ITU-T
ETSI
IETF

G.711 G.723 G.728 G.729a
H.225 H.235 H.245 H.323 T.38
Q.931 E.164 Diff-Serv

VoIP ITSP SIP OSP UDP
RSVP MPLS MGCP RTP LDAP
RTCP RFC RAS

А.В. РОСЛЯКОВ
М.Ю. САМСОНОВ
И.В. ШИБАЕВА

IP-ТЕЛЕФОНИЯ

MCU ADPCM QDU
DTMF CS-ACELP MOS
MGC CA-ACELP PDP
MG MP-MLQ PEP

ИНЖЕНЕРНАЯ ЭНЦИКЛОПЕДИЯ
ТЕХНОЛОГИИ ЭЛЕКТРОННЫХ КОММУНИКАЦИЙ

IPv.6
QoS

TIPHON i-NOW

А.В. Росляков,
М.Ю. Самсонов,
И.В. Шибаева

IP-телефония

Издание второе

ЭКО-ТРЕНДЗ

Москва, 2003

ИНЖЕНЕРНАЯ ЭНЦИКЛОПЕДИЯ ТЕХНОЛОГИИ ЭЛЕКТРОННЫХ КОММУНИКАЦИЙ

УДК 621.395.37
681.324
ББК 32.882

А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева

IP-телефония. – М.: Эко-Трендз, 2003. – 252 с.: ил.

ISBN 5-88405-044-5

В книге представлены концептуальные основы технологии передачи речи по сетям пакетной коммутации, работающим по протоколу IP (Internet Protocol). Рассмотрены архитектуры системы IP-телефонии на базе Рекомендаций ITU-T H.323 и концепции TIPHON, разработанной ETSI. Описаны вопросы сигнализации, адресации, обеспечения качества в сетях IP-телефонии. Отдельные главы посвящены вопросам стандартизации и правового регулирования IP-телефонии, системам биллинга и менеджмента пользователей, вопросам безопасности, мобильности услуг. Дан анализ принципов построения сетей IP-телефонии, описана практика внедрения услуг пакетной передачи речи за рубежом и в России, приведен обзор оборудования для построения сетей IP-телефонии.

Книга будет полезна широкому кругу специалистов в области телекоммуникаций, аспирантам и студентам соответствующих специальностей.

ББК 32.882

ISBN 5-88405-044-5

Содержание

ВВЕДЕНИЕ

Что такое телефония знает не только каждый взрослый человек, но даже любой ребенок. Существенно меньшее количество людей могут толково объяснить, что такое Интернет. И уж совсем немногие (в основном узкие специалисты) знают, что скрывается под термином «Интернет-телефония». Хотя понятно, что с точки зрения словообразования, новый термин получился путем соединения двух старых: «Интернет» и «телефония». Отсюда следует достаточно простое определение Интернет-телефонии (интернет-телефонии, как часто пишут в последнее время) – 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.

На страницах отечественных и зарубежных телекоммуникационных журналов в последнее время развернулась дискуссия по поводу определения места и роли IP-телефонии в дальнейшем развитии средств передачи речи. Взгляды сторон, участвующих в дискуссии, резко противоположны.

Одни из них утверждают, что будущее принадлежит только протоколу IP, их главный тезис «Всё по IP, IP по всему». Сейчас даже появилось понятие «айпизм», которое подразумевает универсальность применения данной технологии для передачи любых видов информации (голоса, данных, видео) и замену всех других сетей на сеть с пакетной коммутацией на базе протокола IP. Часто приходится слышать, что дни традиционной телефонии с коммутацией каналов сочтены и через 10-15 лет от нее уже ничего не останется.

Сторонники противоположных взглядов указывают на то, что несмотря на большие темпы роста объема трафика IP-телефонии за последние годы (150-200%), его доля в США составляет около одного процента от трафика классической телефонии, а во всем мире и того меньше. Даже с учетом всех оптимистических прогнозов операторы сетей связи и в перспективе будут получать основную прибыль от предоставления услуг телефонных сетей с коммутацией каналов. Аргументами в пользу этих доводов являются существующие проблемы с обеспечением требуемого качества передачи речи по публичным каналам Интернет, сравнительно меньшая надежность существующих IP-сетей, трудность управления такими сетями.

Похоже истина где-то посередине. Действительно, 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 экономиии 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.

В международных организациях и форумах идет непрерывная разработка новых стандартов и протоколов, связанных с передачей речи по сетям с пакетной коммутацией. Производители аппаратного и программного обеспечения регулярно представляют на рынок свои новые продукты. За последние год-полтора редкий номер отечественных телекоммуникационных журналов обходится без статьи, затрагивающей технологию IP-телефонии. За рубежом издано несколько монографий, посвященных даной тематике, в сети Интернет имеется огромное количество сайтов, содержащих информацию по IP-телефонии. Все это говорит о перспективности данной технологии.

Насколько известно авторам, в России до сих пор не издано ни одной монографии, посвященной технологии IP-телефонии. В этих условиях авторы поставили перед собой задачу обобщения и систематизации информации по данной тематике. Трудность ее решения обусловлена, с одной стороны, огромным объемом имеющихся нормативных, технических и аналитических материалов, а с другой стороны, – неустоявшейся терминологией, быстрой сменой технических решений и непрерывным появлением новых промышленных разработок.

Авторы не претендуют на абсолютную полноту и глубину представления материала по IP-телефонии. Но представление в рамках одной книги концептуальных основ технологии IP-телефонии (архитектура системы, вопросы стандартизации, сигнализации, обеспечения качества и другие аспекты) – вот основная цель, к которой стремились авторы. Насколько точно она достигнута – решать читателям.

Авторы благодарны сотрудникам научно-производственного центра «Инфосфера» (г. Самара) Имамову А.Т. и Городновой Н.В. за помощь в подготовке части материала книги.

