюз.

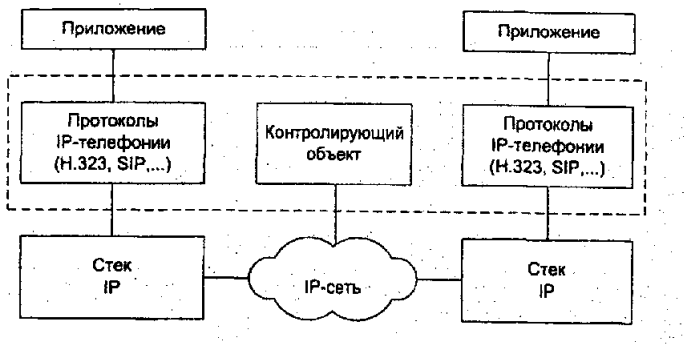

Рис. 4.2. Механизмы сигнализации IP-телефонии в протокольном стеке

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

- найти gatekeeper, на котором возможна регистрация оконечного устройства;
- зарегистрировать свой мнемонический адрес на gatekeeper;
- указать требуемую полосу пропускания;
- передать запрос на установление соединения;
- установить соединение;
- в процессе вызова управлять параметрами соединения;
- разъединить соединение.

Для выполнения этих операций в настоящее время могут использоваться различные протоколы сигнализации, рассмотренные ниже.

4.2. Сигнализация по стандарту H.323

Рекомендация Международного союза электросвязи (МСЭ-Т) H.323 определяет основы процесса передачи аудио, видео и данных по сетям с коммутацией пакетов, например по сетям IP. В ней описаны объекты, необходимые для мультимедийной связи, их функции и способы взаимодействия, в частности алгоритмы формирования пакетов, сжатия аудио- и видеоинформации. Кроме того, рекомендация H.323 нацелена на решение задач администрирования конечных пользователей, адресации, контроля за использованием полосы пропускания сети и сетевых объектов.

В настоящее время действительна версия 2 H.323 - это зонтичная рекомендация, в которой описаны компоненты сети и даны рекомендации к применению множества дополнительных рекомендаций. Все вместе эти рекомендации часто называют семейством H.32 (рис. 4.3).

Сейчас готовится следующая версия стандарта. В ней будут описаны: создание пакетных сетей факсимильной связи и организация связи между H-323-шлюзами. Речь идет и о таких функциях, распространенных в современной телефонии, включая уведомление о поступлени второго вызова и режим справки. Некоторые компании добиваются включения в H.323 поддержки мультимедиа-возможностей, основанных на предложенном IETF протоколе Session Initiation Protocol. Помимо «телефонных» функций, новая версия будет дополнена средствам» позволяющими учитывать параметры сеансов для целей тарификации, а также поддержка каталогов - вместо цифровых IP-адресов

можно будет пользоваться именами абонентов.

Для выполнения действий сигнализации между шлюзами и gatekeeper в соответствии Рекомендацией МСЭ-Т Н.323 должны использоваться следующие протоколы:

- сигнализация RAS (Registration, Admission, Status);
- сигнализация Q.931 (согласно Н.225.0);
- протокол управления Н.245.

Сигнализация RAS

Протокол сигнализации RAS (регистрации, подтверждения и состояния) применяетеся для передачи служебных сообщений между терминалами и контроллером зоны Н.323. RAS сообщения служат для регистрации терминалов, допуска их к сеансу связи, изменения используемой полосы пропускания, информирования о состоянии сеанса и его прекращении. В отсутствии контроллера зоны (gatekeeper) протокол RAS не задействуется.

Функции сигнализации RAS используют сообщения протокола Н.225.0. Канал сигнализации RAS не зависит от канала управления вызовом и канала управления Н.245.

С помощью сигнализации RAS должно осуществляться:

- нахождение gatekeeper, на котором возможна регистрация оконечного оборудования;
- регистрация оконечного устройства;
- определение географического положения оконечного устройства;
- указание необходимой полосы пропускания;
- изменение полосы пропускания.

Передача сообщений RAS осуществляется в дейтаграммах UDP. Для адресации RAS должна использоваться адресная информации, в которую входят:

- сетевой адрес оборудования;
- идентификатор TSAP (Transport Layer Service Access Point);
- мнемонический адрес (Alias Address).

Сетевой адрес является адресом в формате, используемом в сети с коммутацией пакетов, например, адрес в форматах IPv4, IPv6, IPX, NetBIOS.

Идентификатор TSAP используется для идентификации информационных потоков, отправленных с одного сетевого адреса. Для gatekeeper выделены постоянные значения идентификатора TSAP: 1718 (для поиска gatekeeper) и 1719 (для передачи сообщений сигнализа ции RAS).

Мнемонический адрес служит для адресации оконечного оборудования в удобной пользователю форме. Адресом может быть телефонный номер в формате E.I 64, телефонный номер в корпоративной сети, адрес электронной почты и т.д. Gatekeeper не имеет мнемонического адреса.

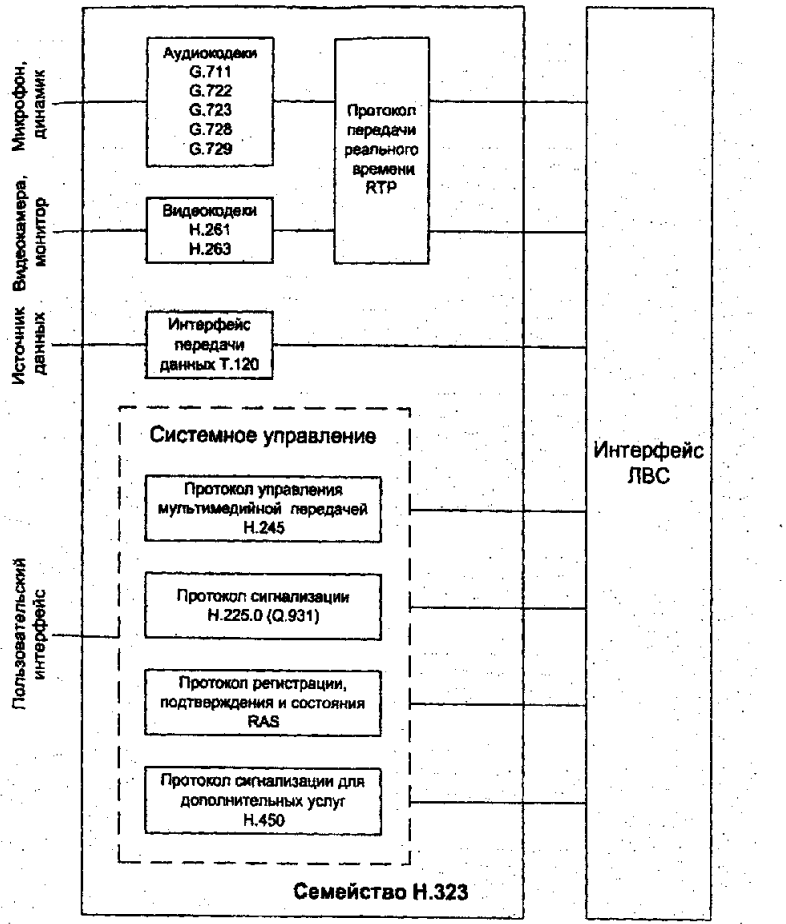

Рис. 4.3. Совокупность рекомендаций H.323

Нахождение gatekeeper должно осуществляться с помощью широковещательного запроса GRQ (Gatekeeper Request), передаваемого оконечным оборудованием с идентификатором TSAP, равным 1718. Если gatekeeper найден, и он готов обслужить запрос от оконечнного оборудования, в ответ оно должно получить сообщение GCF (Gatekeeper Confirm). Если оконечное оборудование получило ответ от нескольких gatekeeper, выбор одного из них должен осуществляться оконечным оборудованием произвольным образом. Если gatekeeper не может обслужить запрос от оконечного оборудования, то в ответ он должен передать сообщение GRJ (Gatekeeper Reject), в котором должна сообщаться причина отказа, и может содержаться адрес альтернативного gatekeeper. При нахождении gatekeeper между ним и оконечным оборудованием осуществляется установление логического канала сигнализации, по которому будут передаваться остальные сообщения RAS (рис. 4.4).

После нахождения gatekeeper оконечное оборудование в сообщении RRQ (Registration Request) должно сообщить gatekeeper свой сетевой и мнемонический адрес. В ответ gatekeeper должен передать сообщение RCF (Registration Confirm) для подтверждении регистрации оконечного оборудования, либо RRJ (Registration Reject) в случае отказа от регистрации. Сообщение RRQ может передаваться при включении оконечного оборудования. Если при повторной регистрации мнемонический и сетевой адреса, переданные gatekeeper оконеченым оборудованием, совпадают с ранее переданными, то gatekeeper должен передать сообщение RCF. Если при повторной регистрации мнемонический адрес равен ранее указанному, а сетевые отличаются, должно быть передано сообщение RRJ с причиной отказа «duplicate registration». Для отмены регистрации используются сообщения URQ (Unregistered Request), передаваемое оконечным оборудованием, и UCF (Unregistered confirm), URJ (Unregistered reject) передаваемые gatekeeper оконечному оборудованию.

Регистрация оконечного оборудования на gatekeeper может осуществляться один раз и не повторяться при включении оконечного оборудования. В этом случае gatekeeper должен определять состояние оконечного оборудования. Для этого gatekeeper должен периодически передавать сообщение IRQ (Information Request). Интервал определяется производителями оборудования и должен быть не менее 10 секунд.

После регистрации оконечного оборудования на gatekeeper оно может установить соединение с вызываемым оконечным оборудованием. Для этого оконечное оборудование-инициатор должно передать сообщение ARQ (Admissions Request) и установить логический канал для передачи сообщений Q.931. В сообщении ARQ указываются скорость передачи, кратная 100 бит/с, и количество каналов, необходимых для передачи речевой информации. Например, при использовании интерфейсов ISDN для выделения полосы 192 кбит/с необходимо указать значения соответственно 640 и 3. Скорость указывается без учета размеров заголовков пакетов и блоков данных транспортных протоколов. Если сеть может обеспечить требуемые параметры, то gatekeeper должен передать подтверждение ACF (Admissions Confirm), в противном случае передается сообщение ARJ (Admissions Reject) с указанием причины отказа.

После получения подтверждения оконечное оборудование устанавливает соединение с вызываемым оконечным оборудованием с использованием сигнализации Q.931 (в соответствии с H.225.0). Сообщения сигнализации Q.931 могут передаваться по логическому каналу через gatekeeper или непосредственно между двумя оконечными устройствами. Выбор способа осуществляет gatekeeper и сообщает об этом оконечному оборудованию в сообщении ACF.

Если сообщения передаются через gatekeeper, то он может либо закрыть логический канал после установления соединения для передачи речевой информации, либо остановить его до конца сеанса связи, если поддерживаются дополнительные услуги.

Для установления соединения используются сообщения Setup и Connect, после передачи которых устанавливается канал управления H.245. Канал для передачи информации управления H.245 может быть установлен двумя способами: через gatekeeper или непосредственно между оконечными устройствами. В случае, если логический канал сигнализации Q.931 устанавливается через gatekeeper, то канал для передачи информации управления H.245 также должен устанавливаться через gatekeeper. Способ установления канала для передачи информации управления H.245 между оконечным оборудованием в настоящее время не специфицирован.

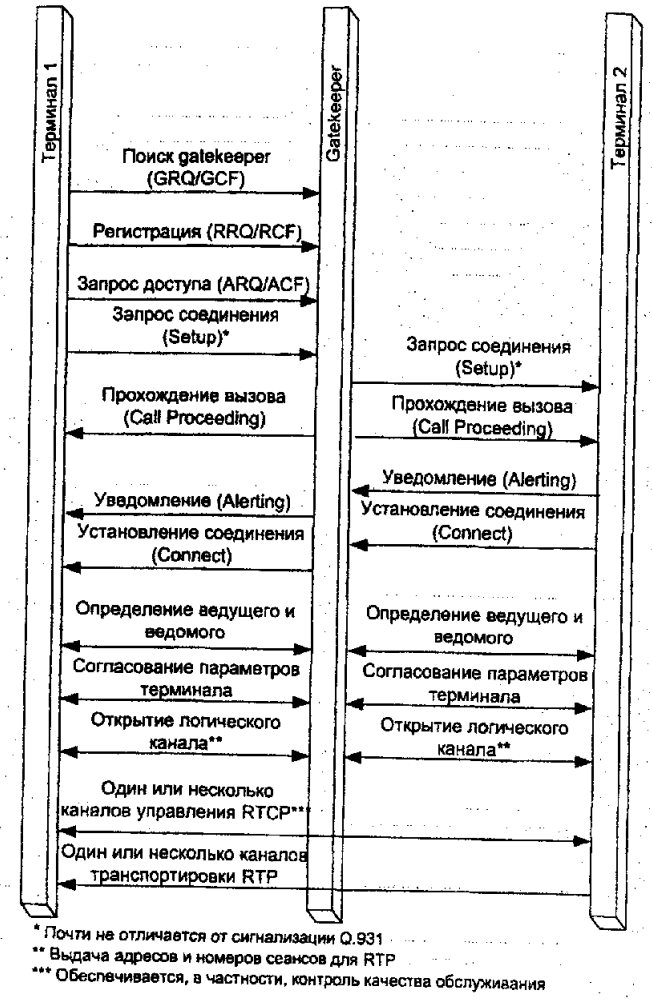

Рис. 4.4. Этапы прохождения вызова в среде H.323

Если канал сигнализации RAS установлен, то он может использоваться для установления нескольких соединений. Идентификация сообщений сигнализации, принадлежащих одному и тому же соединению, осуществляется с помощью идентификатора Call ID.

Сигнализация H.225.0 (Q.931) и протокол управления H.245

Стандарт H.225 описывает протоколы сигнализации и формирования пакетов в системах пакетной передачи мультимедийного графика. Канал управления вызовами

H.225.0 пользуется для установления и разрыва соединений между двумя терминалами H.323, а также между теминалом и шлюзом. Служебные сообщения этого протокола передаются поверх TCP или UDP (рис. 4.5). Соответствующий механизм H.225.0 основан на протоколе 0.931, который был разработан для сетей ISDN. Он обеспечивает предоставление целого ряда, дополнительных видов обслуживания и возможность взаимодействия с сетями, базирующимися на коммутации каналов. Канал управления вызовом не зависит от канала RAS и канала управления H.245.

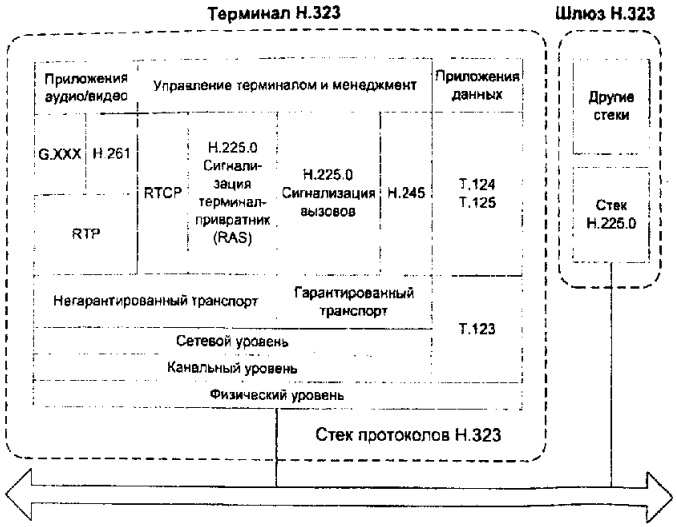

Рис. 4.5. Положение H.225.0 в стеке протоколов H.323

Рекомендация H.245 определяет синтаксис и семантику терминальных сигнальных сообщений, а также процедур, которые используются для передачи их в полосе разговора в начале или в течение сеанса связи. Определены процедуры подтверждения сигнальной информации для обеспечения гарантии надежной передачи аудиовизуальной информации и данных.

Рекомендация охватывает широкий диапазон приложений, включая хранение/повторную передачу, передачу сообщений и распределение услуг, а также обеспечение диалога. Это применимо к системам передачи всех видов информации, которые используют методы мультиплексирования, определенные в Рекомендациях H.222.0, H.223 и H.225.0.

Протокол управления мультимедийной передачей H.245 обеспечивает:

- согласование возможностей компонентов;
- установление и разрыв логических каналов;
- передачу запросов на установление приоритета;
- управление потоком (загрузкой канала);
- передачу общих команд и индикаторов.

Сообщения протокола H.245 передаются по специальному каналу управления. Это логический канал «О», который, в отличие от каналов обмена мультимедиа-потоками,

постоянно открыт. Обмен параметрами между терминалами позволяет согласовывать режимы работы и форматы кодирования информации, что обеспечивает взаимодействие терминалов от разных производителей. В процессе обмена сообщениями о параметрах уточняются возможности терминалов принимать и передавать различные виды графика.

С помощью сигнализации Q.931 согласно рекомендации МСЭ-Т Н.225.0 и протоколу управления Н.245 должно осуществляться:

- передача запроса на установление соединения;
- инициализация соединения и обмен информацией о возможностях;
- установление соединения для передачи речевой информации;
- разъединение соединения.

Для установления соединения инициатор вызова (оконечное оборудование 1) должно передать сообщение Setup оконечному оборудованию 2 по логическому каналу сигнализации с идентификатором TSAP, равным 1719.

В ответ получатель (оконечное оборудование 2) должен передать сообщение Connect, сообщающее инициатору о готовности установить соединение. Инициатор сообщения должен получить сообщения Call proceeding, Connect, Alerting в течении 4 секунд.

После получения сообщения Connect должен быть установлен логический канал управления Н.245, по которому передается информация о возможностях оконечного оборудования в сообщении terminal Capability Set.

Для определения инициатора установления канала RTP используется идентификатор status Determination Number в сообщении Master Slave Determination.

После инициализации соединения создается логический канал для передачи речевой информации. Установление канала для передачи речевой информации осуществляется оконечным оборудованием после получения сообщения open Logical Channel по каналу управления Н.245. Передача речевой информации по логическому каналу должна осуществляться в пакетах RTP. Передача управляющей информации должна осуществляться в пакетах RTCP.