Глава 1

ОБЩИЕ ПРИНЦИПЫ IP-ТЕЛЕФОНИИ

1.1. Сеть Интернет и протокол IP

О технологии и сети Интернет и используемом в ней протоколе IP (Internet 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 (FNC или Federal Networking Counsil) 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/ Internet 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

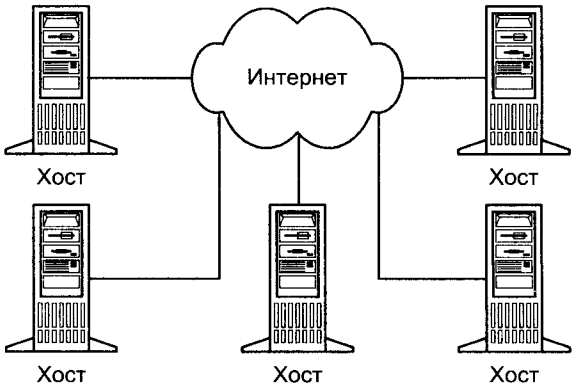


Рис. 1.1. Сеть Интернет с точки зрения пользователя

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 компьютер. На этом уровне работают драйвер устройства в операционной системе и соответствующая сетевая плата компьютера.

Сетевой уровень – основа стека протоколов TCP/IP. Именно на этом уровне реализуется принцип межсетевого соединения, в частности маршрутизация пакетов по сети Интер-

нет. 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.

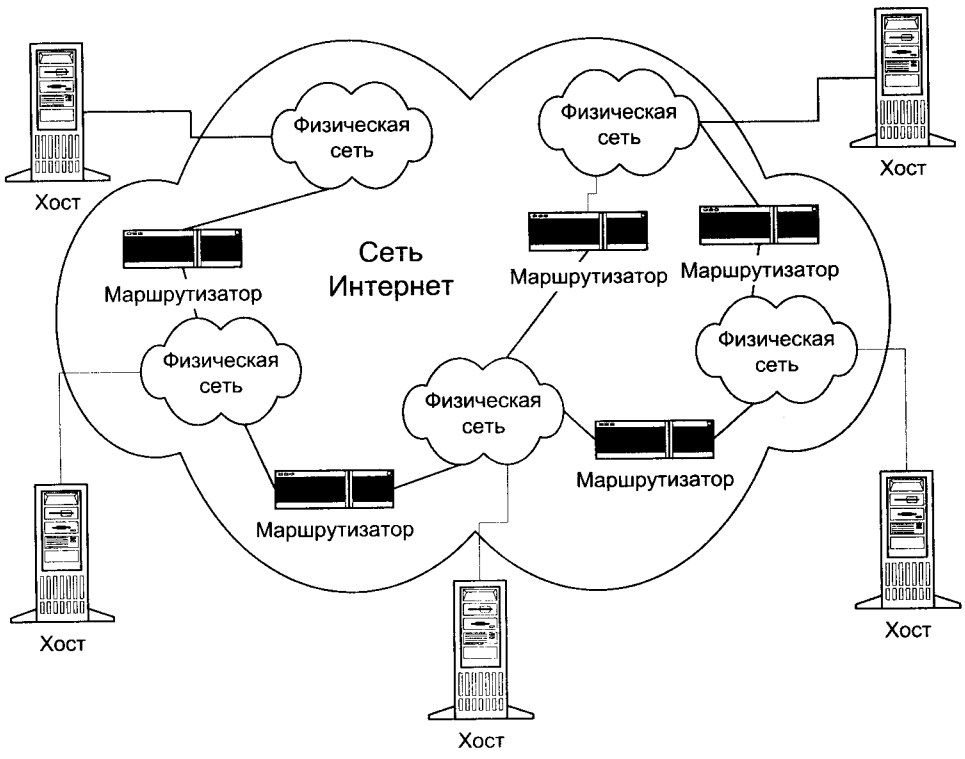


Рис. 1.2. Внутренняя структура сети Интернет

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 трафика 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.

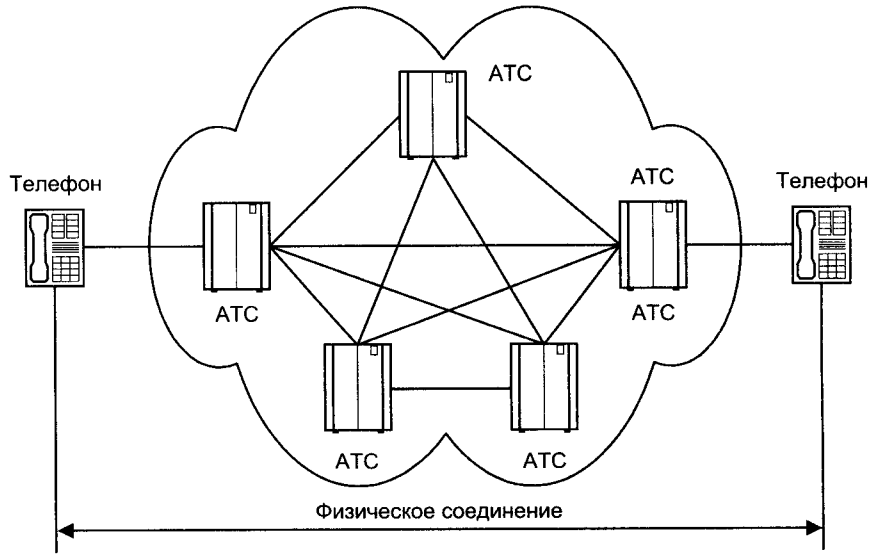


Рис. 1.4. Соединение в «классической» телефонной сети

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.

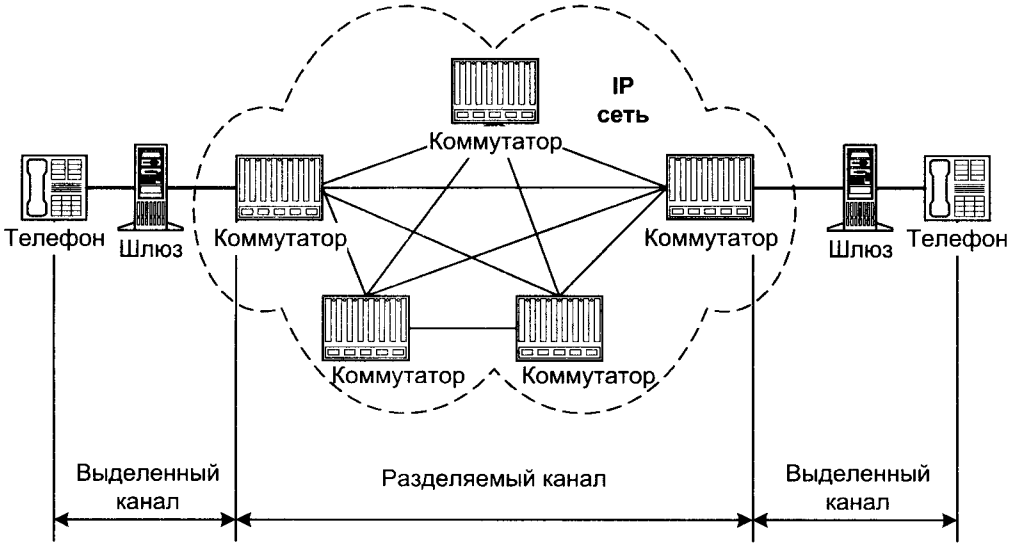


Рис. 1.5. Соединение в сети с коммутацией пакетов

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 декомпрессируется 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 Интернет по назначению с использованием протокола IP. Для пакетов, приходящих из сети на телефонный сервер и уходящих в телефонную линию, операция происходит в обратном порядке. 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 трафик 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 прироста рынка до 2002 г., а эксперты Frost&Sullivan ориентируются на 149%. Аналитики Philips 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 Lucent 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-телефонии возрастет всего лишь до 2%. По прогнозу экспертов исследовательской компании Insight 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).

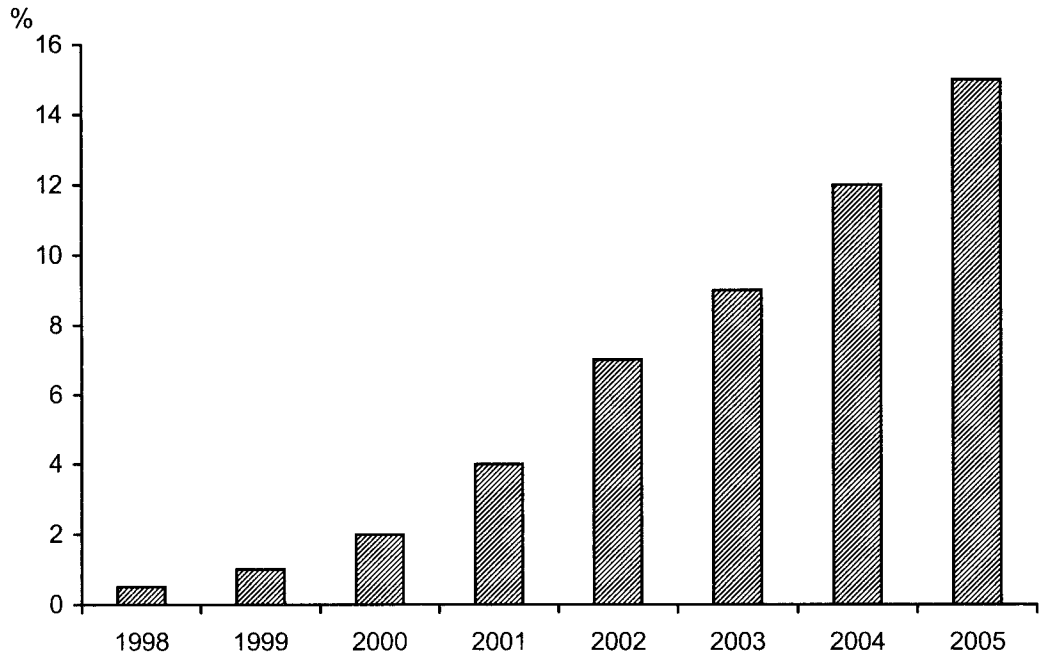


Рис. 1.6. Состояние и прогноз доли трафика IP-телефонии в США (по данным фирмы Yankie Group)

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 мультимедийной 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.

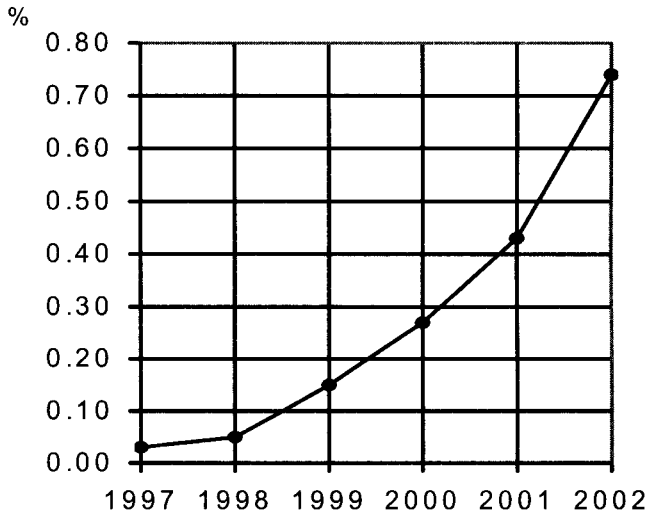


Рис. 1.7. Доля IP-телефонии в общих доходах телефонных компаний в США и Европе, % (по данным Datamonitor)

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.