При необходимости изменить требуемую полосу пропускания используется сообщение BRQ (Bandwidth Change Request) сигнализации RAS, которое может передаваться как gatekeeper, так и оконечным оборудованием. Если изменение полосы пропускания невозможно, то посылается сообщение BRJ (Bandwidth Reject). Если изменение возможно, то передается сообщение BCF (Bandwidth Confirm).

Уменьшение полосы пропускания возможно всегда, а для увеличения полосы пропускания свыше значения, указанного в последнем сообщении ARQ, оконечное оборудование должно закрыть все логические каналы и открыть их заново. Логический канал должен быть закрыт сообщением close Logical Channel протокола управления Н.245, а открыт с повыми параметрами сообщением open Logical Channel.

Соединение разъединяется следующим образом:

- инициатор разъединения должен закрыть канал сообщением close Logical Channel, передаваемым по каналу управления Н.245;
- инициатор разъединения должен передать сообщение end Session Command, передаваемым по каналу управления Н.245;
- удаленное оборудование дожидается сообщения end Session Command, передаваемое по каналу управления Н.245;
- если логический канал сигнализации Q.931 открыт, он закрывается сообщением Release Complete.

Если в системе присутствует Gatekeeper, то он должен освободить ранее выделенную полосу пропускания. Освобождение полосы пропускания осуществляется сообщением DRQ (Disengage Request) сигнализации RAS, передаваемым оконечным оборудованием. В ответ должно быть получено сообщение подтверждения DCF

(Disengage Confirm) или сообщение отказа DRJ (Disengage Reject).

Сигнализация H.450

Дополнительные услуги в сетях IP-телефонии определяет семейство рекомендаций H.450. Так, 450.1 описывает протокол сигнализации между двумя компонентами сети, позволяющий предоставлять дополнительные услуги, а 450.2 - механизмы услуги трансформации вызова (Call Transfer), благодаря которой соединение между терминалами А и Б преобразуется в соединение между Б и В. Дополнительная услуга Call Diversion, которую определяет H.450.3, предоставляет возможность переадресовать вызов в тех случаях, когда вызываемый абонент занят, не отвечает или когда предварительно установлен соответствующий параметр.

4.3. Сигнализация на основе протокола SIP

Протокол SIP (Session Initiation Protocol) является протоколом прикладного уровня, разработанным рабочей группой по управлению многоточечными сеансами мультимедиа-связи (MMUSIC) организации IETF (Рекомендация RFC 2543). Он позволяет организовать и провести такой сеанс, обеспечивая его установление, модификацию и завершение.

При организации мультимедийного сеанса используется два основных метода для нахождения и информирования заинтересованных участников:

• уведомление о сеансе с использованием разных средств - электронной почты, новостных групп, Web-страниц или специального протокола SAP (Session Announcement Protocol);

• приглашение к участию в сеансе с помощью протокола SIP.

Для установления сеансов одноадресного вещания, которое характерно при IP-телефонии, основным протоколом установления соединений является протокол SIP. SIP работает по схеме клиент-сервер (рис. 4.6): клиент запрашивает определенный тип сервиса, а сервер обрабатывает его запрос и обеспечивает предоставление сервиса. Согласно протоколу SIP, пользовательская система может не только формировать, но и принимать запросы. Это означает, что она должна быть оснащена и клиентской (клиент агента пользователя - UAC) и серверной (сервер агента пользователя - UAS) частями.

Обработка вызовов осуществляется сервером SIP, который может работать в режиме непосредственного установления связи или в режиме переадресации. В обоих режимах сервер принимает запросы на определение местоположения нужного пользователя, но если в первом режиме он сам доводит вызов до адресата, то во втором - возвращает адрес конечного пункта запрашиваемому клиенту.

В протоколе SIP определены два вида сигнальных сообщений - запрос и ответ. Они имеют текстовый формат (кодировка символов согласно RFC 2279) и базируются на протоколе HTTP (синтаксис и семантика определены в RFC 2068). В запросе указываются процедуры, вызываемые для выполнения требуемых операций, а в ответе - результаты их выполнения.

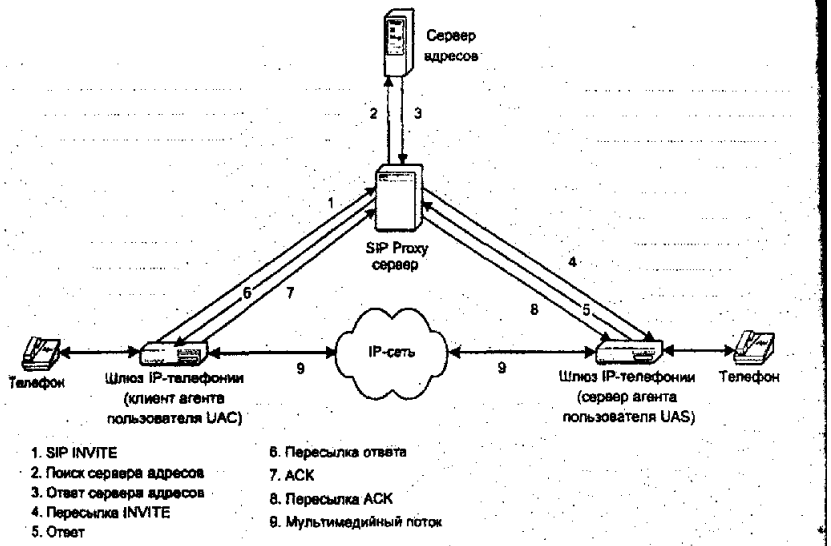

Рис. 4.6. Схема сигнализации по протоколу SIP

Определены шесть процедур:

• INVITE - приглашает пользователя принять участие в сеансе связи (служит для установления нового соединения; может содержать параметры для согласования);

• BYE - завершает соединение между двумя пользователями;

• OPTIONS - используется для передачи информации о поддерживаемых характеристиках (эта передача может осуществляться напрямую между двумя агентами пользователей или через сервер SIP);

• ACK - используется для подтверждения получения сообщения или для положительного ответа на команду INVITE;

• CANCEL - прекращает поиск пользователя;

• REGISTER - передает информацию о местоположении пользователя на сервер SIP, который может транслировать ее на сервер адресов (Location Server).

Оба протокола SAP и SIP используют механизм SDP (Session Description Protocol) для описания характеристик сеанса: время проведения, требуемые ресурсы и т.д. (Рекомендация RFC 2327). SDP используется исключительно для текстового описания сеанса и не имеет ни транспортных механизмов, ни средств согласования требуемых для сеанса параметров. Эти функции должны выполнять протоколы, применяемые для передачи информации SDP.

Сообщения-ответы могут содержать шесть типов возможных результатов: запрос в процессе выполнения (1xx), успешный запрос (2xx), переадресация (3xx), неправильный запрос (4xx), отказ сервера (5xx) и глобальный отказ (6xx).

Используемая в SIP адресация основана на унифицированном указателе ресурсов SIP URL, в котором может быть записано имя домена (user@domain) или IP-адрес (user@IPadess) пользователя. Цель использования подобного формата - интеграция SIP-услуг с существующими службами Интернет. Сервер имен доменов (DNS) преобразует доменные имена в IP-адреса конечной точки (рис. 4.7). Вся маршрутизация и передача мультимедийных потоков выполняется нижележащей IP-сетью. Таким образом, услуги

SIP хорошо интегрируются в традиционную модель Web-коммуникаций с сервером DNS, обеспечивающим преобразовав доменного имени в сетевой адрес.

Предназначенный для инициации сеансов протокол SIP обеспечивает определение адреса пользователя и установление соединения с ним. Кроме этого, он служит основой для применения других протоколов, реализующих функции защиты, аутентификации, описании канала мультимедийной связи и т.д. Для биллинга, например, может использоваться прокол Radius.

В работах над протоколом SIP участвуют ведущие производители сетевого и телекоммуникационного оборудования (Cisco Systems, Lucent Technologies, 3Com) и крупнейшие операторы (AT&T, MC1, Level 3). О своих планах по его поддержке заявили и многие компании, в частности, CableLabs, Telcordia, General Instrument, Com21.

Примером реализации протокола SIP может служить программная платформа Convergence Server Solutions фирмы Dynamicsoft, включающая следующие продукты:

- SIP Proxy Server - маршрутизатор между конечными точками, каждая из которых определена как UAC или UAS; в дополнение к функциям обеспечения взаимодействия между различными серверами платформы он предоставляет услуги перенаправления и регистрации/определения местоположения пользователей;
- SIP Location Server обеспечивает безопасную сигнализацию вызовов, хранит информацию о пользователях, необходимую сервис-провайдерам для гибкого управления доступом пользователей и маршрутизации вызовов с целью предоставления наилучшего качества услуги;
- SIP User Agent - управляет соединениями между исходящей и входящей сторонами обеспечивая поддержку необходимого качества услуг;
- SIP CallAccounting Server - выполняет функции сбора и обработки информации в виде детальных отчетов о транзакциях TDR, получаемых от SIP Proxy Server, которая в дальнейшем может быть использована в системах биллинга и менеджмента пользователей.

4.4. Сравнение протоколов H.323 и SIP

Протоколы H.323 и SIP представляют существенно различные подходы к решению одних и тех же задач: если H.323 близок к традиционным системам сигнализации (с коммутацией каналов на основе протокола Q.931 или более ранних рекомендаций серии H), то SIP Реализует более простой, интернетовский подход на основе HTTP.

Следует отметить, что стандарт H.323 не решает проблемы, связанные с защитой вызова от несанкционированного доступа, взаимодействием между шлюзами и gatekeeper разных сетей, между телефонами и персональными компьютерами, роумингом и интеграцией телефонной сигнализацией ОКС №7. Протокол H.323 может лишь гарантировать взаимодействие типа шлюз-шлюз и телефон-телефон, поскольку ориентирован на транспортные сервисы в середине сети и не способен что-либо улучшить на уровне конечных узлов. Он не предусматривает каких-либо средств, облегчающих разработку новых приложений. Алгоритмы H.323 не оптимизированы для реальных сетей, они сложны в реализации и требуют больших ресурсов на клиентской стороне. Тем не менее, рекомендация неплохо подходит для популярных сегодня магистральных приложений IP-телефонии в виде Интернет-телефонии, обеспечивающих существенное снижение расходов на междугородную и международную связь

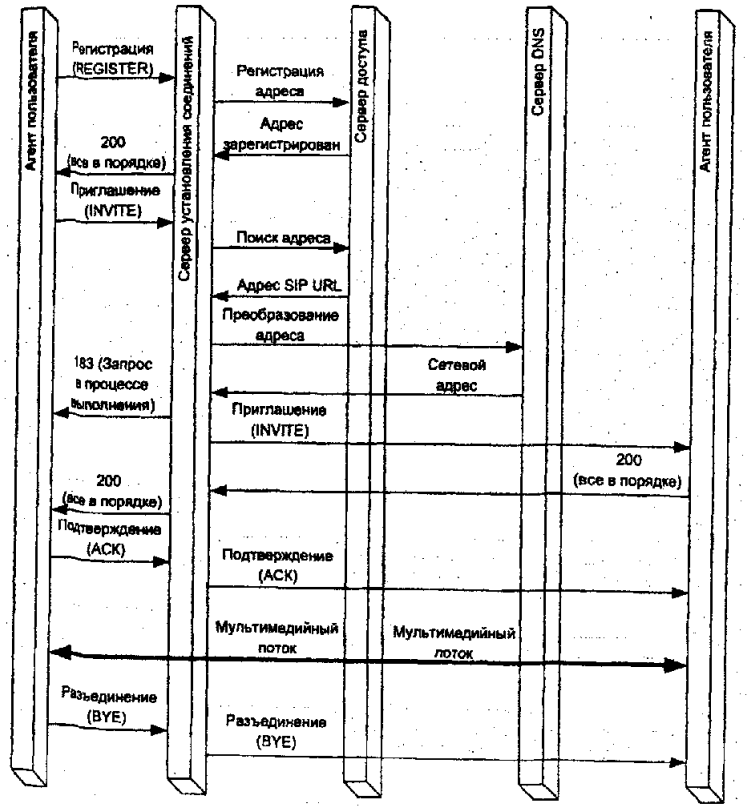

Рис. 4.7. Возможный сценарий установления и завершения сеанса связи по протоколу S1P

По сравнению с H.323 протокол SIP базируется на текстовом формате, более прост для реализации и добавления новых функций. Простота SIP не означает скудность его функциональных возможностей. Протокол обеспечивает реализацию важных для систем Интернет телефонии функций, включая шифрование и аутентификацию. То, что SIP базируется на архитектуре клиент-сервер, позволяет обеспечить управление вызовами на уровне сервера (подобное невозможно в одноранговых схемах обслуживания вызовов, используемых большинством конечных точек H.323). В настоящее время предложены спецификации, которые расширяют протокол SIP средствами управления безопасностью вызова, запроса качества обслуживания, сигнализации изменения состояния сети.

Систему объектов H.323 можно рассматривать как прикладную сеть, наложенную на сеть передачи данных (IP-сеть), в то время как службы SIP ориентированы на интеграцию со службами Интернет. Какой из вариантов более предпочтителен, зависит от требуемых функциональных возможностей и целей бизнеса.

Технология H.323 предоставляет больше возможностей по управлению конкретной услугой в части аутентификации и учета и контроля за использованием сетевых ресурсов Возможности протокола SIP здесь значительно меньшие. Выбор этого протокола

компанией-поставщиком услуг фактически означает, что технологическая интеграция услуг для нее важнее возможностей гибкой тарификации и контроля за использованием сетевых ресурсов.

В целом можно сделать вывод, что протокол SIP ориентирован на Интернет-провайдеров, которые рассматривают услугу Интернет-телефонии лишь как небольшую часть своего сервисного пакета. Будучи самодостаточной, технология H.323 больше подходи для корпоративных сетей (интранет) и поставщиков услуг IP-телефонии, для которых данные услуги не являются доминирующими. В целом H.323 и SIP не следует рассматривать как конкурирующие технологии, они являются различными подходами, предназначенными для разных сегментов рынка. Они могут работать параллельно и даже взаимодействовать через специальный пограничный шлюз.

4.5. Особенности сигнализации по концепции TIPHON

Базируясь на стандарте H.323 для IP-сети, спецификация TIPHON дополняет его некоторыми обязательными процедурами, а также механизмами взаимодействия с сетями коммутации каналов. Функциональная модель TIPHON состоит из тех же компонентов-gatekeeper, шлюза и терминала, - что и модель H.323, однако в ней предусмотрено разделение шлюза на три функциональных объекта. Это шлюз сигнализации (SG – SignallingGate way) транспортный шлюз (MG - Media Gateway) и контроллер транспортного шлюза (MGC - Media Gateway Controller) (рис. 4.8).

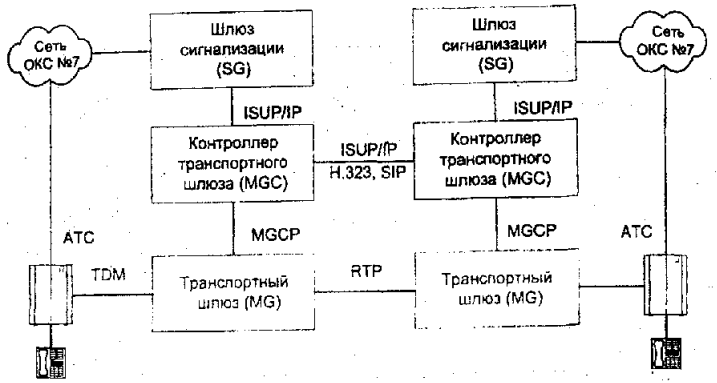

Рис. 4.8. функциональная модель сети по проекту TIPHON

Шлюз сигнализации служит промежуточным звеном сигнализации между сетями с пакетной и канальной коммутацией. В задачи транспортного шлюза входит преобразование и/или перекодирование передаваемой информации; он обеспечивает терминирование ИКМ-трафика телефонных сетей и пакетного графика, транслирует адреса, подавляет эхо, воспроизводит различные сообщения для абонентов, принимает и передает цифры кодом DTMF и т.д. Контроллер сигнализации MGC выполняет процедуры сигнализации H.323, которые определены в рекомендациях H.323, H.225 (RAS и Q.931) и H.245, и преобразует сообщения сигнализации телефонных сетей в сообщения сигнализации H.323. Основная его задача - управлять работой транспортного шлюза, т.е. осуществлять контроль за соединениями, использованием ресурсов, трансляцией

протоколов и т.п. Следует отметить, что MGC не обеспечивает управление вызовами. Это задачи gatekeeper, который выполняет их в соответствии с рекомендациями H.323.

При использовании сигнализации ОКС №7 в контроллер MGC по IP-сети будут передаваться сообщения ISUP (подсистемы обслуживания вызовов сети ISDN). Если же применяется сигнализация по выделенному каналу (CAS), сигнальные сообщения сначала вместе с информацией абонента поступят в транспортный шлюз, а затем уже будут выделены в контроллер MGC. При этом предполагается использовать протокол MDTP (Multi-Network Datagram Transmission Protocol), который служит для инкапсуляции телефонных протоколов сигнализации (ISUP, CAS, PRI) и передачи переносимой ими информации в контроллер транспортного шлюза.

MGC анализирует информацию сигнализации и передает управляющую информацию в транспортный шлюз посредством специального протокола управления, в задачи которого входит обеспечение управления различными ресурсами (системой интерактивного речевого отклика, мостами конференцсвязи и т.д.), приемом и формированием сигналов DTMF, формированием тональных сигналов (готовности к набору номера, контроля посылки вызова «занято» и пр.), эхо-подавлением, использованием кодеков (G.711, G.723.1, G.729, т.д.), сбором статистики, тестированием конечных точек (например, испытания по шлейфу резервированием, разъединением и блокировкой конечных точек, шифрованием.

Протокол управления транспортными шлюзами MGCP представляет собой достатоно простой протокол клиент-сервер. Логика управления вызовами выполняется агентом (Call Agent), находящимся вне транспортного шлюза. Сам же транспортный шлюз представляется в виде объекта, состоящего из конечных точек - точек входа/выхода информационных потоков и соединений - двух или более соединенных конечных точек. Модель определяет физические конечные точки (например, окончания соединительных линий) и виртуальные конечные точки (например, аудиоисточники). Сам протокол MGCP использует принцип «ведущий/ведомый», согласно которому агент управления вызовами передает транспортному шлюзу команды для управления конечными точками и соединениями, а также инициации определенных действий.