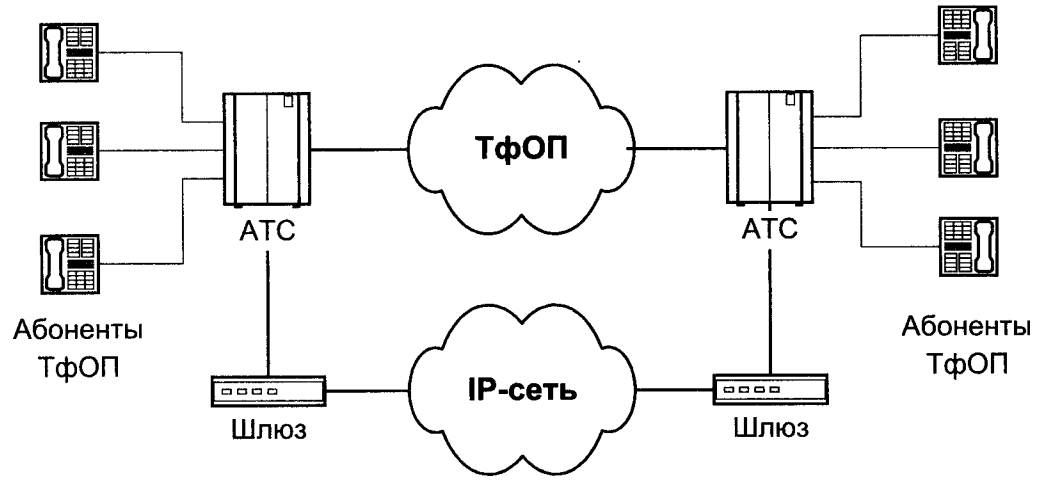


Рис. 1.8. Схема связи «телефон-телефон»

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.

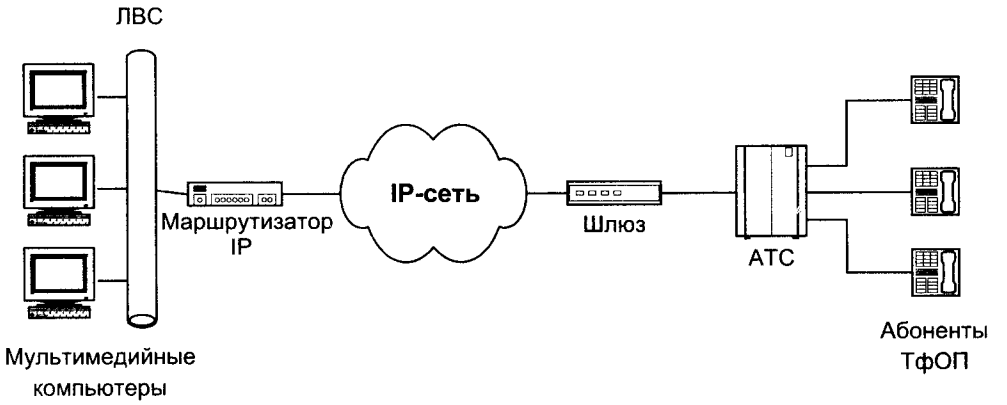


Рис. 1.9. Схема связи «компьютер-телефон»

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.

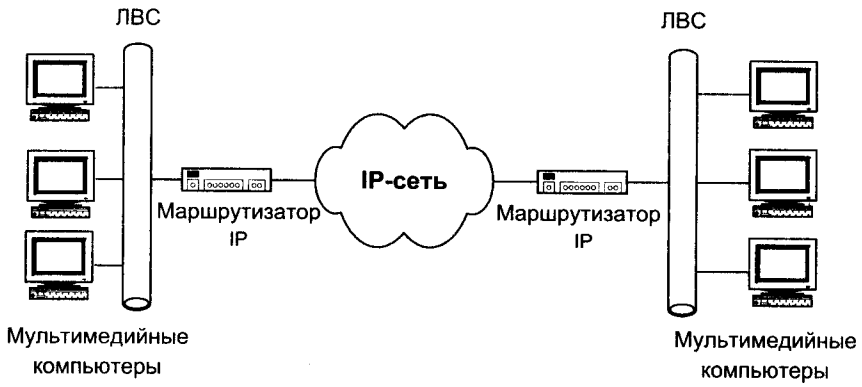


Рис. 1.10. Схема связи «компьютер-компьютер»

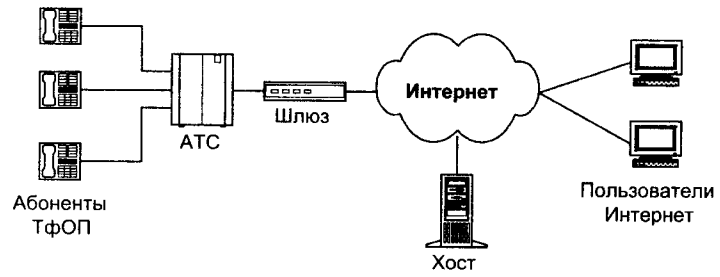


Рис. 1.11. Схема связи «WEB-браузер – телефон»

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 трафика 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 для 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 преимущества:

- 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 их 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 трафика 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 трафика 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 с успехом 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 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 (ТфОП). Для гарантии качества 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 установка 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 – это способ более эффективно использовать существующий 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.

Поэтому, несмотря на имеющее сегодня в мире место превышение объемов трафика данных над объемами голосового трафика в ближайшие годы не ожидается каких-либо революционных изменений, например, как полное вытеснение традиционных технологий передачи голоса.

1.7. Правовое регулирование IP-телефонии

Статус IP-телефонии в законодательстве Европы

В Европе статус IP-телефонии рассматривается в контексте дерегулирования и демонополизации услуг традиционной «голосовой телефонии». 20 октября 1995 г. специальная комиссия ЕЭС опубликовала Коммюнике, адресованное Европейскому Парламенту и Совету по поводу статуса и выполнения Директивы 90/388/ЕЭС о конкуренции на рынках телекоммуникационных услуг (95/C 275/02, OJ № C 275). В этом документе комиссия изложила свой подход к определению «голосовой телефонии», данному в Статье 1 Директивы 90/388/ЕЭС (в данной Директиве описаны услуги, которые государства-члены ЕЭС могут сохранять за своими регулируемыми государством телекоммуникационными операторами).

В свете появления новых технологий передачи голоса через Интернет комиссия приняла новое Дополнение к Коммюнике по поводу таких услуг.