MGCP является достаточно универсальным протоколом, способным обеспечить распределенное управление различными типами транспортных шлюзов, в частности телефонными шлюзами и серверами доступа. Он может использоваться для установления соединения и выполнения разных функций обслуживания, например тестирования шлейфа.

Дальнейшим развитием протокола MGCP является протокол управления вызовами Megaco (Media Gateway Control), известный также как стандарт ITU H.248, который определяет взаимодействие, с одной стороны, шлюза между разными средами передачи данных (Media Gateway, MG) и, с другой, - контроллера шлюзов между средами передачи данных (Media Gateway Controller, MGC) (рис. 4.9). Иными словами, Megaco разработан для внутридоменного удаленного управления устройствами, отвечающими за установление соединения или проведение сеанса связи, включая шлюзы VoIP, серверы удаленного доступа мультиплексоры цифровых абонентских линий (Digital Subscriber Line Access Multiplexer, DSLAM), маршрутизаторы с поддержкой многопротокольной коммутации с использованием меток (Multiprotocol Label Switching, MPLS), оптические кросс-коннекторы, модули агрегирования сеансов PPP и другие.

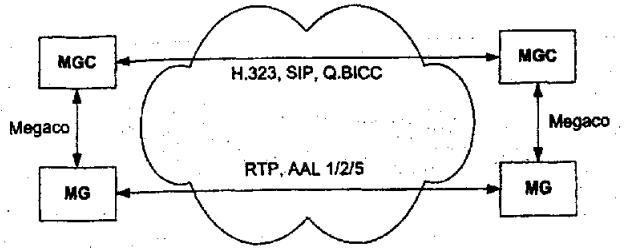

Рис. 4.9. Использование протокола Megaco в сети IP-телефонии

MGCP и Megaco - эти сравнительно низкоуровневые протоколы управления устройствами, которые сообщают шлюзу, каким образом связать потоки, поступающие в сеть с коммутацией пакетов или ячеек, с потоками пакетов или ячеек, переносимыми, например, транспортным протоколом реального времени (Real-Time Transport Protocol, RTP). По существу, Megaco повторяет MGCP в отношении архитектуры и взаимодействия контроллера со шлюзом, но при этом Megaco поддерживает более широкий диапазон сетевых технологий, в том числе ATM.

Типичным примером работы протокола MGCP является проверка состояния конечной точки на предмет снятия трубки (которую поднимает абонент, чтобы сделать звонок). После фиксации события «снятие трубки» шлюз сообщает об этом контроллеру, после чего последний может послать шлюзу команду подать в линию непрерывный гудок и ждать тональных сигналов DTMF набираемого номера абонента. После получения номера контроллер решает, по какому маршруту следует направить вызов, и, используя протокол сигнализации между контроллерами, в том числе H.323, SIP или Q.BICC, взаимодействует с оконечным контроллером. Оконечный контроллер дает соответствующему шлюзу указание подать звонок на вызываемую линию. Когда этот шлюз определяет, что вызываемый абонент снял трубку, оба контроллера дают соответствующим шлюзам команды на установление двухсторонней голосовой связи по сети передачи данных. Таким способом данные протоколы распознают состояния конечных точек, уведомляют об этих состояниях контроллер, генерируют в линии сигналы (например, непрерывный гудок), а также формируют потоки данных между подключенными к шлюзу конечными точками и сетью передачи данных, например потоки RTP.

Протоколы MGCP и Megaco очень похожи друг на друга, и для многих приложений не имеет значения, какой из них будет использоваться. Однако Megaco лучше интегрирован с приложениями с поддержкой нескольких сред передачи, чем MGCP, потому что в базовый протокол включены семантические элементы для конференций. Благодаря этому MGCP может быть лучшей основой для приложений, не привязанных к какой-либо среде, например для управления сеансами на базе MPLS.

Следует отметить, что вопрос о принятии Megaco в качестве международного стандарта для приложений с различными средами передачи данных является пока открытым, хотя некоторые производители приступили к внедрению данного протокола в свои продукты. Подтверждением этого является то, что в конце августа 2000 г. в лаборатории функциональной совместимости университета Нью-Гемпшира проводилось тестирование уже более десяти независимых разработок, использующих протокол Megaco.

4.6. Межсетевое взаимодействие

При внедрении систем IP-телефонии часто необходимо решать задачу обеспечения эффективного взаимодействия сетей различных операторов. Здесь существует масса проблем, связанных с преобразованием адресов между административными доменами, взаиморасчетами между операторами, контролем доступа к ресурсам сети, защитой внутренней топологии и т.д. Успешное решение данных задач должна обеспечивать соответствующая система сигнализации IP-телефонии.

В третьей версии рекомендаций H.323 появилось приложение G к H.225. В нем описан метод взаимодействия административных доменов с помощью объекта, называемого «пограничным элементом» (Border Element). Этот функциональный элемент поддерживает открытый доступ к административному домену для доведения вызова до входящего в этот домен узла или предоставления других услуг, требующих установления мультимедиасвязи с его узлами.

Взаимодействие между пограничными элементами осуществляется посредством протокола, который определен в приложении G. Он может быть использован с целью обмена Длинами нумерации и тарификационной информацией, сведениями для авторизации и маршрутизации вызовов, отчетами об использовании сетевых ресурсов.

Подобные функции межсетевого взаимодействия реализованы и в проекте TIPHON На рис. 4.10 показан пример передачи сигнальной информации между терминалом и шлюзом, расположенными в различных административных доменах.

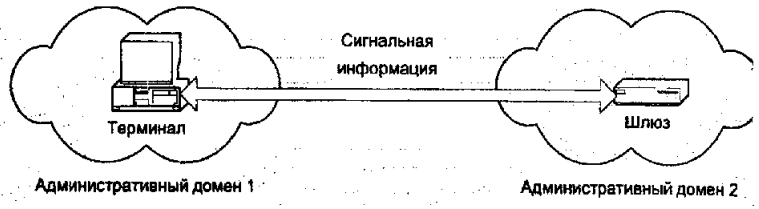

Рис. 4.10. Пример взаимодействия двух доменов

В сценарии, показанном на рис. 4.11, ресурсы зоны H.323 (терминал, шлюз и сервер авторизации), требуемые для реализации вызова IP-телефонии, разделены между тремя административными доменами. В рассматриваемом случае два домена (первый и второй) имеют установленных сигнальных отношений, но каждый должен иметь сигнальные отношения с третьим доменом, в котором расположен центр авторизации. На рис. 4.11 показаны следующие потоки информации:

S 1: Обмен информацией разрешения запроса между терминалом и gatekeeper 1.

S2: Обмен информацией разрешения запроса между gatekeeper 1 и сервером авторизации.

S3: Обмен информацией разрешения запроса между gatekeeper 1 и шлюзом.

S4: Обмен информацией разрешения запроса между шлюзом и его gatekeeper.

S5: Обмен информацией разрешения запроса между gatekeeper 2 и сервер от третьего лица.

S6: Обмен информацией разрешения запроса между gatekeeper 1 и gatekeeper 2.

Следует особо отметить, что реализация передачи сигнальной информации между различными административными доменами в сети IP-телефонии требует обеспечения соответствующей степени защиты информации.

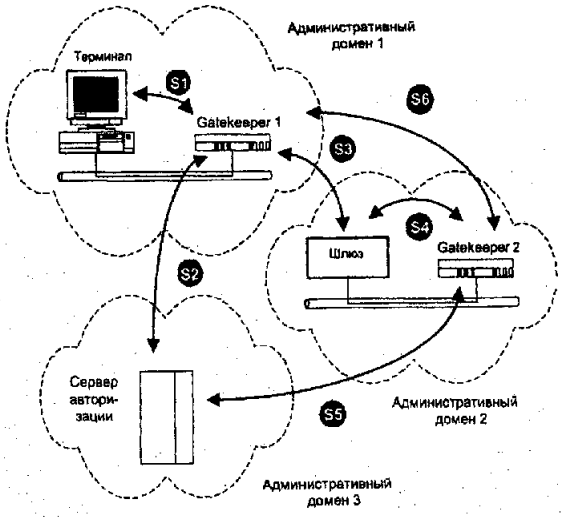

Рис. 4.11. Пример взаимодействия трех доменов

Глава 5

АДРЕСАЦИЯ В СЕТЯХ IP-ТЕЛЕФОНИИ

5.1. Нумерация в телефонных сетях общего пользования

В настоящее время нумерация в сетях общего пользования с коммутацией каналов предоставляющих услуги телефонной связи (телефонные сети, сети ISDN, интеллектуальные сети, сотовые сети и др.), реализуется в соответствии с Рекомендацией ITU-T E.164.

Система нумерации таких сетей включает **международный и национальные планы нумераций.**

Каждая телефонная Администрация разрабатывает национальный план нумераций для своей сети. Этот план разрабатывается таким образом, чтобы любой абонент национальной сети может быть доступен по одному и тому же номеру для разных услуг. Причем это должно выполняться для всех входящих международных вызовов. Национальный план нумерации страны должен быть такой, чтобы анализ цифры не превышал установленные пределы, применимые к национальному (значащему) номеру N(S)N.

Международный номер телекоммуникационной сети общего пользования включает различное число десятичных цифр, объединенных в соответствующие поля. Структура международного номера телекоммуникационной сети общего пользования показана на рис. 5.1.

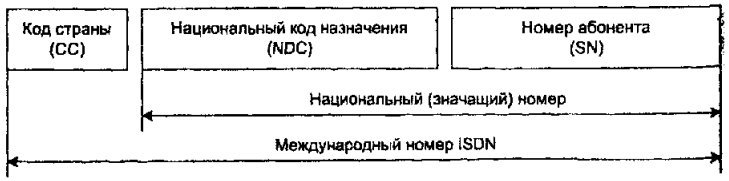

Рис. 5.1. Структура международного номера сети общего пользования

Поле «Код страны (CC)» используется для определения страны или географической области назначения. Данный код имеет различную длину, конкретные значения кодов для стран мира приведены в Рекомендации ITU-T E.I 64. Следует отметить, что код страны начинается с номера мировой зоны нумерации. В настоящее время территория всего земного шара разделена на 9 мировых зон нумерации:

Зона 1 - Северная Америка;
Зона 2 - Африка;
Зоны 3 и 4 - Европа;
Зона 5 - Центральная и Южная Америка;
Зона 6 - Австралия и Океания;
Зона 7 - Россия и Казахстан;
Зона 8 - Юго-Восточная Азия;
Зона 9 - Азия.

Поле «Национальный (значащий) номер N(S)N» используется для определения конкретного абонента в сети. При выборе требуемого абонента иногда необходимо определить еще и сеть назначения. В этом случае национальный код включает поле национального кода назначения (NDC). Национальный код назначения может иметь различную длину в зависимости от требований национальных Администраций.

Поле «Номер абонента SN» также имеет произвольную длину в каждой национальной сети согласно Рекомендации ITU-T E.I 60.

Следует отметить, что общая длина международного номера в настоящее время не должна превышать 15 цифр. При этом в данную длину номера не входят префиксы, символы, адресные ограничители (например, окончание импульсных сигналов), так как они не являются частью международного номера сети общего пользования.

5.2. Адресация в IP-сетях

Типы адресов в IP-сетях

Каждый терминал в сети TCP/IP имеет адреса трех уровней:

1. *Физический (MAC-адрес)* - локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети - это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-AO-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем. Для узлов, входящих в глобальные сети, включая X.25 или frame relay, локальный адрес назначается администратором глобальной сети.

2. *Сетевой (IP-адрес)*, состоящий из 4 байт, например, 109,26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла номер сети может быть выбран администратором произвольно или назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами.

Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае, узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

3. *Символьный (DNS-имя)* - идентификатор-имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне, например, в протоколах FTP или telnet.

Три основных класса IP-адресов.

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например: в 128.10.2.30 - традиционная десятичная форма представления адреса, Ц 10000000 00001010 00000010 00011110 - двоичная форма представления этого же-

адреса. На рис. 5.2 показана структура IP-адреса. чН

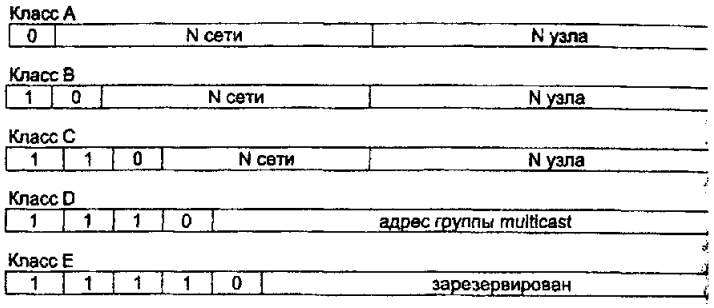

Рис. 5.2. Структура IP-адреса

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

- Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезвирован для специальных целей, о чем будет сказано ниже.) В сетях класса A количечество узлов должно быть больше 216 , но не превышать 224.
- Если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов 28-216. В сетях класса B под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта.
- Если адрес начинается с последовательности 110, то это сеть класса C с числом узлов не больше 28. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов.
- Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

В табл. 5.1 приведены диапазоны номеров сетей, соответствующих каждому классу сетей

Таблица 5.1. Диапазоны номеров IP-сетей

Класс	Наименьший адрес	Наибольший адрес
A	01.0.0	126.0.0.0
C	128.0.0.0	191.255.0.0
E	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.	247.255.255.255

Отображение физических адресов на IP-адреса

В протоколе IP-адрес узла, то есть адрес компьютера или порта маршрутизатора, назначается произвольно администратором сети и прямо не связан с его локальным адресом, как это сделано, например, в протоколе IPX. Подход, используемый в IP, удобно использовать в крупных сетях и по причине его независимости от формата локального адреса, и по причине стабильности, так как в противном случае, при смене на компьютере сетевого адаптера эти изменения должны бы были учитывать все адресаты всемирной сети Internet (в том случае, конечно, если сеть подключена к Internet).

Локальный адрес используется в протоколе IP только в пределах локальной сети при обмене данными между маршрутизатором и узлом этой сети. Маршрутизатор, получив пакет для узла одной из сетей, непосредственно подключенных к его портам, должен для передачи пакета сформировать кадр в соответствии с требованиями принятой в этой сети технологии и указать в нем локальный адрес узла, например его MAC-адрес. В пришедшем пакете этот адрес не указан, поэтому перед маршрутизатором встает задача поиска его по известному IP-адресу, который указан в пакете в качестве адреса назначения. С аналогичной задачей сталкивается и конечный узел, когда он хочет отправить пакет в удаленную сеть через маршрутизатор, подключенный к той же локальной сети, что и данный узел.

Для определения локального адреса по IP-адресу используется протокол разрешения адреса *Address Resolution Protocol, ARP*. Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети - протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети, или же протокол глобальной сети (X.25, Frame Relay), как правило, не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу - нахождение IP-адреса по известному локальному адресу. Он называется реверсивный ARP - *RARP (Reverse Address Resolution Protocol)* и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

В локальных сетях протокол ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP-адресом.

Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения Узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP-запросе отправитель указывает свой локальный адрес. ARP-запросы и ответы используют один и тот же формат пакета. Так как локальные адреса могут в различных типах сетей иметь различную длину, то формат пакета протокол ARP зависит от типа сети. На рис. 5.3 показан формат пакета протокола ARP для передачи по сети Ethernet.

В поле типа сети для сетей Ethernet указывается значение 1. Поле типа протокола позволяет использовать пакеты ARP не только для протокола IP, но и для других сетевых протоколов. Для IP значение этого поля равно 0800_{16}.

Длина локального адреса для протокола Ethernet равна 6 байтам, а длина IP-адреса - 4 байтам. В поле операции для ARP запросов указывается значение 1 для протокола ARP для 2 протокола RARP.

Узел, отправляющий ARP-запрос, заполняет в пакете все поля, кроме поля искомого локального адреса (для RARP-запроса не указывается искомый IP-адрес). Значение этого поля заполняется узлом, опознавшим свой IP-адрес.

Тип сети		Тип протокола
Длина локального адреса	Длина сетевого адреса	Операция
Локальный адрес отправителя (байты 0-3)		
Локальный адрес отправителя (байты 4-5)		IP-адрес отправителя (байты 0-1)
IP-адрес отправителя (байты 2-3)		Искомый локальный адрес (байты 0-1
Искомый локальный адрес (байты 2-5)		
Искомый IP-адрес (байты 0-3) а		

Рис.5.3. Формат пакета протокола ARP

В глобальных сетях администратору сети чаще всего приходится вручную формировать ARP-таблицы, в которых он задает, например, соответствие IP-адреса адресу узла сети X.25, который имеет смысл локального адреса. В последнее время наметилась тенденция автоматизации работы протокола ARP и в глобальных сетях. Для этой цели среди всех маршрутизаторов, подключенных к какой-либо глобальной сети, выделяется специальный маршрутизатор, который ведет ARP-таблицу для всех остальных узлов и маршрутизаторов этой сети. При таком централизованном подходе для всех узлов и маршрутизаторов вручную нужно задать только IP-адрес и локальный адрес выделенного маршрутизатора. Затем и каждый узел и маршрутизатор регистрирует свои адреса в выделенном маршрутизаторе, а при необходимости установления соответствия между IP-адресом и локальным адресом узел обращается к выделенному маршрутизатору с запросом и автоматически получает ответ без участия администратора.

Отображение символьных адресов на IP-адреса

Служба DNS (Domain Name System) - это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен - в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет - то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос или передать его другому DNS-серверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов

сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого *доменным пространством имен*, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:

- corn - коммерческие организации (например, microsoft.com);
- edu - образовательные (например, mit.edu);
- gov - правительственные организации (например, nsf.gov);
- org - некоммерческие организации (например, fidonet.org);
- net - организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим *полным доменным именем (fully qualified domain name, FQDN)*, которое включает имена всех доменов по направлению от хоста к корню. Пример полного DNS-имени: citint.dol.ru.

Автоматизация процесса назначения IP-адресов

Как уже было сказано, IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора утомительную процедуру. Ситуация усложняется еще тем, что многие пользователи не обладают достаточными знаниями для того, чтобы конфигурировать свои компьютеры для работы в интерсети и должны поэтому полагаться на администраторов.

Протокол динамической настройки хоста *Dynamic Host Configuration Protocol (DHCP)* был разработан для того, чтобы освободить администратора от этих проблем. Основным назначением DHCP является динамическое назначение IP-адресов. Однако, кроме динамического, DHCP может поддерживать и более простые способы ручного и автоматического статического назначения адресов.