В документе OJ № C6 от 10.1.1998 дается следующая оценка услуг интернет-телефонии на основании определения «голосовой телефонии», данного вышеуказанной Директивой

90/388/ЕЭС: «Комиссия считает, что определение «голосовая телефония» в Директиве 90/388/ЕЭС, рассматриваемое вместе с существующими прецедентами, дает хорошее руководство для оценки позиции услуг по голосовому сообщению в Интернете в условиях окололиберализационной ситуации по отношению к имеющемуся законодательству. Услуги интернет-телефонии не могут рассматриваться как «голосовая телефония» в той трактовке, которая изложена в Директиве и, таким образом, они уже переходят в, так называемую, «свободную зону» дерегулирования. В заключении к этому документу также сказано: «на основании того, что голосовое сообщение в Интернете рассматривается как услуга, отличная от услуги «голосовой телефонии» в трактовке Директивы, по нему не может быть затребовано никаких дополнительных сборов и лицензий от провайдеров услуг Интернет».

Статус IP-телефонии в законодательстве США

В США принято делить услуги связи на так называемые «базовые» (basic services) и «расширенные» (enhanced services). По определению Федеральной комиссии США по связи (FCC):

Базовые услуги – это обеспечение чистой передачи по линии связи, которая «прозрачна» с точки зрения взаимодействия с информацией клиента.

Расширенные услуги – это услуги, предлагаемые поверх существующих сетей связи (оказывающих базовые услуги), и/или:

- использующие компьютерные приложения, изменяющие формат, содержание, код, протокол или любой другой атрибут информации клиента;
- предоставляющие дополнительную или измененную информацию;
- требующие диалога пользователя для получения хранимой информации.

Иными словами, базовые услуги – это «передача без изменений в электрических сигналах», а расширенные – «создание, удаление и изменение информации».

Первые подлежат строгому регулированию, вторые являются предметом свободной конкуренции провайдеров Интернет.

Вопрос относительно Интернет-телефонии рассматривался Федеральной комиссией США по связи на основании аналитической записки, подготовленной Коалицией передачи голоса через сети (Voice on the Net Coalition).

На основании этого документа и ранее рассмотренных прецедентов передача голоса через сети пакетной передачи данных относится к «расширенным», поскольку:

1) компрессия и подавление пауз, используемые в интернет-телефонии – это есть анализ и удаление «лишней» информации, что не соответствует определению «базовых услуг», поскольку связано с изменением первоначальных данных (Определение компрессии в руководящем документе FCC «Computer», том II, с. 420);
2) пакетизация и добавление протокольной информации на основании раздела 64.702 Правил и Ограничений FCC (документы 55 RR 2d 104 и 95 FCC 2d 584) есть «расширенная услуга»;
3) передача голоса через сети пакетной ПД связана с временным хранением информации в оборудовании оператора, что противоречит основному признаку «базовых услуг» – «чистой передаче» информации, поскольку эта задержка не есть следствие самой передачи по сети или установленного пользователем приоритета;
4) компенсация потерянных пакетов и ошибок при передаче голоса по сетям пакетной ПД приводит к созданию дополнительной информации, не содержащейся первоначально в информации пользователя, что автоматически относит данный вид услуг к «расширенным».

Таким образом, Федеральная комиссия США по связи (FCC) не относит Интернет-телефонию к «базовым услугам», подлежащим специальному лицензированию или государственному регулированию, и эти услуги являются предметом свободной конкуренции провайдеров Интернет.

Правовое регулирование IP-телефонии в России

В России деятельность по предоставлению услуг Интернет-телефонии подлежит лицензированию. Интернет-телефония в силу ряда технологических и потребительских особенностей отличается от традиционной телефонной связи. Эти отличия учитываются при решении вопроса лицензирования деятельности операторов по предоставлению услуг Интернет-телефонии. Именно поэтому Интернет-телефония классифицируется как разновидность услуг **телематических служб**.

Компаниям, которые планируют заниматься Интернет-телефонией и уже владеют какой-либо лицензией на любую другую телематическую службу, необходимо подать заявку на **расширение** имеющейся лицензии. При отсутствии лицензии подается заявка на **новую** лицензию.

Нормативные документы, регулирующие деятельность операторов Интернет-телефонии в России, разрабатываются рабочей группой «Интернет-телефония» при Ассоциации документальной электросвязи (АДЭ).

Ввиду необходимости сертификации оборудования, используемого для передачи речевой информации по протоколу IP, Гостелеком России 12.11.99 г. утвердил **Руководящий Документ 45.046-99** «*Аппаратура связи, реализующая функции передачи речевой информации по сетям передачи данных с протоколом IP. Технические требования*». Сертификационные испытания оборудования на соответствие утвержденным требованиям проводит Испытательный центр документальной электросвязи.

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 реализаций 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 инициати-

вах производителей аппаратно-программного обеспечения IP-телефонии. Далее дается краткое описание наиболее значимых 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 трафика 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 трафика 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 пакетами 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

Таблица 2.1 (окончание). Организации, участвующие в стандартизации IP-телефонии

Softswitch Consortium	www.soft-switch.org	Учрежден в 1999 г., более 50 членов	Основное внимание уделяет протоколу SIP/MGCP и другим технологиям взаимодействия сетей
Internet & Telecoms Convergence Consortium	itel.mit.edu	Академии/ корпорации	Выпускает технические, экономические и технологические обзоры
Промышленные инициативы	URL	Учредители	Основные направления деятельности
Interoperability Now! (iNow)	www.imtc.org /act_inow.htm	ITXC, Lucent, VocalTec	Стандартный профиль взаимодействия систем IP-телефонии различных производителей и провайдеров, основанный на H.323
IP Call Detail Record Initiative (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	Jeff Pulver и 22 соучредителя	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 (IP-телефония), передачи звука и видео (видеотелефония), а также 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 телефо-

нов 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 рекомендация 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. Рекомендация 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.

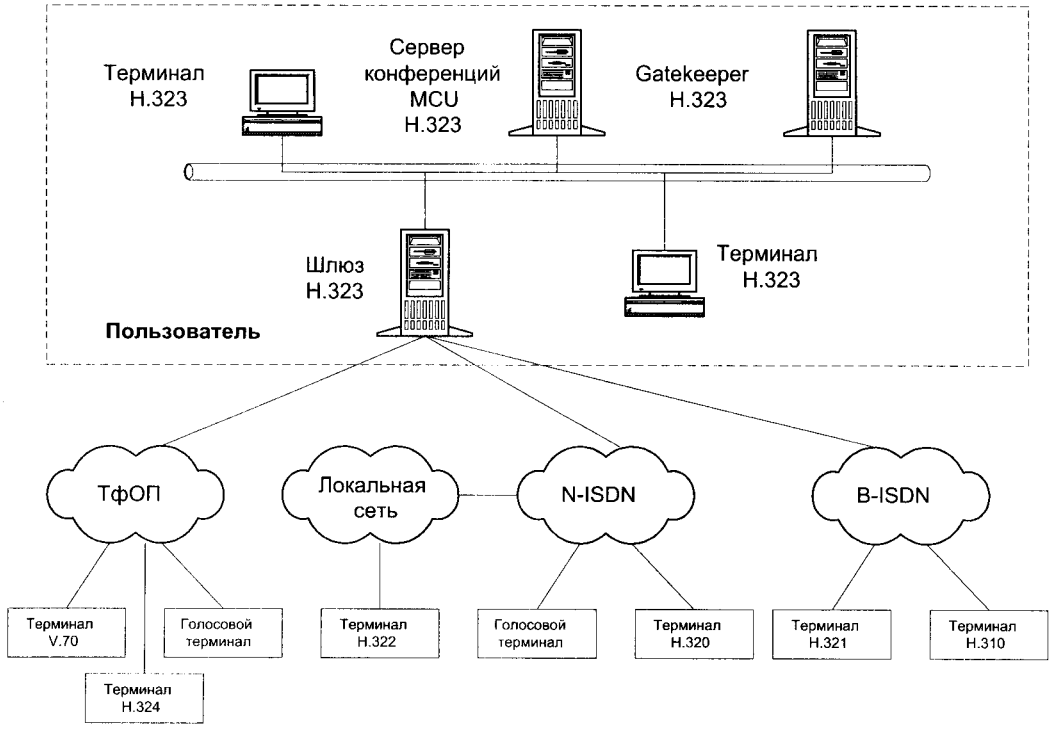


Рис. 2.1. Конфигурация сети на базе стандарта H.323

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

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 трафика.

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.

2.3. Стандарты ETSI

Европейский институт стандартизации телекоммуникаций ETSI разрабатывает проект, получивший название **TIPHON** (Telecommunications and IP Harmonization over 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.164. 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 (рис. 2.5). 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 и 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