В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP-серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула наличных IP-адресов без вмешательства оператора. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом по-прежнему как и при ручном назначении, существует постоянное соответствие. Оно устанавливается момент первичного назначения сервером DHCP IP-адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP-адреса) другими компьютерами. Динамическое разделение адресов позволяет строить IP-

сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP-адресов.

DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределнием. Администратор управляет процессом назначения адресов с помощью параметра «продолжительности аренды» (lease duration), которая определяет, как долго компьютер может использовать назначенный IP-адрес, перед тем как снова запросить его от сервера DHC в аренду.

Примером работы протокола DHCP может служить ситуация, когда компьютер, являющийся клиентом DHCP, удаляется из подсети. При этом назначенный ему IP-адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес. Ни пользователь, ни сетевой администратор не вмешиваются в этот процесс. Это свойство очень важно для мобильных пользователей.

Протокол DHCP использует модель клиент-сервер. Во время старта системы компьютер-клиент DHCP, находящийся в состоянии «инициализация», посылает сообщение discover (исследовать), которое широковещательно распространяется по локальной сети и передается всем DHCP-серверам частной интерсети. Каждый DHCP-сервер, получивший это сообщение отвечает на него сообщением offer (предложение), которое содержит IP-адрес и конфигурационную информацию.

Компьютер-клиент DHCP переходит в состояние «выбор» и собирает конфигурационные предложения от DHCP-серверов. Затем он выбирает одно из этих предложений, переходит в состояние «запрос» и отправляет сообщение request (запрос) тому DHCP-серверу, чье предложение было выбрано.

Выбранный DHCP-сервер посылает сообщение DHCP-acknowledgment (подтверждение), содержащее тот же IP-адрес, который уже был послан ранее на стадии исследования, а также параметр аренды для этого адреса. Кроме того, DHCP-сервер посылает параметры сетевой конфигурации. После того, как клиент получит это подтверждение, он переходит в состояние «связь», находясь в котором он может принимать участие в работе сети TCP/IP. Компьютеры-клиенты, которые имеют локальные диски, сохраняют полученный адрес для использования при последующих стартах системы. При приближении момента истечения срока аренды адреса компьютер пытается обновить параметры аренды у DHCP-сервера, а если этот IP-адрес не может быть выделен снова, то ему возвращается другой IP-адрес.

В протоколе DHCP описывается несколько типов сообщений, которые используются для обнаружения и выбора DHCP-серверов, для запросов информации о конфигурации, для продления и досрочного прекращения лицензии на IP-адрес. Все эти операции направлены на то чтобы освободить администратора сети от утомительных рутинных операций по конфигурированию сети.

Однако использование DHCP несет в себе и некоторые проблемы. Во-первых, это проблема согласования информационной адресной базы в службах DHCP и DNS. Как известно, DNS служит для преобразования символьных имен в IP-адреса. Если IP-адреса будут динамически изменятся сервером DHCP, то эти изменения необходимо также динамически вносить в базу данных сервера DNS. Хотя протокол динамического взаимодействия между службами DNS и DHCP уже реализован некоторыми фирмами (так называемая служба Dynamic DNS), стандарт на него пока не принят.

Во-вторых, нестабильность IP-адресов усложняет процесс управления сетью. Системы управления, основанные на протоколе SNMP, разработаны с расчетом на статичность IP-адресов. Аналогичные проблемы возникают и при конфигурировании фильтров маршрутизаторов, которые оперируют с IP-адресами.

Наконец, централизация процедуры назначения адресов снижает надежность системы: при отказе DHCP-сервера все его клиенты оказываются не в состоянии получить IP-адрес и другую информацию о конфигурации. Последствия такого отказа могут быть уменьшены

путем использовании в сети нескольких серверов DHCP, каждый из которых имеет свой пул IP-адресов.

Служба каталогов на базе протокола LDAP

Протокол LDAP (Lightweight Directory Access Protocol - упрощенный протокол доступа к каталогам) является стандартом доступа к службам сетевых каталогов, а протокол DHCP используется для динамического присвоения IP-адресов пользователям для доступа к сетевым ресурсам. Как заявляют компании-разработчики, объединение этих двух технологий поможет разрешить некоторые серьезные проблемы, присущие протоколу TCP/IP, например, управление адресами, разработку стратегии безопасности и одновременное использование информации об адресах (на что не способны DHCP-серверы).

Протокол LDAP упрощает работу в сетевой среде. Так, пользователи получают возможность входить в систему с любого узла сети и работать с привычными для себя настройками, поскольку информация о них будет сохраняться в основанном на LDAP каталоге. В будущем основанные на LDAP каталоги могут применяться для поддержки инфраструктуры интрасетей и Internet. Например, службы типа системы именования доменов (DNS) и DHCP будут использовать серверы каталогов на базе LDAP в качестве своих хранилищ информации. Тогда эти службы приобретут дополнительные достоинства - модульную структуру и независимость от места размещения.

Протокол LDAP специально предназначен для использования с управляющими и браузерными приложениями, которые обеспечивают интерактивный доступ к каталогам с возможностью чтения и записи. LDAP - это протокол взаимодействия клиента и сервера, обеспечивающий доступ к службе каталогов и работающий непосредственно поверх протокола TCP/IP.

Набор API-интерфейсов протокола LDAP достаточно прост. Протокол становится одним из наиболее предпочтительных для работы с каталогами в Internet. Поскольку уже более 40 компаний обеспечивают поддержку LDAP в своих продуктах или заявили о таком намерении, этот протокол быстро завоевывает себе популярность и получает все более широкое распространение. В настоящее время серверы LDAP выпускаются компаниями Microsoft, Netscape Communications, Lucent Technologies, ISODE, Critical Angle, Novell, Banyan Systems и др. Некоторые браузеры Web, например Netscape Communicator, имеют встроенный клиент LDAP.

Применяемая в LDAP информационная модель основана на схеме, использована в протоколе X.500, которая, в свою очередь, базируется на «именных записях». Именные записи обозначают либо реальные объекты, например какого-нибудь пользователя, либо некоторую сетевую службу, например службу преобразования адресов. Каждая запись сопровождается атрибутами, имеющими одно или несколько значений, и хранит информанию, которую при необходимости можно найти. Как правило, каталог на базе LDAP поддерживает репликацию, что повышает надежность и увеличивает быстродействие системы.

Система именования доменов (DNS) нужна для того, чтобы компьютеры могли находить друг друга в сети. С помощью коммуникационных протоколов служба DHCP распространяет информацию об IP-адресах и другие сведения среди клиентов сети; обычно это делается при запуске системы. Службу DHCP можно настроить таким образом, чтобы временно присваивать клиентам динамические адреса из некоторого банка свободных адресов переназначать эти адреса по мере необходимости.

Автоматическое присвоение IP-адреса требует относительно тесной связи между серверами DNS и DHCP, установленными на данном узле сети. Эта связь необходима, поскольку, присваивая клиенту IP-адрес, сервер DHCP должен иметь возможность обновления информации о соответствии имени клиента присвоенному ему адресу.

Совмещение технологий DHCP и DNS с возможностями каталогов на базе LDAP r зволит добиться как минимум следующих преимуществ:

- доступ к информации - новая система позволит организовать стандартный метод доступа для поиска и сохранения данных в информационном хранилище серверов DHCP и DNS;
- гибкость построения сети - поскольку сетевой протокол LDAP способен работать на различных платформах, появляется возможность размещения серверного хранилища информации на других машинах;
- репликация - уже сейчас многие поставщики встраивают функции репликации в создаваемые ими службы каталогов на базе LDAP; в будущем они еще больше расширятся, так как комитет IETF начинает разрабатывать стандартный протокол LDAP возможностью репликации.

Главная цель объединения серверов - дать пользователям возможность встраивать в их системы управления сетевыми адресами средства повышения надежности, безопасности синхронизации имен и адресов.

Процесс взаимодействия серверов LDAP и DHCP показан на рис. 6.4. Клиент посылает запрос на доступ в Internet с указанием нужного адреса и ресурса. Сервер DHCP автоматически присваивает клиенту IP-адрес и связывает пользователя с ресурсами в каталоге LDAP. Сервер LDAP находит указанные ресурсы и автоматически соединяет пользователя с сооветствующим узлом сети.

Как и DNS, LDAP - это служба каталогов в архитектуре клиент-сервер. Каталоги могут содержать самую разную информацию, например, базу данных пересчета телефонных номеров E.1 64 в IP-адреса для пользователей IP-телефонии. Составляющие дерево каталога LDAP данные хранятся на одном или более серверах LDAP. Если при обращении клиента LDAP, например шлюза IP-телефонии, сервер не может ответить на запрос, то во всяком случае он может возвратить ему указатель на другой сервер LDAP, где запрашиваемая информация может быть найдена.

Рис. 5.4. Процесс взаимодействия серверов DHCP и LDAP

Адресация в IPv6

Одним из основных отличий внедряемого в настоящее время протокола IPv6 от протокола IPv4 является использование более длинных адресов. Адреса получателя и источника в IPv6 имеют длину 128 бит или 16 байт. Версия 6 обобщает специальные типы адресов версии 4 в следующих типах адресов:

- Unicast - индивидуальный адрес. Определяет отдельный узел - компьютер или порт маршрутизатора. Пакет должен быть доставлен узлу по кратчайшему маршруту.
- Cluster - адрес кластера. Обозначает группу узлов, которые имеют общий адресный префикс (например, присоединенных к одной физической сети). Пакет должен быть маршрутизирован группе узлов по кратчайшему пути, а затем доставлен только одному из членов группы (например, ближайшему узлу).
- Multicast - адрес набора узлов, возможно в различных физических сетях. Копии пакета должны быть доставлены каждому узлу набора, используя аппаратные

возможности групповой или широковещательной доставки, если это возможно.

Как и в версии IPv4, адреса в версии IPv6 делятся на классы, в зависимости от значения нескольких старших бит адреса.

Большая часть классов зарезервирована для будущего применения. Наиболее интересным для практического использования является класс, предназначенный для провайдеров услуг Internet, названный *Provider-Assigned Unicast*.

Адрес этого класса имеет следующую структуру:

Идентификатор провайдера	Идентификатор абонента	Идентификатор подсети	Идентификатор узла

Каждому провайдеру услуг Internet назначается уникальный идентификатор, которым помечаются все поддерживаемые им сети. Далее провайдер назначает своим абонентам уникальные идентификаторы и использует оба идентификатора при назначении блока адресов абонента. Абонент сам назначает уникальные идентификаторы своим подсетям и узлам этих сетей.

Абонент может использовать технику подсетей, применяемую в версии IPv4, для дальнейшего деления поля идентификатора подсети на более мелкие поля.

Описанная схема приближает схему адресации IPv6 к схемам, используемым в территориальных сетях, включая телефонные сети или сети X.25. Иерархия адресных полей позволит магистральным маршрутизаторам работать только со старшими частями адреса, оставляя обработку менее значимых полей маршрутизаторам абонентов.

Под поле идентификатора узла требуется выделения не менее 6 байт, для того чтобы можно было использовать в IP-адресах MAC-адреса локальных сетей непосредственно.

Для обеспечения совместимости со схемой адресации версии IPv4, в версии IPv6 имется класс адресов, имеющих 0000 0000 в старших битах адреса. Младшие 4 байта адреса этого класса должны содержать адрес IPv4. Маршрутизаторы, поддерживающие обе версии адресов, должны обеспечивать трансляцию при передаче пакета из сети, поддерживающей адресацию IPv4, в сеть, поддерживающую адресацию IPv6, и наоборот.

5.3. Проблемы адресации в сетях IP-телефонии

В системах IP-телефонии, так же как и в сетях с коммутацией каналов, номера в соответствии с Рекомендацией E.I 64 используются конечными пользователями, чтобы идетифицировать вызов. В IP-системах, когда конечный пользователь идентифицируется терминалом, номер E.I 64 этого конечного пользователя временно связан с адресом IP (транспортный адрес) этого терминала (оконечной точки). Проблема нумерации в сети IP-телефонии связана с определением точки назначения вызова при внутридоменной и междоменной связи в IP-сети. В качестве такой конечной точки может выступать или IP-терминал с соответствующим приложением пользователя или шлюз для доступа в сеть с коммутацией каналов.

От решения задач адресации в IP-телефонии во многом зависят удобство пользования услугой, работа алгоритмов маршрутизации, обеспечение мобильности номеров и т.д. Главная проблема организации взаимодействия сетей с коммутацией каналов и IP-сетей заключается в том, что единственный метод адресации обычного терминала абонента телефонной сети - это использование номера этого терминала (в сетях общего пользования номера E.I 64). Вопрос преобразования номера сети с коммутацией каналов в IP-адрес представляется пока еще достаточно сложным и разрабатывается не только рабочей группой 4 в рамках проекта TIPHON, но и другими

организациями, например IETF. В то же время ITU-T только подходит к решению вопросов взаимодействия услуг IP-телефонии и ТфОП, ограничивается пока рассмотрением функций межсетевого взаимодействия на уровне транспортных технологий. Такая позиция объясняется, в частности, отсутствием общих для всех национальных администраций связи подходов к определению статуса услуги IP-телефонии.

Оператору IP-телефонии, предлагающему свои услуги абонентам сетей с коммутацией каналов, необходимо, естественно, использовать уже имеющиеся схемы нумерации. Согласно рекомендациям TIPHON, для организации вызовов от абонентов сетей с коммутацией каналов пользователям IP-сети желательно, чтобы последние имели номер E.I 64. В проекте TIPHON также исследуется возможность использования в Интернет кода страны и кода услуги, которые будут задействованы в Интернет-телефонии.

В сетях IP-телефонии, построенных на базе стандарта H.323, преобразование телефонных номеров E.I 64 в IP-адреса и обратно входит в функции gatekeeper. В системах, использующих протокол SIP, эти функции выполняются в специальном сервере.

Табл. 6.2 показывает отношения между именами и адресами для телефонных сетей и приложений Интернет. Она также включает различия в адресации между концепций TIPHON и решениями по Интернет-телефонии, основанными на протоколе SIP.

Цель преобразования номера - замена цифр, набранных вызывающим пользователем, в имена E.I 64 и преобразование этих имен в адреса, имена или идентификаторы, которые необходимо использовать для маршрутизации IP-сообщений управления телефонными вызовами. При этом телефонные соединения устанавливаются внутри домена или между доменами и/или далее маршрутируются в сеть с коммутацией каналов. Для выполнения функций маршрутизации при обслуживании вызовов необходимо иметь базу данных о пользователях и шлюзах, о преобразованиях номеров, имен и адресов.

Таблица 6.2. Отношения между именами и адресами для телефонных сетей и приложений интернет

	Телефонные или нные сети с коммутацией каналов	**E-mail**	**Концепция TIPHON**	**Решение на базе протокола SIP**
Имя	Номер E.164	user@host где host – имя домена	Номер E.164	user@host, возможно с подстано-вочн E.164 для входящих вызовов из сетей с коммутацией каналов
Адрес	Маршрутизация по номеру E. 164 (или префикс маршрутизации +-номер E.164)	IP-адрес	IP-адрес	IP-адрес

Сети IP-телефонии должны поддержать преобразование номеров в двух случаях:

1. Маршрутизируемые вызовы направляются в сеть с коммутацией каналов. В этом случае необходим, по крайней мере, один маршрут к домену, в котором расположен шлюз к сети с коммутацией каналов, обеспечивающий доступ к адресату. Хотя могут быть доступны более чем один маршрут, так как несколько доменов и несколько

шлюзов позволяют обслужить этот вызов.

2. Маршрутизируемые вызовы направляются в сеть с коммутацией пакетов (IP-сеть). В этом случае вызывающий пользователь использует номер E.I 64 как имя, идентифицирующее адресата IP-сети. При этом возможен только один маршрут через соответствующий шлюз.

В соответствии с концепцией TIPHON сети IP-телефонии должны поддерживать, по крайней мере, одну из следующих схем нумерации:

1. Домены сети IP-телефонии должны поддержать все схемы нумерации на сетях связи с коммутацией каналов и обеспечивать надлежащее межсетевое взаимодействие с ними.

2. План нумерации для пользователей сетей IP-телефонии может быть таким же, как и для пользователей сетей с коммутацией каналов, причем с учетом национальных особенностей.

3. Нумерация для предоставления услуг пользователям IP-телефонии должна быть аналогичной нумерации, используемой в сетях с коммутацией каналов.

Система нумерации IP-телефонии должна обеспечивать возможность замены одного номера E.I 64 на другой. Это необходимо для обеспечения поддержки следующих услуг:

- мобильность номера;
- персональная нумерация;
- негеографические услуги типа freephone.

При таких услугах номер направляется в виде запроса на шлюз IP-телефонии и идентифицируется как номер маршрутирования E.I 64. Ответ на запрос будет всегда в виде номера E.164.

В системе IP-телефонии может существовать два вида планов нумерации: открытый (внутренний и международный) и частный. При этом возможны три формата номеров:

1. ***Фиксированный*** - набираемый номер фиксирован;
2. ***Переменный*** - набираемый номер может изменяться;
3. ***Корпоративный*** - набираемый номер определяется данными конфигурации корпоративного плана набора (Custom Dailing Plan).

Формат номера внутреннего плана **имеет следующий вид:**

- Фиксированный: внутренний национальный код (если есть) + код города + номер абонента;
- Переменный: набираемый номер зависти от следующих факторов:
  - локальный вызов (код города соответствует коду, определенному для шлюза Интернет-телефонии) - набирается только номер абонента;
  - междугородный звонок (код города отличается от кода, определенного для шлюза) - набирается внутренний национальный код (если есть) + код города + номер абонента;
- Корпоративный: набираемый номер конфигурируется администратором и зависит от определенных им кодов.

Формат номера международного плана **имеет следующий вид:**

- Фиксированный: код выхода на международную сеть + код страны + код города + номер абонента;
- Корпоративный: набираемый номер конфигурируется администратором и зависит от определенных им префиксов.

Формат номера частного плана **имеет следующий вид:**

- Фиксированный: номер абонента;
- Переменный: набираемый номер зависит от следующих факторов:
  - локальный вызов (код частной зоны соответствует коду, определенному для шлюза) - набирается только номер абонента;

- междугородный звонок (код частной зоны отличается от кода, определенного для шлюза) - внутренний национальный код (если есть) + код города + номер абонента.