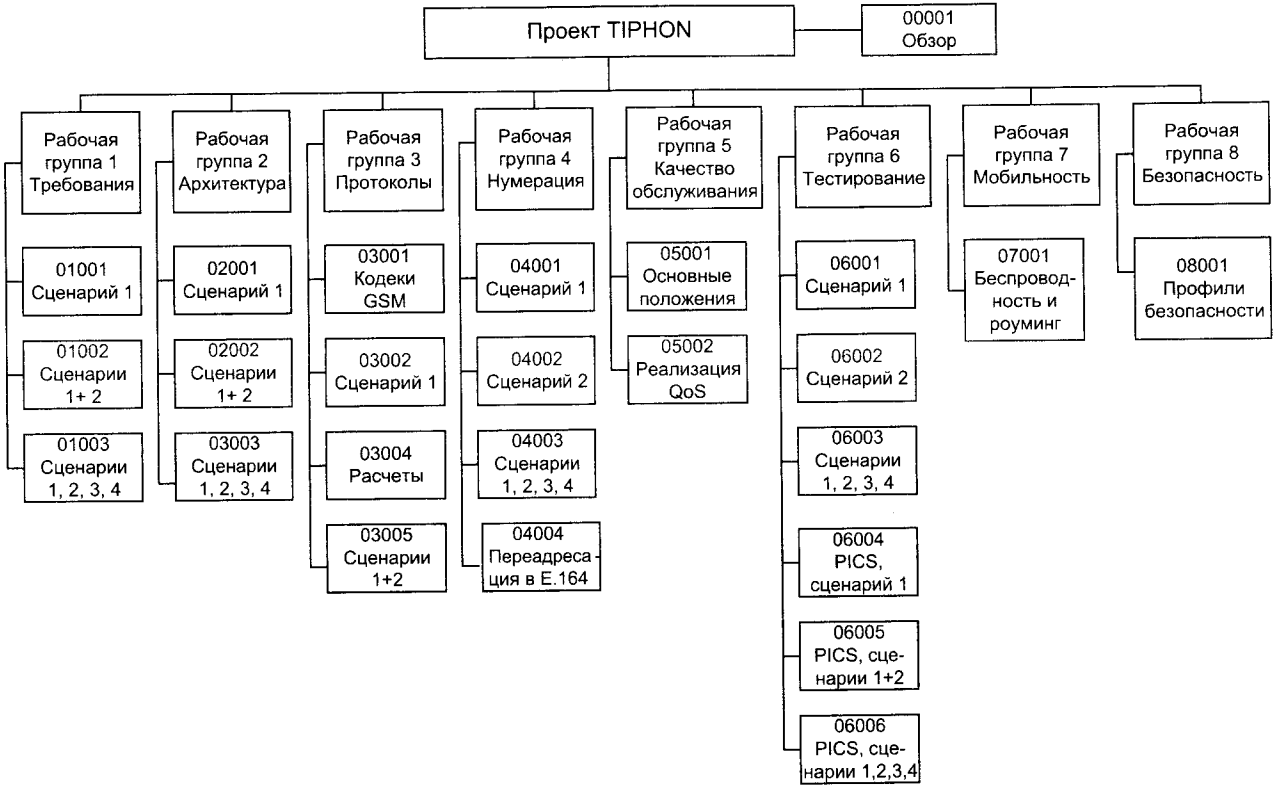


Рис. 2.2. Структура проекта TIPHON

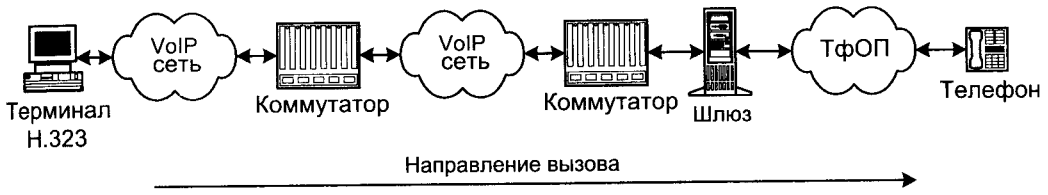


Рис. 2.3. Сценарий 1 проекта TIPHON

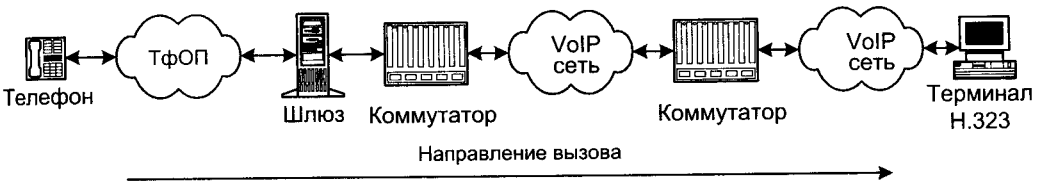


Рис. 2.4. Сценарий 2 проекта TIPHON

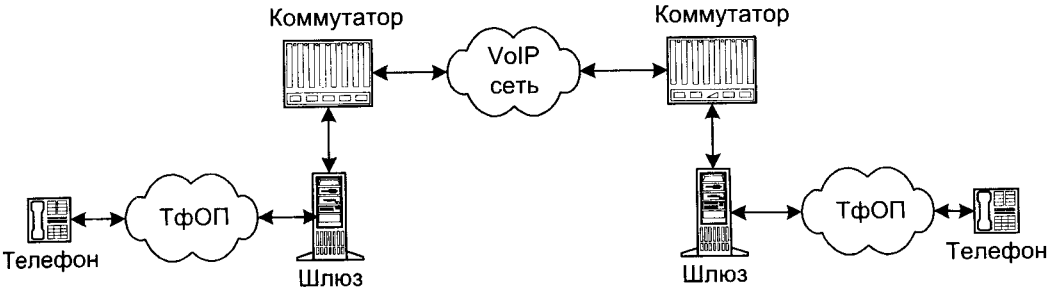


Рис. 2.5. Сценарий 3 проекта TIPHON

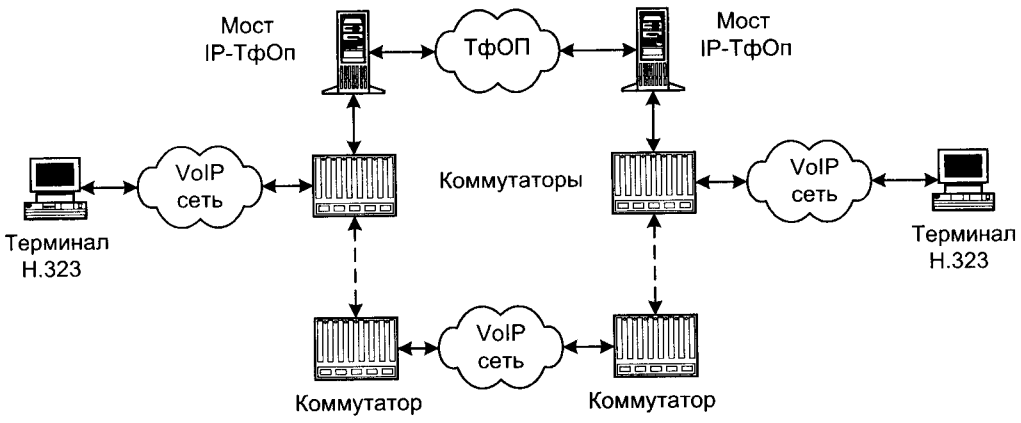


Рис. 2.6. Сценарий 4 проекта TIPHON

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 *(RTP, Real-time Transport Protocol)*. Протокол описан в документе RFC 1889, а также включен в 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, 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 в 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 Transport Control Protocol, RTCP)*. С помощью протокола RTCP программы могут приспосабливаться к изменяющимся нагрузкам на сеть, уведомляя отправителей и получателей о всплесках (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 рабочая 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 могут 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 трафика 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 ус тановления 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).

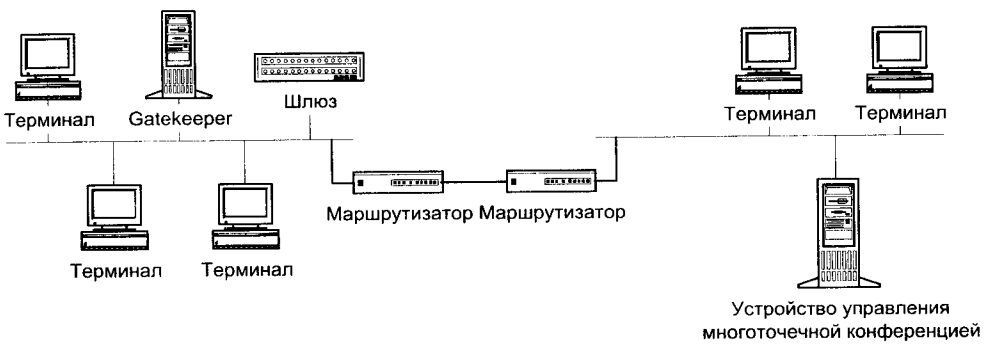


Рис. 3.1. Зона H.323

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 Selsius 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.

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.