- Корпоративный: набираемый номер конфигурируется администратором и зависит от определенных им кодов.

Глава 6•

ОБОРУДОВАНИЕ IP-ТЕЛЕФОНИИ

6.1. Классификация оборудования IP-телефонии

Сегодня IP-телефония - один из наиболее динамичных рынков в мире телекоммуникаций. И операторы связи, и производители сетевого оборудования, и участники рынка компьютерной телефонии - все пытаются предложить отличные от других решения, использующие различное оборудование.

В зависимости от сфер применения, количества поддерживаемых портов, набора реализуемых услуг и других факторов, все оборудование IP-телефонии можно отнести к следующим основным классам.

1. Аппаратно-программные комплексные платформы IP-телефонии.
2. Выделенные или совмещенные с другим оборудованием шлюзы IP-телефонии.
3. УАТС с функциями IP-телефонии.
4. IP-телефоны (аппаратные и программные).

В настоящее время шлюзы IP-телефонии, служащие для преобразования оцифрованных голосовых сигналов в IP-пакеты для передачи их по IP-сетям, являются ключевыми компонентами сегодняшних реализации IP-телефонии. Но и технология, и рынок меняются очень быстро. Стандарты постоянно совершенствуются, некоторым из них еще предстоит пройти тестирование и воплотиться в коммерческих продуктах.

Другие, более долгосрочные тенденции типа разработки телефонов, факс-аппаратов и других устройств на базе протокола IP для конечных пользователей могут в конечном итоге устранить необходимость в IP-шлюзах. Однако внедрение этих разработок предполагает замену имеющихся телефонных устройств - вряд ли многие пользователи в настоящее время могут себе это позволить. Поэтому реализации IP-телефонии в общественном секторе будут, скорее всего, использовать другие решения.

В общем можно выделить несколько основных подходов к использованию данного оборудования при реализации сети IP-телефонии, достоинства и недостатки которых зависят от того, кто использует данное оборудование и для каких потребителей.

Например, если сеть IP-телефонии строится крупным региональным оператором связи, то предпочтительней являются решения на выделенных или интегрированных в АТС шлюзах.

С другой стороны, провайдерам услуг Интернет (ISP) при внедрении услуг IP-телефонии наиболее целесообразно использовать решение, основанное на дооборудовании серверов доступа в сеть Интернет функциями речевого преобразования. А для обеспечения заданного качества для речевого графика в маршрутизаторы добавляются функции QoS.

Если услуги IP-телефонии внедряют крупные фирмы, то для них можно рекомендовать различные варианты: дооборудовать имеющуюся УАТС функциями IP-телефонии илидооборудовать имеющийся корпоративный маршрутизатор речевыми портами, или установить в локальной вычислительной сети аппаратные или программные IP-телефоны.

С точки зрения производителей естественно выгодней развивать те направления) производства оборудования, которыми они давно занимались и по которым имеют большую клиентскую базу. Например, фирма Cisco - лидер по производству оборудования сетей передачи данных, предлагает решения на базе специализированного оборудования IP-сетей. В то же время, признанные производители коммутационного оборудования, например Lucenet Technologies и Alcatel предлагают решения для своих АТС и УАТС. А новые, только что образовавшиеся фирмы, также стараются занять свою нишу на рынке и

ориентируются, в основном, на выделенные шлюзы, голосовые платы или абонентское оборудование.

Далее представлены краткие технические характеристики некоторых типов оборудования IP-телефонии ведущих мировых производителей. Отметим, что ввиду ограниченного объема учебного пособия, в приведенном обзоре указана только небольшая часть выпускаемых продуктов, так как в настоящее время список даже крупных производителей оборудования IP-телефонии содержит несколько десятков позиций. Кроме этого, ситуация на рынке так быстро меняется, что к моменту выхода в свет книги некоторые фирмы возможно перейдут на новые изделия. Поэтому, мы рекомендуем для получения самой свежей информации обращаться непосредственно к производителям или получить информацию на соответствующих сайтах в Интернете.

6.2. Аппаратно-программные комплексные платформы IP-телефонии

Отдельную нишу на рынке оборудования IP-телефонии занимают комплексные решения VoIP, представляющие собой единый комплект аппаратных и программных средств, настроенных на совместную работу. Обычно такое решение включает в себя шлюз, gatekeeper систему управления и другие компоненты и предназначено для использования в сетях крупных операторов IP-телефонии.

Такими решениями являются следующие комплексы:

- программно-аппаратный комплекс MultiVoice, включающий шлюз MultiVoice Gateway, контроллер шлюзов MultiVoice Access Manager, систему управления и мониторинга Navis компании Lucent Technologies;
- семейство шлюзов Clarent Carrier Gateway, Clarent Gatekeeper, пакет ПО для биллинга, маршрутизации и администрирования Clarent Command Center компании Clarent Corp.;
- шлюз/маршрутизаторы серий 2600 и 3600, система управления Cisco Voice Manager компании Cisco Systems;
- Telephony Packet Network компании Nortel Networks;
- шлюз Hi-Gate 1000, gatekeeper Hi-Keeper 1000, менеджер Hi-Manage 1000, пакет По Client Applications и другие компании EC1 Telecom-Hi-Net.

Решение компании Lucent Technologies

Аппаратно-программный комплекс Lucent Technologies MultiVoice для аппаратуры MAX включает в себя компоненты, позволяющие поставщикам услуг и корпоративным клиентам вводить голосовые транспортные услуги реального времени в магистральных IP-сетях. MultiVoice позволяет вести телефонный разговор с обычных телефонных аппаратов, соединенных через открытую или частную пакетную сеть, с использованием стандартного шлюза VoIP. Основой платформы MultiVoice Gateway являются коммутаторы доступа к глобальным сетям MAX 2000 и MAX 6000, а в качестве диспетчера (контроллера шлюзов) - ПО Multivoice Access Manager (MVAM).

Комплекс MultiVoice обладает следующими преимуществами.

- Масштабируемая платформа на базе MAX 2000 и 6000 (с дополнительными картами DSP) легко интегрируется и наращивается вместе с ростом сети.
- Голосовые кодеки поддерживают стандарты G. 711 и G.729A (переговорное качество голоса) и G.723.1 (приложения с малой скоростью передачи).
- Программное обеспечение IP Navigator гарантирует качество обслуживания, необходимое для передачи голоса в реальном времени.
- Менеджер доступа MultiVoice Access Manager (совместимый со стандартом H.323 менеджер шлюзов) обеспечивает обработку функций маршрутизации и тарификации в пределах многошлюзовой сети.
- Аутентификация пользователей с использованием персонального кода PIN и/или

автоматического определения номера (для вызывающего абонента) защищает сетевые ресурсы.

• Регистрация параметров вызова (Call Detailed Recording, CDR) позволяет поставщикам услуг внедрять гибкие схемы тарификации, на основе использованной полосы пропускания и времени разговора.

• Сетевое резервирование обеспечивает повышенную общую надежность сети.

Шлюз MultiVoice Gateway

Шлюз MultiVoice Gateway для аппаратуры MAX обеспечивает сопряжение ТфОП и пакетной сети IP. Для пакетной телефонной сети он является точкой входа/выхода обычных телефонных звонков. Шлюз MultiVoice Gateway выполняет следующие функции.

• Оконечное устройство для стандартных сетевых интерфейсов ТфОП (такие как T1, PRI,E1/DPNSS и E1/R2).

• Поддержка различных голосовых кодеков, что обеспечивает различные уровни сжатия голоса, снижая требования к пропускной способности пакетной сети.

• Генерация/обнаружение тоновых посылок DTMF для эмуляции телефонных сетей ТфОП.

• Поддержка эхокомпенсации и обнаружения пауз для повышения качества голоса передачи речи и снижения требуемой полосы пропускания.

• Поддержка стека протокола ITU-T H.323 для разговора с обычных телефонных аппаратов по IP сети.

• Работа в паре с MultiVoice Access Manager для установления и разъединения вызовов VoIP.

Схема коммутатора доступа MAX 6000 показана на рис. 6.1. Управляющий цифровой сигнальный процессор (control DSP) взаимодействует с основным процессором шасси MAX (host CPU), установленным на материнской плате для связи с сетью IP и выполнения других управляющих функций. После того, как голос оцифрован и сжат, он обрабатывается основным процессором для передачи по IP-сети.

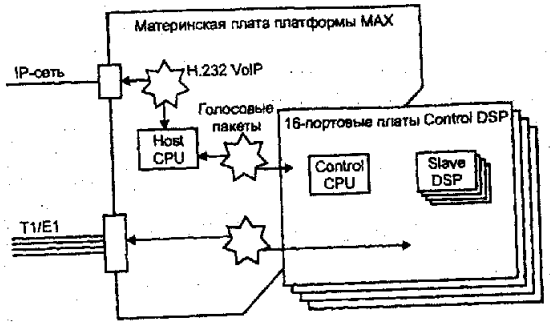

Рис. 6.1. Схема коммутатора доступа MAX 6000

Менеджер доступа - MultiVoice Access Manager

Менеджер доступа MultiVoice Access Manager осуществляет сетевую маршрутизацию, соединяя голосовые вызовы по IP сети. Access Manager выполняет следующие функции.

• Управление зоной H.323, включающей несколько шлюзов MultiVoice Gateway.

Зонной считаются несколько шлюзов H.323, управляемых определенным менеджером Access Manager.

- Трансляция адресов стандартных национальных и международных телефонных номеров (номера E. 164 и частные планы нумерации) в IP адреса и обратно.
- Поддержка аутентификации пользователей и регистрации шлюзов.
- Сопряжение с приложениями тарификации третьих фирм путем использования файлов регистрации данных вызова (CDR) или интерфейсов API.
- Функционирует под управлением Windows NT 4.0 и Solaris 2.5.1

На рис. 12.2 показана типовая схема сети на базе оборудования Lucent Technologies для предоставления услуг IP-телефонии.

Система управления и мониторинга Navis

Navis - это комплекс приложений сетевого управления и управления услугами, который позволяет поставщикам услуг предлагать своим клиентам новые, необходимые им услуги. В числе типичных примеров: виртуальные частные сети (VPN), оптовая продажа портов полосы пропускания, гибкое управление полосой пропускания и сетью клиента, включая подробные отчеты на базе Web и верификацию соглашений об уровне сервиса.

Все продукты линии Navis используют интуитивный графический интерфейс, доступ на базе Web и интеллектуальную обработку информации. При помощи Navis сетевой администратор может осуществлять мониторинг, диагностику и контроль сетевых интерфейсов, устройств и услуг, получая широкий диапазон сетевых диаграмм - от полного вида всей сети до производительности конкретного порта. Кроме того, масштабируемость решений Navis дает возможность сетевым администраторам идти в ногу с ростом сети, поддерживая доступ многочисленных централизованных и распределенных операторов.

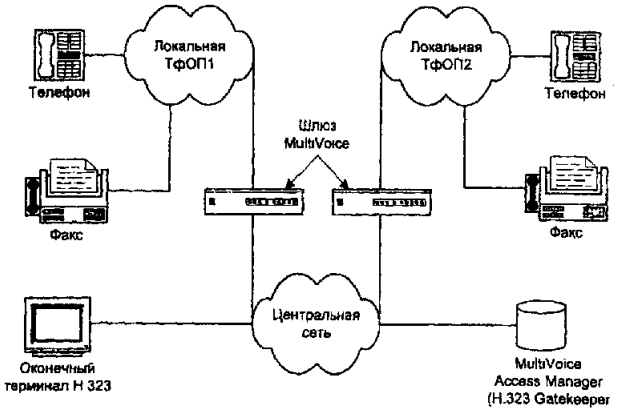

Рис. 6.2. Схема сети IP-телефонии на базе оборудования Lucent Technologies

Следует отметить, что для реализации сети пакетной передачи голоса на базе ATM-сетей Lucent Technologies выпускает семейство мультисервисных мультимедийных шлюзов/коммутаторов доступа ATM PacketStar PSAX. Семейство включает 6 моделей шлюзов PSAX, отличающихся количеством и типами портов для подключения к LAN, Frame Relay или ATM для передачи графика голоса, видео и данных (рис. 12.3). Все

оборудование управляется единой системой Integrated Navis Management.

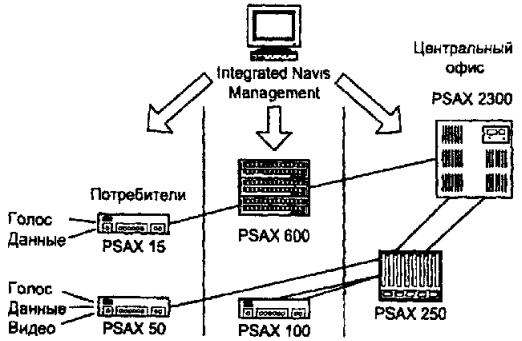

Рис. 6.3. Семейство мультимедийных шлюзов Lucent Technologies для сетей ATM

Решения фирмы Clarent Corporation

Clarent Command Center

Программный пакет Clarent Command Center работает под Windows NT Server и MS SQL Server или Oracle и сочетает в себе функции биллинговой системы и контроллера сети одновременно. Command Center является центральным узлом архитекуры Clarent Distribed Softswitch, которая, помимо этого, включает в себя Clarent Call Manager, Clarent GateKeeper Clarent Connect, и в комплексе предоставляет полный набор функций, необходимых для организации сетей IP-телефонии.

Clarent Command Center реализует следующие задачи.

1. Сервер транзакций осуществляет авторизацию шлюзов и пользователей, маршрутизацию, тарификацию и запись информации о звонках (биллинг). Содержит всю информацию, необходимую для работы сети Clarent.
2. Авторизация пользователей дебетных карт.
3. Нормализация номеров и маршрутизация звонков.
4. Система гибкой тарификации звонков в зависимости от направления и времени вызова Call Rating (учитываются праздники, время дня, маршрут и т.п.)
5. Хранение информации о пользователях абонентских шлюзов: данные о пользователе, его телефонный номер, сервисный профиль.
6. Биллинговая система для всех категорий абонентов: предоплаченные (дебитные) карты, постоплаченные стандартные счета, абонентские счета.
7. Генерация и хранение детальных записей о звонках CDR (Call Detail Records) (кроме генерации печатных или электронных счетов для каждого из абонентов).

В штатной поставке управляется и конфигурируется через Web - приложение Clarent Assist. Общается со шлюзами по протоколу CAM, разработанному Clarent. Поддерживает предоплаченную (дебитные карты) и постоплаченную (взаиморасчет провайдеров) модель звонков. Не содержит машины состояния телефонных портов, поэтому легко конфигурируетсяв избыточные кластеры. Производительность Command Center ограничена только производительностью базы данных, с которой оно работает, и в зависимости от кофигурации сети достигает нескольких миллионов звонков в час наибольшей нагрузки. Обычно поставляется уже установленным на компьютер в производственном корпусе для размещения в 19" стойке.

Clarent Gatekeeper (GK)

Clarent Gatekeeper - программный продукт, который предоставляет шлюзам и сетям, работающим по протоколам H.323 и SIP, прозрачно обмениваться графиком с сетями на базе оборудования Clarent, а также интегрирует шлюзы третьих фирм как составные части сети Clarent. Gatekeeper является еще одной составной частью архитектуры Clarent Distributed Softswtich. Контроль за работой интегрированной сети осуществляется с помощью Clarent Command Center также, как для шлюзов и сетей на базе только оборудования Clarent Gatekeeper работает под управлением Windows NT или Sun Solaris. Обычно поставляется уже установленым на компьютер в производственном корпусе для размещения в 19" стойке.

Clarent Local Access Call Manager

Аналогичен Clarent GateKeeper, но предоставляет интерфейс по протоколу MGCP и предназначен для устройств доступа в Интернет и IP-телефонии по цифровым каналам последней мили - DSL, кабельные модемы, модемы доступа по сетям питания, цифровые ISDN-модемы. Clarent Local Access Call Manager предоставляет полный набор телефонных услуг для абонентов: присвоение номера, трансляция и авторизация, биллинг, ожидание перевод звонка, интеграция с голосовой почтой, совмещенных с высокоскоростным доступом в Интернет. Для интеграции с ТфОП можно использовать любые шлюзы, способные работать под управлением Clarent Distributed Softswitch.

Call Manager является новым добавлением в структуру Clarent Distributed Softswitch, которая также включает в себя Clarent Command Center, Clarent GateKeeper и Clarent Connect. Clarent Distributed Softswitch позволяет строить абонентские и магистральные сети IP-телефонии, которые вообще не будут пересекаться с ТфОП, кроме как по номерной емкости. Голос таким образом будет проходить по пакетным сетям «от трубки до трубки». Call Manager работает под управлением Windows NT или Sun Solaris. Обычно поставляется уже установленым на компьютер в производственном корпусе для размещения в 19" стойке.

Clarent Connect

Clarent Connect позволяет сетям на базе Clarent Command Center безопасно и эффективно объединяться для обмена графиком. Пользуясь механизмами авторизации, маршрутизации и биллинга Clarent Command Center, программный пакет Connect позволяет не просто создавать маршруты в другие сети, но регулировать количество графика между сетями на базе кредитных лимитов, проверяемых в реальном времени, при каждом соединении. Connect также гарантирует, что каждый из партнеров, через чью сеть проходила установка звонка, получит соответствующие биллинговые записи.

Connect строится на базе двух основных типов соглашений о взаимодействии — билатеральное и клирингхаус (центр взаиморасчетов). Первое - работает как стандартное соглашение об обмене графиком между двумя сетями, второе - предоставляет всем членам кли-рингхауса получать регулируемый доступ к терминации графика в сети любого другого члена клирингхауса. Так, например, всероссийский клирингхаус в Москве может предоставить своему партнеру (провайдеру IP-телефонии) в Брянске, у которого есть соглашение только с данным клирингхаусом, возможность маршрутизировать звонок в Екатеринбург по низкому тарифу при том, что партнеры в Екатеринбурге и Брянске могут и не знать о взаимном существовании и между ними нет взаимной договоренности о пропуске графика.

Connect работает под управлением Windows NT или Sun Solaris. Обычно поставляется уже установленым на компьютер в производственном корпусе для размещения в 19" стойке.

Clarent CPG (Customer Premise Gateway)

Семейство шлюзов Clarent CPG представляет собой набор 2-8-портовых шлюзов, предназначених для организации доступа в сеть IP-телефонии на «последней миле». В него входят устройства, поддерживающие только голос, и интегрированые со средствами доступа в Интернет на последней миле - кабельными и DSL модемами. На базе технологий, содержащейся в шлюзах CPG, партнерами Clarent разработаны шлюзы, подключаемые к Интернет по ISDN и сетям переменного тока.

Шлюзы поддерживают протокол MGCP и под управлением Clarent Call Manager или эквивалентного программного обеспечения предоставляют широкий спектр абонентских услуг. Все шлюзы имеют lOOBase-T интерфейс LAN для подключения других устройств к локальной сети и поддерживают технологии NAT, DiffServ и взвешеное распределение с приоритетом, что обеспечивает высокое качество разговора. Шлюзы также поддерживают Clarent fhroughPacket - разработаную Clarent технологию агрегации пакетов голоса с разных портов, которая позволяет уменьшить количество пакетов в сети в 4-10 раз, в зависимости от объема Шлюза, одновременно снижая задержки и увеличивая качество передачи голоса и факса.

Clarent Carrier Gateway

Семейство провайдерских шлюзов IP-телефонии фирмы Clarent включает модели, различающиеся внешним видом, числом подключаемых аналоговых телефонных портов или Цифровых трактов T1/E1, ценой и, конечно, возможностями. Общее для них – процессоры Pentium или Celeron от Intel + Windows NT Server, карты AudioCodes для оцифровки голоса телефонные интерфейсы Natural Microsystems. В семейство входят следующие шлюзы:

- Gateway 100;
- Gateway 400;
- Gateway 1200.

Характеристики семейства шлюзов Clarent приведены в табл. 6.1-6.3. Шлюзы подключаются к телефонной сети по аналоговым портам или нескольким цифровым трактам T1/E1 и осуществляют передачу голосовых сообщений и факсов в режиме реального времени. Шлюз Gateway 100, кроме цифрового интерфейса, может комплектоваться картами с аналоговыми телефонными портами по 8 портов на карте. Шлюзы Gateway 400 и Gateway 1200 могут также комплектоваться картами SS7/C7, которые позволяют присоединять шлюзы ТфОП с помощью общеканальной сигнализации. Дополнительных устройств или изменения конфигурации сети при этом не требуется.

Таблица 6.1. Характеристики семейства шлюзов Clarent Carrier Gateway

Шлюз	Gateway 100	Gateway 400	Gateway 1КЦ
Подключение к ТфОП	FXO, E&M analog, T1/E1	4 x T1/E1	4, 8, 10 или12 T1/E1 ,1
Возможность передачи факса	Да	Да	Да
Поддержка IVR	Да	Да	Да
Нормализация номера	Да	Да	Да
Подключение к ЛВС (адаптер Ethernet)	100 BaseT	100 BaseT	100 BaseT
Процессор	Celeron 366	Pentium II 600	Dual Pentium II 600
Объем памяти. Мбайт	128	256	256
Количество и мощность блоков питания, Вт	1x250	2x250	2x400

Таблица 6.2. Поддержка абонентских телефонных интерфейсов в шлюзах Clarent

Семейство или шлюз	FXS	FXO	E&M	ISDN BRI
Clarent CPG	Есть	Разрабатывается	Разрабатывается	Разрабатывается
Clarent Gateway 100	Нет	Есть	Есть	Нет

Таблица 6.3. Поддержка межстанционных телефонных интерфейсов в шлюзах Clarent

Семейство или шлюз	E1R2	E1 R1.5	User-Side PRI	Network-Side PRI	E1E&M
Gateway 100	Да	Да	Да	Да	Да
Gateway 400	Да	Да	Да	Да	Да
Gateway 1200	Да	Да	Да	Да	Да

Как и Clarent CPG, шлюзы поддерживают Clarent ThroughPacket. При повреждении внешнего IP канала, шлюзы могут направить весь входящий график обратно в ТфОП с целью сохранения непрерывности услуги для абонентов, при этом по-прежнему будут производиться схема отработки голосового меню IVR и компрессия речевого сигнала. Все разъемы для подключения трактов T1/E1, телефонных портов, PS/2 мышки и клавиатуры, а также монитора расположены с тыльной стороны.

Оборудование фирмы Clarent работает в сетях провайдеров и крупнейших телефонных компаний первого уровня: AT&T, British Telecom, NTT, China Mobile, Concert, ITXC, Singtel и др.

Решения компании Cisco Systems

Свою концепцию по созданию устройств, осуществляющих интеграцию различных типов данных, голоса и видео компания Cisco Systems окрестила AVVID (Architecture for Voice, Video and Integrated Data). Основная идея Cisco при разработке оборудования IP-телефонии - создание специализированных модулей и развитие возможностей операционной системы уже существующих моделей. Для своих модульных маршрутизаторов и серверов доступа компания Cisco выпустила специализированные модули расширения, которые осуществляют компрессию и декомпрессию голоса. Семейство оборудования VoIP, производимого Cisco, достаточно широкое, здесь представлены и недорогие устройства средней емкости, которые способны выполнять задачи не только по передаче голоса через IP, но и осуществлять доступ в Интернет, связывать локальные сети и т.д. В приведенной ниже таблице 6.4 представлены официально заявленные компанией Cisco устройства, способные выполнять функции голосовых шлюзов (информация от 30 июня 2000 г.).

Поддержка аналоговых интерфейсов телефонных сетей для голосовых шлюзов Cisco отражена в табл. 6.5.

Таблица 6.4. Характеристики шлюзов Cisco

Семейство или шлюз	MGCP (межшлюзовый протокол управления)	H.323v2
VG200	Есть	Есть (фаза2)
CISCO 1750	Нет	Есть
CISCO 3 810 V3	Планируется	Есть
CISCO 2600	Планируется	Есть
CISCO 3600	Планируется	Есть
CISCO 5300	Планируется	Есть
CISCO 7200	Нет	Есть
CISCO 7500	Нет	Разрабатывается
Catalyst 4000 WS-X4604-GWY	Планируется	Да
Catalyst 6000 WS-X6608-xl	Планируется	Нет

В табл. 6.6. отражена поддержка голосовыми шлюзами Ciscoовых интерфейсов телефонной сети.

Как видно из таблиц, спектор оборудования и список его возможностей достаточно широк. Большим достоинством изделий Cisco является их изначально узкая специализация только для решения определенных сетевых задач. Отсутствие механических носителей информации и использование вместо них модулей памяти FLASH существенно повышается надежность и производительность оборудования Cisco, а также увеличивает его срок службы.

Таблица 6.5. Поддержка аналоговых телефонных интерфейсов в шлюзах Cisco

Семейство или шлюз	FXS	FXO	E&M	Аналоговый DID/CLIDI
VG200	Есть	Есть	Нет	Разрабатывается
CISCO 1750	Есть	Есть	Есть	Разрабатывается
CISCO 3810 V3	Есть	Есть	Есть	Присутствует в версиях IOS 12.1(4)T, 12.1(2) xx
CISCO 2600	Есть	Есть	Есть	Присутствует в версиях IOSИЧЦ 12.1(4)T,12.1(2)xx
CISCO 3600	Есть	Есть	Есть	Присутствует в версиях IOS 12.1(4)T, 12.1(2) xx
CISCO 5300	Нет	Нет	Нет	____
CISCO 7200	Нет	Нет	Нет	____
CISCO 7500	Нет	Нет	Нет	____
Catalyst 4000 WS-X4604-GWY	Есть	Есть	Есть	Присутствует в версиях IOS 12.1(4)T, 12.1(2) xx +
Catalyst 6000 WS-X6608-xl	Есть	Нет	Нет	Есть в IOS 12.1(4)T Нет в 12.1(2) xx

При использовании оборудования Cisco, реализующего функции серверов доступа или I шлюзов VoIP, для организации биллинга и ведения абонентских счетов необходима биллинговая система, способная работать с использованием протоколов Radius и/или TACACS+. Функции контроллера шлюза (gatekeeper) H.323 реализуются в отдельном дополнительном маршрутизаторе (предлагается 3бхх или 26хх) со специализированной операционной системой IOS. Для каждого семейства существует несколько разновидностей операционной системы, выбор которых зависит от конкретной задачи.

Таблица 6.6. Поддержка цифровых телефонных интерфейсов в шлюзах Cisco

Семейство или шлюз	E1 R2	E1 CAS	User-Side PM	Network -Side PRI	User Side BRI	Network-Side BRI	Цифровой DID/CLID
VG200	Разр.	Разр.	Разр.	Разр.	Нет	Нет	Разр.
CISCO 1750	Нет	Нет	Нет	Нет	Разраб.	Разраб.	___
CISCO 3810 V3	Нет	Есть	Нет	Нет	Есть	Нет	Есть
CISCO 2600	IOS 12.1x	IOS 12.1x	IOS 12.1x	IOS 12.1x	Есть	Разраб.	Есть
CISCO 3600	IOS 12.1x	IOS 12.1x	IOS 12.1x	IOS 12.1x	Есть	Разраб.	Есть
CISCO 5300	Есть	Есть	Есть	IOS 12.0.7T	Нет	Нет	Есть
CISCO 7200	Разр.	Разр.	IOS 12.1.3T	IOS 12.1.3T	Нет	Нет	Есть
CISCO 7500	Разр.	Разр.	Разр.	Разр.	Нет	Нет	Разраб.
Catalyst 4000 WS-X4604-GWY	Есть	Есть	Есть	Есть	Разраб.	Разраб.	Есть
Catalyst 6000 WS-X6608-xl	Нет	Нет	Есть	Есть	Нет	Нет	Есть j

Для мониторинга и управления сетью с поддержкой передачи речи Cisco предлагает Cisco Voice Manager. Voice Manager представляет собой приложение на Java и предназначен для упрощения процесса развертывания и управления сетью с поддержкой передачи речи. Он облегчает конфигурацию голосовых и факсимильных интерфейсов и администрирование плана голосовой связи, предоставляет подробные совокупные и текущие отчеты о вызовах, измеряет такие параметры QoS, как задержка, потеря пакетов и тип услуги.

Оборудование Cisco имеют в своем распоряжении многие крупные провайдеры IP-телефонии международного уровня, включая ITXC, iBasis, GTE Inemetworking, GRIC, Carrieri, AT&T, Arbinet и другие.

Кратко рассмотрим наиболее часто используемые в сетях IP-телефонии продукты фирмы Cisco.

Модульный маршрутизатор доступа Cisco 1750

Модульный маршрутизатор доступа Cisco 1750 хотя и невелик по размерам и цене, но имеет достаточно мощный RISC процессор Motorola MPC860T PowerQUICC с тактовой частотой 48 МГц, поддерживает от 16 до 48 Мбайт ОЗУ и содержит три слота расширения для установки различных интерфейсных карт. В слоты 0 и 1 возможна установка интерфейсных карт WIC и VIC в любом сочетании. В слот 2 можно установить только одну голосовую интерфейсную карту VIC с двумя аналоговыми портами FXO/FXS/E&M.На шасси имеется встроенный порт Ethernet 10/100, есть также консольный порт. Использование Cisco 1750 в сочетании с возможностями операционной системы (IOS) версии 12.1(3)T, позволяет получить VoIP H.323 v2 шлюз с 6-тью голосовыми аналоговыми портами, (но без интерактивного голосового меню IVR). Такой IP-шлюз, кроме своего непосредственного предназначения, обладает многими присущими маршрутизатору полезными функциями, например, установка очередей для голоса и данных, поддержка шифрования информации на скоростях до 512 кбит/с, возможность организации сетевых экранов.

Модульные маршрутизаторы серии Cisco 26xx

Модульные маршрутизаторы доступа семейства Cisco 26xx построены на базе центральных процессоров Motorola MPC860 40 МГц - 261 x и Motorola MPC860 50 МГц - 262x соответственно. Содержат на своем шасси три слота для установки различных модулей расширения. Два из них (WAN1 и WAN2) позволяют устанавливать уже упомянутые выше интерфейсные карты WIC для организации синхронных/асинхронных портов в различных сочетаниях друг с другом. Третий слот предназначен для установки одного модуля NM-1V или NM-2V, который в свою очередь, в зависимости от потребностей, можно укомплектовать одной или двумя 2-х портовыми аналоговыми интерфейсными картами с портами FXO/FXS/E&M

В результате можно получить до 4-х голосовых аналоговых портов. В третий слот также возможна установка рассмотренных выше модулей NM-HDV-1E1-30E (или NM-HDV-2E1-60) совместно с интерфейсными картами T1/E1 Multiflex Voice/WAN Interface (Multiflex VWIC). Внутри маршрутизатора имеется разъем для установки дополнительного модуля расширения AIM, снижающего загрузку основного процессора и улучшающего общую производительность системы.

На шасси маршрутизаторов серии 26xx имеется от одного до двух встроенных портов Ethernet-Fast Ethernet, консольные порты управления. При построении на базе семейства26xx голосового шлюза с цифровыми интерфейсами телефонной сети E1, в зависимости от версии IOS, наличия модуля AIM, объема оперативной памяти и выбранного типа сложности ков, возможна поддержка от 30 до 60 голосовых портов.

Голосовой шлюз Cisco VG200

Голосовой шлюз Cisco VG200 представляет собой упрощенную версию маршрутизатора семейства 26xx. Исключены два слота для установки интерфейсных карт WIC, а также внутренний слот расширения для модуля AIM. Центральный процессор - Motorola MPC860 оперативная память расширяется до 32 Мбайт. Устройство имеет один слот для установки стандартных сетевых модулей серии NM-xxxx. Поддерживает до 4-х аналоговых интерфейсов сов FXS/FXO/E&M или до двух цифровых трактов T1-CAS, в ближайшее время анонсирована поддержка T1/E1 PRI и El CAS. На шасси имеется встроенный интерфейсный Ethernet 10/100 Base-T.

Маршрутизаторы Cisco 3бxx для IP-телефонии

Семейство модульных маршрутизаторов Cisco 3бxx является самым популярным решением в мире для передачи данных и Internet. По утверждениям самой компании Cisco объем проданных во всем мире маршрутизаторов этой серии составил около 350 000. В семейство входят: Cisco 3620 с RISC процессором Motorola R4700 (тактовая частота 80 МГц два слота расширений, Cisco 3640 с RISC процессором Motorola R4700 (тактовая частота 100 МГц) и четыре слота расширений, Cisco 3660 с RISC процессором Motorola OED R5271 (тактовая частота 225 МГц) и шесть слотов расширений.

Модульный принцип построения маршрутизаторов, производимых Cisco Systems, позволяет использовать одни и те же унифицированные модули в различных платформах. Поэтому сетевые модули NM-HDV-1E1-30E (или NM-HDV-2E1-60) совместно с интерфейсными картами T1/E1 Multiflex Voice/WAN Interface Card (Multiflex VWIC) можно установить и 36-ую серию. Однако следует отметить, что разработчики не предусмотрели на шасси своих маршрутизаторов 3620 и 3640 встроенных портов Ethernet.

Для того, чтобы превратить 3620 или 3640 в шлюз VoIP, необходимо приобрести и установить в один из слотов дополнительно, по крайней мере, модуль NM-1E с одним портом Ethernet 10BaseT. Таким образом можно получить ряд IP-шлюзов H.323 v2 следующей емкости:

- Cisco 3620 с одним модулем NM-HDV-2E1-60E, в зависимости от выбранного типа сложности кодеков - от 30 до 60 голосовых портов;
- Cisco 3640 с тремя модулями NM-HDV-2E1-60E, в зависимости от выбранного типа кодеков - от 90 до 180 голосовых портов;
- Cisco 3660 содержит на шасси встроенный порт Ethernet и благодаря этому имеет возможность установить шесть модулей NM-HDV-2E1-60E, что в зависимости от выбранного типа кодеков, позволяет получить от 180 до 360 голосовых портов.

Сервер доступа Cisco AS5300

Сервер доступа Cisco AS5300 на основе процессора R4700 с тактовой частотой 150 МГц был разработан, прежде всего, как гибкое и многофункциональное решение для компаний провайдеров услуг Интернет. Данная платформа принципиально отличается от рассмотненных выше решений на базе семейств 26xx-36xx. Главное отличие AS5300 - более узкоспециализированная концепция модульной архитектуры. Шасси сервера доступа имеет три установочных слота, расположенных на тыльной стороне устройства. Модули расширения для серии AS5300 объединены в наборы или «бандлы» (в терминологии Cisco, «банда» - совокупность интерфейсной карты, и карты «постобработки», например, интерфейсная карта на 4 тракта E1 PRI + карта на 60 цифровых модемов - решение для организации сервера доступа в Интернет по коммутируемым линиям). Интерфейсные карты, в зависимости от разновидности, позволяют подключить от 4-х до 8-ми цифровых трактов T1/E1 и до 4-х портов WAN с интерфейсом V.35.

Специально разработанный набор AS53-E1-60VOXD (D - означает использование модулей DSP двойной плотности) содержит интерфейсную карту на 4 тракта E1 и карту постобработки с DSP на 60 голосовых портов. Карта постобработки содержит на себе ОЗУ и отдельный процессор Motorola MIPS 4700 с тактовой частотой 100 МГц, а также пять посадочных мест для плат DSP. Одна голосовая карта двойной плотности может обеспечить передачу до 60 одновременных разговоров/факсов. Плата позволяет дискретно наращивать число голосовых каналов путем установки небольших плат - модулей DSP.

Плата модуля DSP содержит шесть DSP Texas Instruments TMS320C549 с тактовой частотой 100 МГц (внутренняя память SRAM 128 К слов 16 бит). Для поддержки 60-ти голосовых портов и, соответственно, двух трактов E1 потребуется установить 5 модулей DSP. Установив в свободный третий слот на шасси AS5300 еще одну голосовую карту, можно довести общее число голосовых портов до 120 и полностью использовать все четыре тракта E1 интерфейсной карты бандла. С версией операционной системы IOS 12.1(3) и программного обеспечения для голосовой карты VFCWare версии 7.14, бандл позволяет получить поддержку кодеков G.711, G.729, G.726, G.723.1, G.728, оптимизированную трансляцию команд факсимильной передачи сообщений - fax relay и специфических команд модемных соединений, а также оптимальную трансляцию тональных команд DTMF. Число голосовых портов не зависит от типов выбранных кодеков, а определяется лишь пропускной способностью WAN-каналов.

Вариант использования сервера доступа Cisco AS5300 в сети IP-телефонии показан на рис. 6.4.

6.3. Оборудование шлюзов IP-телефонии

Шлюз PathBuilder S200 Voice Access Switch компании 3Com

Продукт компании 3Com Corp. - PathBuilder S200 Voice Access Switch - представляет собой маршрутизатор, коммутатор доступа и шлюз в едином исполнении. Допускает подключение до 28 речевых каналов. Поддерживает аналоговые телефонные интерфейсы FXS, FXO, E&M и цифровые E1 и PRI-ISDN. Важным достоинством является возможность передачи речи через Frame Relay-сети.

Поддерживает стандарт H.323 и, соответственно, алгоритмы кодирования голоса G.711, G.723.1 и G.729a. При этом достигается компрессия голоса до 5,3 кбит/с.

PathBuilder S200 Voice Access Switch может быть использован для задач маршрутизации в глобальных сетях и для обеспечения решения голос/данные.

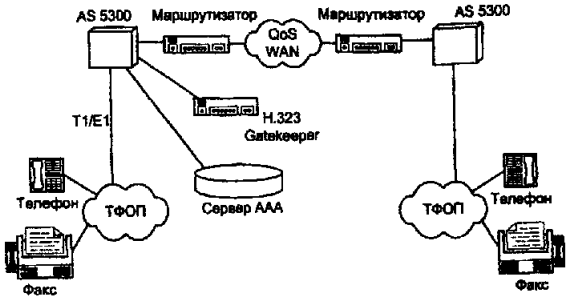

Рис. 6.4. Построение сети IP-телефонии на базе Cisco AS5300

На рис. 6.5 представлено решение, при котором существующая ATM-сеть, построенная на базе оборудования 3COM, решает также задачу VoIP. Маршрутизаторы 3 COM PathBuilder S200 в данном случае оснащены функциями VoIP.

Шлюз MainStreetXpress 36100 VoIP Gateway компании Newbridge Networks

MainStreetXpress 36100 VoIP Gateway представляет собой платформу для операторов, объединяющую функции шлюза IP-телефонии и концентратора доступа. Следует отметить поддержку машиной режимов ATM и Frame Relay, а также возможность работы с системой сигнализации ОКС7. При этом максимальное число речевых портов - до 1500. Поддерживаемые телефонные интерфейсы: El, PRI.

Шлюз является составной частью архитектуры IP-телефонии компании Newbridge Networks Corp. - Newbridge IP Telephony Network Architecture, включающей в себя также точку контроля голосовых служб (VSCP) - MainStreetXpress 56040, терминальные устройства и клиентское программное обеспечение, а также средства менеджмента сети - MainStreetXpress 46020 Network Manager и MainStreetXpress 45020 Element Manager. Данное решение -VoIP поверх существующей сети ATM или Frame Relay - представлено на рис. 6.6.

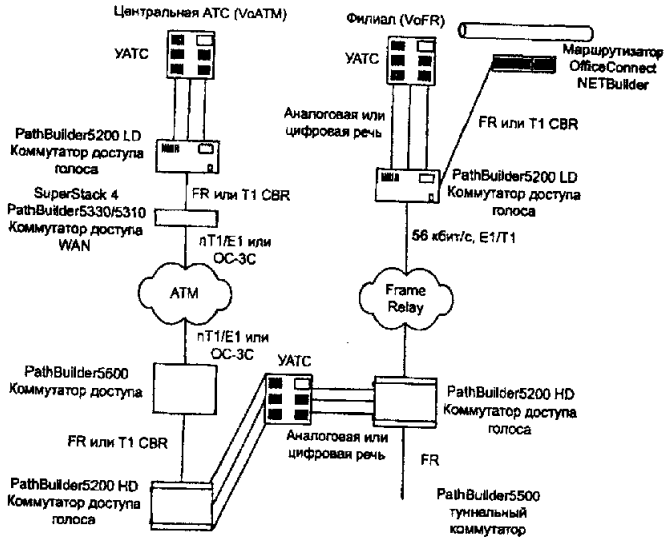

Рис. 6.5. Решение VoIP компании 3COM

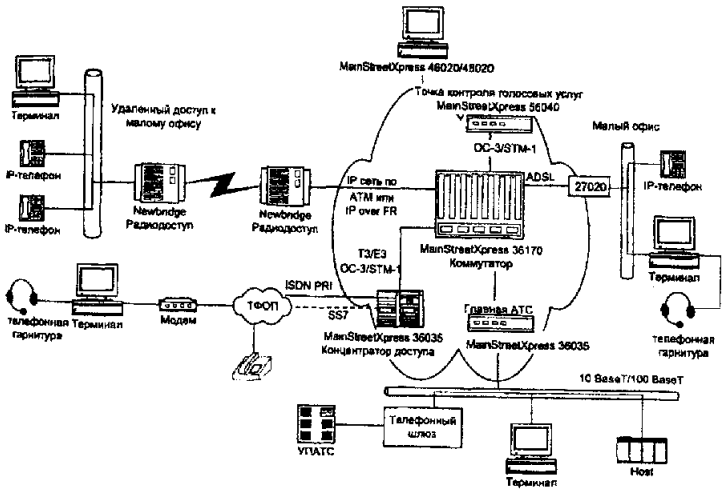

Рис. 6.6. Решение VoIP на базе оборудования компании Newbridge

Шлюз IEN 5000 серии Integrated Enterprise Network компании Hypercom Corp.

Семейство многофункциональных коммутаторов/маршрутизаторов Integrated Enterprise Network (IEN) компании Hypercom, в частности IEN 5000, позволяет сжимать голос по алгоритму ACELP до 6,2 кбит/с.

В крупных сетях мелкие филиалы связываются с более крупными, а те, в свою очередь, с центральными или региональными офисами с такими мощными устройствами, как IEN 5000. Служащие в качестве мощных коммутаторов/маршрутизаторов центральных офисов IEN 5000 позволяют более эффективно использовать имеющиеся линии и снизить затраты на связь.

IEN поддерживают SNA и другие унаследованные протоколы, осуществляют многопротокольную маршрутизацию и выполняют функции интегрированных CSU/DSU, сжатия (голоса и данных, коммутации и резервных каналов. 16-слотовое шасси вмещает до 256 портов на узел и способно обслуживать тысячи филиалов. Что касается интерфейсов с общедоступными сетями, то система может работать с линиями T-l/E-1, ISDN или Frame relay.

Гораздо более гибкая и масштабируемая, чем традиционные IP-маршрутизаторы, IEN-5000 имеет, помимо функций коммутации каналов, пакетов и ячеек, архитектуру параллельной обработки Hypercom - комбинацию высокоскоростных пакетных и TDM-шин –для интеграции унаследованного (SNA, BSC и т. д.), локально-сетевого, голосового, факсимильного и видеографика.

IEN 5000 использует собственные методики задания приоритетов и предотвращения перегрузок, чтобы все филиалы получали при передаче, скажем, речи параллельно с данными по сети Frame relay качество, сравнимое с качеством телефонной связи. Пакеты данных сегментируются, а скорость сжатия меняется динамически для обеспечения надежной передачи голоса и данных при изменяющихся условиях в сети.

Программное обеспечение выполняется в Windows 95, Windows NT, UNIX, HP UNIX и AIX. Системой можно управлять по SNMP с помощью HP Open View, HP Open View UNIX NetView for AIX.

Системные утилиты включают RMON (с интегрированной функцией контроля), загрузку ПО и конфигурации, протоколирование тревожных ситуаций, индикатор использования глобальной сети и систему управления защитой.

Шлюз LinkNet IP Gateway компании Linkon Corporation

LinkNet IP Telephony Gateway от Linkon выполняется на станциях SPARC под управлением Solaris (UNIX). Обработка пакетов осуществляется мощным 64-разрядным процессором компьютера, а маршрутизация - встроенными средствами SPARC.
Плата Maestro «с универсальным портом» (для речи, факсов или данных) использует DSP компании Lucent Technologies. Один DSP обслуживает один разговор (два канала), выполняет 80 млн. операций с плавающей точкой в секунду. Каждый процессор цифровой обработки сигналов сравним с RISC-процессором с 40 целочисленными MIPS, причем один сервер Sun может содержать до 72 DSP (или 2880 MIPS). Благодаря своей мощи DSP позволяют сократить задержки при сжатии до 30 миллисекунд.

LinkNet IP масштабируется от четырех аналоговых портов до четырех T-1 или E-1, что в сумме дает до 96 полнодуплексных каналов. По сути, Linkon предоставляет готовые системы на базе платформы Sun с шиной PCI.

TeraVox - это предлагаемый компанией высокоуровневый API. С его помощью разработчик может создавать приложения для обмена сообщениями с функциями интерактивного голосового ответа и распознавания речи. Объединение TeraVox с программным обеспечением LinkNet Internet позволило создать шлюз с полным пакет-

услуг, в том числе с IVR для телефонных карт.

Поддержка SS7 позволяет осуществлять интеллектуальную маршрутизацию без потребления избыточной пропускной способности для сигналов «занято», ускорить установление соединения и повысить уровень интеллектуальности маршрутизации вызовов.

Система осуществляет аппаратное эхоподавление с помощью микросхем TECO производства Lucent Technologies (точно такие же микросхемы используются основными телекоммуникационными компаниями в их сетевых коммутаторах). На основе этой микросхемы Linkon разработала модуль вспомогательной платы с обеспечением эхоподавления для 32 портов, что достаточно для линии E-1. Одной из интересных функций является возможность выбора звонящим с помощью IVR желательного маршрута между Internet/Intranet и обычной телефонной сетью. Шлюз позволяет выбирать не только различные маршруты, но испособы сжатия.

Функция gatekeeper обеспечивает проведение процедуры ping других сетевых узлов. Если задержка или потеря пакетов превосходит заданный порог, то gatekeeper переключит вызовы на альтернативный маршрут, например на Intranet и телефонную сеть.

Отказоустойчивость gatekeeper Linkon обеспечивается за счет распределения функций между всеми взаимно зарегистрировавшимися узлами. Если маршрут становится недоступен или компонент оказывается в аварийной ситуации, то вызовы могут быть направлены на другой шлюз.

Система Linkon будет вести подробную запись о звонках с предоставлением отчетов о занимаемой пропускной способности и выпиской счетов. Она может составлять отчеты о потере пакетов, задержках, длительности звонков и сообщать другие подлежащие учету данные.

Linkon предлагает также IP LinkNet Developer's Kit, с помощью которого разработчики программного обеспечения для UNIX могут создавать приложения для передачи голоса и факса по IP. Комплект содержит две четырехпортовые аналоговые платы FS4000 (Sbus) Maestro и программное обеспечение LinkNet с драйверами Solaris 2.5, исходный код приложения для передачи факсов по IP и интерфейс прикладного программирования LinkVox Direct Driver Interface (DDI) для контроля коммуникаций по IP. Низкоуровневый интерфейс DDI дает приложениям полный контроль и быстрый доступ к голосовым данным реального времени в однопотоковой или многопотоковой среде. DDI имеет свыше 10 утилит на базе командной строки и свыше 100 вызываемых функций на Си в своей библиотеке интерфейса.

IP LinkNet Developer's Kit предлагает также технологии сжатия аудио по выбору, LinkNet Transcoder для преобразования сжатого аудио в реальном времени, драйверы для Solaris 2.5, исходный код демонстрационного приложения для организации связи между телефонами по IP, специальный комплект приложений для DTMF и эхоподавления. Кроме того, комплект содержит специальный набор API под названием LinkVox для ускоренной разработки коммутации IP-телефонии и преобразования информации между IP и телефонными сигналами.

LinkVox представляет собой весьма сложную среду разработки приложений, поддерживающую коммутацию, обмен сообщениями, передачу факсов и интерактивную связь. Модель прикладного интерфейса является однопотоковой и способна поддерживать асинхронную речь. Специальный менеджер голосовых файлов обеспечивает вдвое большую производительность, чем с помощью стандартных файловых систем UNIX. LinkVox содержит свыше 35 утилит на базе командной строки для контроля и мониторинга событий в системе и свыше 100 вызываемых функций на Си в своей библиотеке интерфейса.

LinkVox рекомендуется использовать, когда необходимо разработать автономное решение с высокой плотностью каналов (48 и более каналов на одно шасси).

Возможные варианты включают 6-слотовое шасси расширения, что дает до 12

аналоговых портов, и 24-слотовое шасси расширения, что обеспечивает до 72 цифровых портов с интерфейсом T-1.

Многосервисный шлюз IP Network Exchange 2210 компании Netrix Corporation

Многосервисный шлюз IP Network Exchange 2210 и программное обеспечение Vodex Voice Gateway были выпущены Netrix в 1998 году.

Будучи «многосервисной» коммутирующей платформой, Exchange 2210 может одновременно с IP-коммуникациями поддерживать и Frame relay. Шлюз предлагает оптимальную комбинацию коммутации, сжатия речи и многопротокольной поддержки на одной компактной платформе.

Многосервисная коммутация позволяет данному шлюзу поддерживать такие сетевые службы, как IP, Frame relay, X.25 и ISDN (рис. 6.7), а также дает возможность создавать недорогие решения для приложений передачи данных, речи и изображений на базе выделенных линий, общедоступных сетей или их комбинации. Выбор протоколов и методов передачи осуществляется с помощью программного обеспечения.

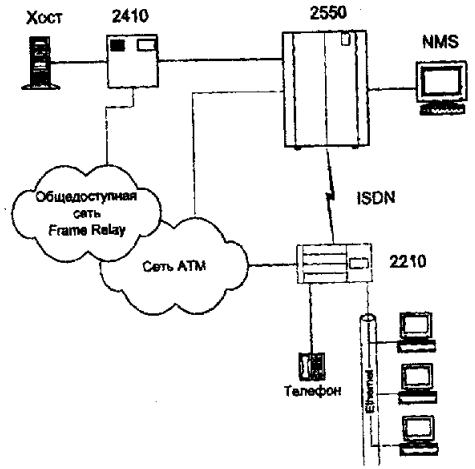

Рис. 6.7. Решение VoIP на базе оборудования компании Netrix Corp.

Каждый узел способен обслуживать свыше 180 разговоров одновременно и предоставляет выбор алгоритмов сжатия, поэтому администраторы сетей могут предпочесть оптимальную для каждого случая комбинацию скорости передачи речи и качества связи.

Network Exchange 2210 имеет до 64 последовательных портов данных/линий со скоростями до 2 Мбит/с, свыше 180 речевых каналов и интерфейс локальной сети. Как и все платформы Netrix, Network Exchange 2210 настраивается программным образом - каждый порт данных шлюза 2210 может быть сконфигурирован независимо под любого абонента или любой протокол линии выполняются одновременно с любыми протоколами на других портах.

Алгоритмы обеспечивают сжатие до 4,8-12 кбит/с, причем каждому адресу может быть назначен свой алгоритм. Помимо поддержки речи, шлюз 2210 может определять тональные сигналы факс-модемов на любом этапе вызова и затем передавать этот трафик

по сети.

Как и другие члены семейства Network Exchange, шлюз 2210 интегрируется со своими старшими родственниками - Network Exchange 2550 (он поддерживает ATM, Frame relay, X.25, TDM и ISDN для приложений передачи данных, речи и изображений) и 2410 (Frame relay, X.25, TDM и ISDN), поэтому разработанное решение может масштабироваться от низкоскоростной асинхронной передачи до высокоскоростных сетей ATM.

Шлюз VocalTec Telephony Gateway компании Vocaltec Communications Ltd.

VocalTec Telephony Gateway представляет собой систему на базе Windows NT для организации моста между телефонной сетью и Intranet/Internet с поддержкой звонков с телефона на телефон, с факса на факс, с ПК на телефон, с телефона на ПК и из браузера Web на телефон.

Пользоваться системой очень просто - после соединения со шлюзом автоматический секретарь спрашивает у звонящего абонента телефонный номер адресата. Звонящий вводит телефонный номер с клавиатуры обычным образом. Местный шлюз автоматически определяет, что вызов должен быть переадресован удаленному шлюзу.

Среди других пользовательских сервисов система интерактивного голосового ответа, отправка факсов в реальном времени или с промежуточным хранением в зависимости от того, какую цель ставит перед собой пользователь.

VocalTec Telephony Gateway использует механизм автоматического обнаружения для предотвращения разъединения в результате длительных периодов молчания.

Система включает также Surf&Call, подключаемый модуль для браузера Web, с помощью которого пользователи могут позвонить с сервера Web на обычный телефон. Пользователи могут также обращаться к голосовой почте с помощью усовершенствованной технологии DTMF, а удаленные пользователи ПК получают удобный доступ к сети через VocalTec Internet Phone.

Технология VocalTec Telephony Gateway пригодится компаниям с несколькими офисами, предлагающим дополнительные платные услуги провайдерам Internet, работающим на дому пользователям и операторам центров телефонного обслуживания.

Версия шлюза за номером 3.2 заменяет магистральные линии (одноступенчатый набор номера), а также позволит иметь универсальные порты для передачи речи/факсов и API для дебетных карт.

Голосовой шлюз-маршрутизатор корпорации NEC

Голосовой шлюз-маршрутизатор IP45/951 японской корпорации NEC объединяет функции речевого преобразования, маршрутизатора и контроллера зоны (gatekeeper) H.323. В дальнейшем планируется включить функции серверов аутентификации и биллинга.

Благодаря поддержке большого числа протоколов кодирования речи VoIP-маршрутизатор может взаимодействовать с любыми голосовыми шлюзами разных производителей. По данным корпорации NEC, их шлюз-маршрутизатор обеспечивает кодирование речевого сигнала согласно рекомендациям G.711, G. 723.1, G. 723. la, G.728, G.729, G.729a, G.729b, G.729ab.

Модель обладает развитыми механизмами обеспечения QoS, что немаловажно для решения задач по передачи голоса через пакетные сети. Наиболее важные из них: фрагментация пакетов, уплотнение заголовков, управление полосой пропускания по протоколу RSVP, подавление пауз. Дополнительно реализованы механизмы повышения качества речи при восстановлении: подавление эхо-сигналов, динамическая и статическая буферизация колебаний задержек сигналов, генерация комфортного шума.

Маршрутизатор IP45/951 поддерживает следующие голосовые интерфейсы: для аналоговых каналов - E&M и FXS, вскоре будет поддерживаться FXO; для цифровых каналов — E1/T1, планируется включить интерфейсы ISDN BRI и PRI. Это устройство может обрабатывать до 30 речевых каналов. Сетевой интерфейс только один – 10BaseT.

Для иллюстрации возможностей IP45/951 на рис. 6.8 представлен типовой вариант построения фрагмента корпоративной сети, соединяющей центральный офис, филиал и небольшую торговую точку (например, пункт обмена валюты). Для организации каналов связи между ними можно использовать сети протоколов Frame Relay или IP. После появления интерфейсов ISDN для этой цели вполне подойдут BRI или PRI.

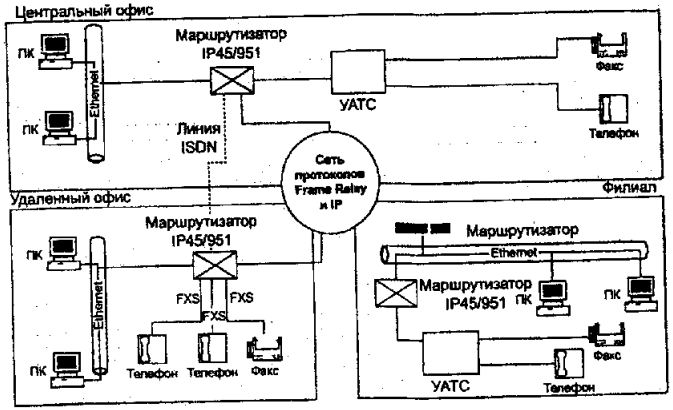

Рис. 6.8. Фрагмент типовой корпоративной сети на базе шлюза-маршрутизатора IP45/951 корпорации NEC

Поскольку маршрутизатор поддерживает сигнализацию по выделенному (CAS) и общему (CCS) каналу для УАТС, он может объединять офисные станции. Такое решение позволяет уменьшить необходимое число голосовых портов и плавно интегрироваться в существующую инфраструктуру.

Business Communications Manager фирмы Nortel Networks

Универсальная система Business Communications Manager (BCM) фирмы Nortel Networks одновременно выполняет функции офисной АТС и шлюза IP-телефонии, маршрутизатора и устройства доступа в территориально распределенную сеть (WAN). В ней реализованы разнообразные IP-сервисы: мощный межсетевой экран обеспечивает работу в Интернет, кэширование DNS-имен и содержимого Web-страниц ускоряет эту работу, а DHCP-сервер облегчает администрирование сети. Встроенный сервер Windows NT позволяет использовать широкий набор прикладного программного обеспечения,

оптимизированного для работы на этой операционной платформе.

При передаче пакетных данных в системе реализуются следующие функции:

- маршрутизатор IP/IPX (статический, RIP, OSPF) с поддержкой DiffServ;
- протоколы WAN (Frame Relay, PPP, MLPP);
- резервирование основного WAN-канала по коммутируемому (V.90 или ISDN BRI/PRI);
- динамическое конфигурирование (сервер DHCP);
- кэширование имен DNS и содержимого Web-страниц;
- межсетевой экран и трансляция адресов (NAT).

Система BCM позволяет реализовать следующие речевые и интегрированные приложения:

- IP-телефония;
- речевая почта и автосекретарь;
- унифицированная обработка сообщений;
- центр обслуживания вызовов;
- консоль телефонистки на базе ПК;
- компьютерно-телефонная интеграция (CTI);
- беспроводная микросотовая связь Companion (DECT с версии 2.5).

На базе системы BCM возможное полное (телефония + Интернет) коммуникационное оснащение небольшого и среднего офиса (рис. 6.9). Емкость системы версии 2.0 составляет 80 телефонных абонентов, в версии 2.5/3 она увеличена до 180 абонентов. Возможно подключение к системе аппаратных и программных IP-телефонов Nortel Networks. Более того, версия 2.5 позволяет использовать с BCM беспроводные H. 323-терминалы.

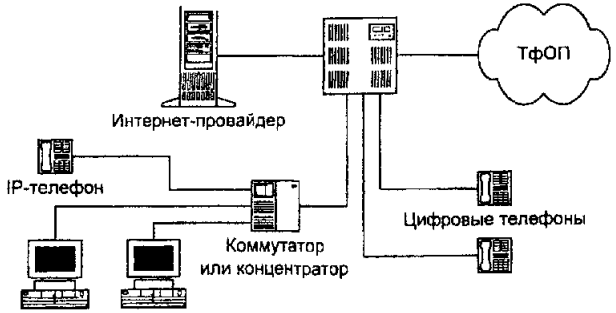

Рис.6.9. Реализация сети IP-телефонии на базе системы BCM фирмы Nortel Networks

Решение компании Netspeak Corporation

С помощью WebPhone Gateway Exchange (WGX) звонок может быть направлен с WebPhone на обычный телефон, с обычного телефона на WebPhone, с телефона на телефон или со страницы Web на обычный телефон (при поддержке WebPhone телефонный вызов со страницы Web может быть отправлен посредством указания на соответствующую ссылку).

Звонок с WebPhone на телефон или звонок с телефона на WebPhone требует посредничества по крайней мере одного, а соединение между двумя телефонами по Internet - двух серверов WGX.

WebPhone Gateway Exchange имеет процессор Pentium на 200 МГц (минимум), оперативную память емкостью 64 Мбайт (рекомендуемая емкость), CD-ROM, AG-T1 (или AG-E1) компании Natural Microsystems со вспомогательной платой RT320, сетевую плату NMS TX2000 10BaseT и, факультативно, NMS T-Connect для аналоговых систем. Работает с операционной системой NT.

WebPhone Gateway Exchange поддерживает кодек Microsoft GSM, имеет программируемую систему интерактивного голосового ответа без и с аудиотекстом, поэтому есть возможность вставлять приветствия пользователю, информацию о продукте и запросы с предложением выбрать тот или иной пункт для дальнейшей маршрутизации вызова.

Каждый WGX имеет конфигурационный файл с информацией о местных телефонных номерах, отвечающих соединению WGX с телефонной сетью. Эту информацию о маршрутах WGX сообщает NetSpeak Connection Server. Все серверы WebPhone Gateway Exchange могут получить доступ к информации о маршрутах WGX4epe3 Connection Server, что исключает необходимость в реконфигурации имеющихся WGX при добавлении нового сервера.

С помощью Connection Server (CS) компании могут предоставлять услуги по установлению соединения, управлению бюджетами и рекламе WebBoard (рекламное окно расположено в области экрана WebPhone) для своих пользователей WebPhone и систем автоматического распределения вызовов. С помощью CS серверы WebPhone и WebPhone Gateway eXchange (WGX) могут устанавливать контакт с другой стороной по электронной почте, IP-адресу и телефонному номеру. Сервер хранит необходимую информацию и отслеживает, какие бюджеты используются на данный момент.

При поступлении запроса на установление соединения по адресу электронной почты CS преобразует запрошенный адрес электронной почты в IP-адрес и таким образом позволяет установить прямое соединение между вызывающим и вызываемым абонентами. При поступлении запроса на установление соединения по телефонному номеру CS возвращает адрес ближайшего к получателю сервера WGX в соответствии с телефонным номером E.I 64 - точнее говоря, в соответствии с кодом страны, города и АТС. Затем соединение с указанным телефонным номером устанавливается через указанный сервер WGX.

CS представляет собой, по сути, краеугольный камень для сетей NetSpeak. Некоторые компоненты NetSpeak, например серверы ACD и WGX, вообще не могут функционировать без CS.

NetSpeak ACD Server (никакого иного физического распределителя вызовов не нужно) направляет звонки пользователей Internet с NetSpeak WebPhones на специальные Agent WebPhones в настольной системе сотрудника центра телефонного обслуживания. При наличии WGX традиционные телефонные вызовы могут направляться непосредственно на Agent WebPhones.

Инструментарий конфигурации и управления потоками вызовов имеет графический интерфейс. Программное обеспечение может осуществлять мониторинг сети и отслеживать состояние звонков. Оно предоставляет информацию, включая номер порта, состояние, идеен тификация входящего/исходящего вызова, время начала разговора и т. д. Вызовы могут направляться предопределенному лицу или использовать PIN-КОД для завершения транзакции.

Серверы WGX поддерживают программируемый интерактивный голосовой ответ, Gateway Message Detail Recording (GMDR), Supervisory Tone Detection - как GSM, так и TrueSpeech 8.5, управление буферами и все необходимые административные процедуры (Operations, Administration, Maintenance and Provisioning, OAM&P) через Netspeak Control Center. Центр управления NetSpeak используется для конфигурации, администрирования, управления и обслуживания функций сервера и служит центральным «концентратором»

для мониторинга серверов NetSpeak и координации взаимодействия между ними.

Система способна регистрировать события в реальном времени с помощью сервера NetSpeak Database Services (DBS) и поддерживать управление вызовами в реальном времени.

6.4. УАТС с функциями IP-телефонии

Реализация функции IP-телефонии в УДТС

Традиционные УАТС давно уже перестали быть просто телефонными станциями. В процессе своего развития они превратились в коммуникационные серверы, подключенные к ЛВС и выполняющие транзакции в режиме реального времени практически со 100%-ной надежностью. В последних версиях УАТС реализована поддержка услуг IP-телефонии, а сами они стали полноценными узлами IP-сетей.

При реализации IP-телефонии с функциональной точки зрения на первый взгляд нет принципиальной разницы, каким образом реализуется IP-шлюз - в виде вставляемой в УАТС платы или отдельного устройства. Однако в действительности это не совсем так. При интеграции IP-телефонии непосредственно в УАТС абонент в общем случае получает доступ к более широкому набору сервисов (ко всему, что есть), а кроме того, это позволяет повысить прозрачность станций (от одного производителя, разумеется).

Обеспечивая связь удаленных УАТС через IP-сеть, шлюзы сохраняют прозрачность телефонных функций, поскольку передают и телефонную сигнализацию, в том числе фирменную (например, ABC у Alcatel или MCDN у Nortel Networks). Что касается сервиса, то IP-УАТС ничем не отличаются от классических, просто речь и сигнализация передаются по IP-сети (рис. 6.10).

Следует отметить, что используемые в УАТС шлюзы постоянно отслеживают качество связи и, если оно становится ниже заданного уровня, переводят соединение в традиционные сети (рис. 6.11).

Большинство IP-шлюзов выполнены в виде плат/модулей., устанавливаемых в стативы УАТС. Что касается алгоритмов кодирования, то здесь наиболее популярны обычная ИКМ (G.711), а также механизмы G.723 (5,3/6,3 кбит/с) и G.729 (8 кбит/с), обеспечивающие приличное сжатие сигнала. Все производители обеспечили соответствие своих шлюзов рекомендации H.323. Вместе с тем, перспективный протокол SIP не реализован пока ни в одном из продуктов, хотя ряд фирм заявили о планах его поддержки.

Следует отметить, что ведущие производители IP-УАТС выпускают аппаратные и программные IP-телефоны. Аппаратные IP-телефоны подключаются непосредственно к локальной сети по интерфейсу Ethernet и по внешнему виду и функциональности они являются практически полными аналогами традиционных аппаратов, производимых этими компаниями. Такие аппараты имеют развитые функциональные возможности и стоят достаточно дорого. Однако очевидно, что такие аппараты не могут стоить дешевле системных телефонов и в настоящий момент позиционируются именно как системные аппараты с несколько большей, чем у стандартных аналогов, функциональностью. Краткий обзор IP-телефонов приведен в следующем разделе.

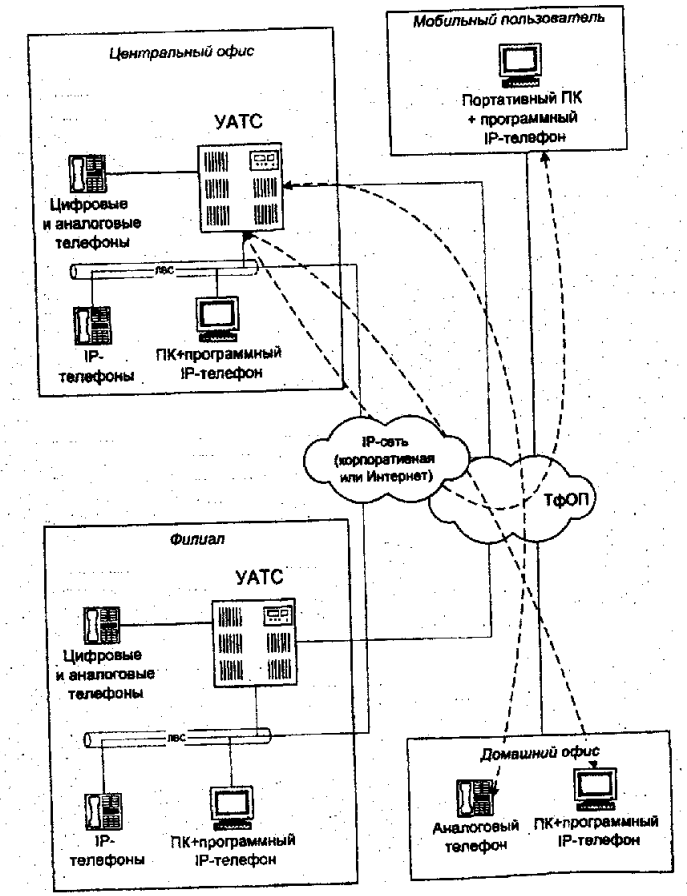

Рис. 6.10. **Реализация корпоративной сети IP-телефонии**

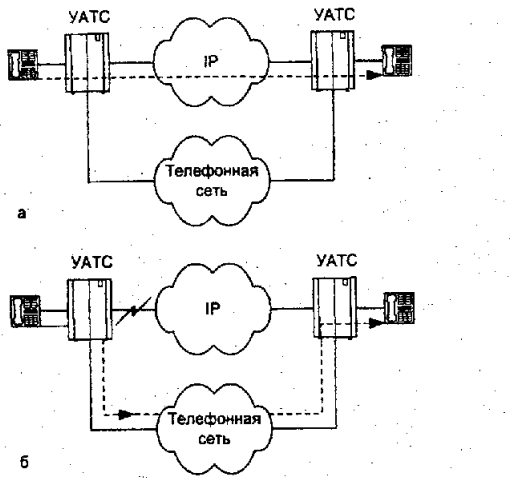

Рис. 6.11. Переход IP-УАТС на телефонную сеть при резком ухудшении качества IP-сети

Программные IP-телефоны реализованы в виде прикладных программ и их функционирование полностью зависит от работы ПК. Подобное решение IP-телефона позволяет использовать разнообразные приложения компьютерно-телефонной интеграции, например телефонную книжку, программу-менеджер управления вызовами, графический интерфейс для работы с речевой почтой и т.д.

Решения по IP-модернизации УАТС ведущих производителей и технические характеристики встраиваемых в УАТС IP-шлюзов приведены в табл. 6.7 и табл. 6.8 [11].

Далее дается краткий обзор УАТС с функциями IP-телефонии ведущих мировых производителей.

Таблица 6.7. Решения по IP-модернизации УАТС

Фирма	УАТС	Интегрируемый в АТС шлюз	Аппаратный IP-телефон	Программный IP-телефон
Alcatel	OmniPCX 4400	+	+	+
Avaya	Definity	+	+	+
ECI	Coral	+	+	+
Ericsson	MD110,BP50/25	+	+	+
Nortel	Meridian 1	+	+	+
Siemens	Hicom150E	+	+	+

Таблица 6.8. Характеристики встраиваемых в УАТС шлюзов IP-телефонии

Характеристика	Alcatel	Avaya	ECI	Ericsson	Nortel	Siemens
Емкость, число одновременных вызовов	30 на плату (1500 на узел)	До 64 на модуль	30	32 или 64	24	16 каналов на карту
Алгоритмы кодирования речи	G.711, G.723.1, G.729A	G.711, G.723, G.729A	G.711, G.723.1, G.729AB, IICelp	G.711, G.723.1, G.729, G.728, G.729 GSM-EFR	G.711, G.723 , G.729 G.729A	G.711, G.723.1,
Поддержка H.323	+	+	+	+	+	+
Поддержка SIP	-	-	-	-	-	-
Перевод графика в ТфОП при ухудшении качества IP-связи	+	+	+	+	+	+
Передача по IP-сигнализации (QSIG и/или фирменных)	+	+	+	+	+	+

УДТС OmniPCX 4400 компании Alcatel

В конце января 2000 года компания Alcatel анонсировала новую УАТС OmniPCX 4400 со встроенной поддержкой IP. Архитектура станции такова, что ее ядро представляет собой UNIX-сервер, а шина - полносвязную ячеистую структуру ATM (отсюда торговая марка технологии - «кристалл»). Такая платформа - вполне естественное для IP окружение.

Alcatel имеет в своем распоряжении ПО для организации на базе мультимедийного компьютера рабочего места Alcatel 4980. Оно интегрируется в существующие платформы коллективной работы и обеспечивает полный доступ ко всем сервисам OmniPCX. Кроме того, компания предлагает ПО для администрирования телефонных сервисов.

OmniPCX 4400 поддерживает такую немаловажную функцию, как гарантированный минимум качества разговоров и их непрерывность. Если, помимо IP-соединения, станция имеет традиционное (как резерв или параллельно используемую альтернативу), то при ухудшении качества связи через IP она переключится на него. Оценка качества соединения на основании параметров прохождения пакетов осуществляется непрерывно, и если на станцию поступает вызов, а параметры IP-соединения ниже допустимых, то станция задействует традиционные каналы. Кроме того, переключение на резервную линию может осуществляться динамически, для чего OmniPCX должны быть установлены по обе стороны соединения. Динамическое переключение происходит прозрачно для абонента (за исключением, возможно, изменения звука), без прерывания разговора.

Все пакетные нововведения Alcatel в телефонии являются преимущественно результатом приобретения ряда компаний: Xylan, Packet Engines и AssuredAccess, но вследствие курса на унификацию всех имеющихся платформ (это выражается, в частности, в присутствии в названиях большинства серий оборудования слова «Omni») решения компании имеют высо кую степень интегрированности. В частности, сетевые устройства с поддержкой коммутации третьего и четвертого уровней оптимизируют передачу голосового IP-трафика в сети. Кроме того, мультисервисные граничные устройства серии AssuredAccess способны поддерживать VoFR и VoIP. Иными словами, AssuredAccess может иметь голосовое соединение (локальное в случае удаленного офиса) по VoFR, но при этом,