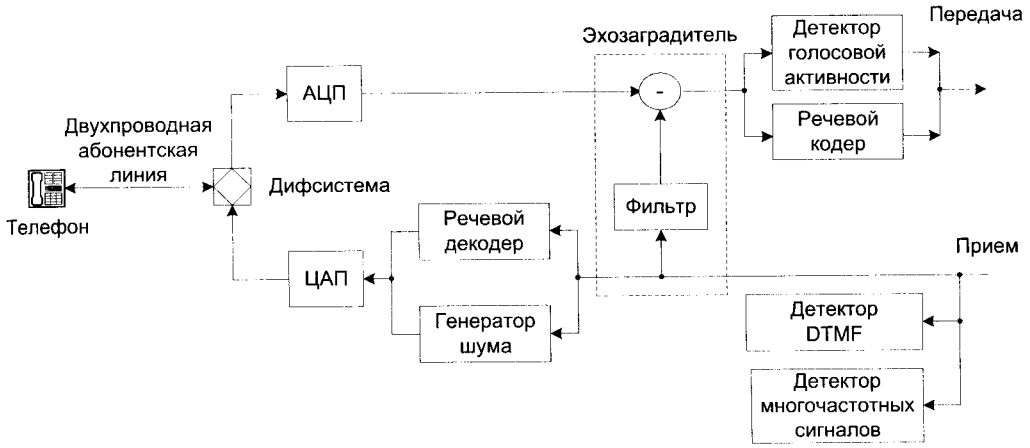


Рис. 3.2. Схема обработки сигналов в шлюзе

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 A-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.165. 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 пере-

дается 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 информационный кадр, либо флаг наличия паузы. На паузных кадрах вместо речевого синтезатора 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 декодер, 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 A – 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 акустического 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 может 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 Lucent 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 Lucent 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 это м 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.

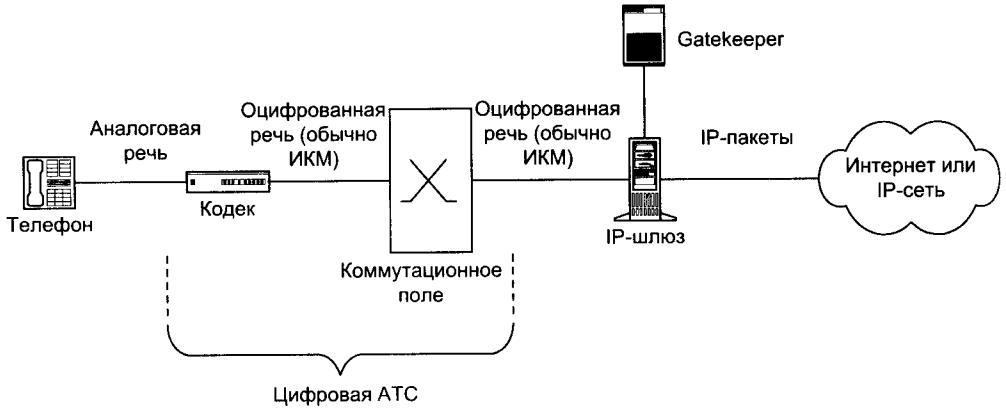


Рис. 3.3. Положение шлюза в сети IP-телефонии

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 для организации голосового трафика. 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 и типов сигнализаций

Важными критериями при оценке характеристик шлюзов является возможно большое разнообразие телефонных интерфейсов, поддерживаемых IP-шлюзом (E1, 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 Multiservice 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, G.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 ECI 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 E1-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 наметилась 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). Установка 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, представляющие собой конструктивно модули для классических учрежденческих АТС. Компании Lucent Technologies и Nortel Networks производят их для своих станций Definity и Meridian 1. 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 10BaseT (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 соединители 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 Sphere

Communications). Такие устройства оборудованы портами RJ-11 для подключения обычного 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 InternetPhone фирмы Vocaltec Communications. Недостатками таких 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 TIPHON

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 того, 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 сети: 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 использования ресурсов;
- управление.

Разработанная в рамках проекта TIPHON модель сети, 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 по событиям, связанным с прохождением информационного потока. Показанные на рис 3.4 службы поддержки могут быть использованы для аутентификации, биллинга, преобразования адресов и других задач.

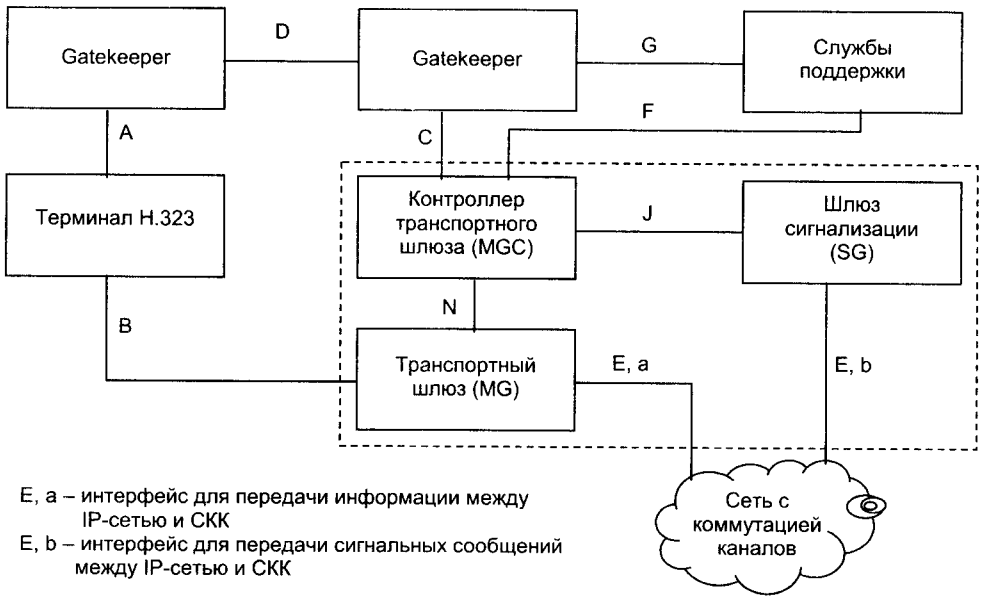


Рис. 3.4. Функциональная архитектура, предложенная в рамках проекта TIPHON

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 интегри-

рована 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.

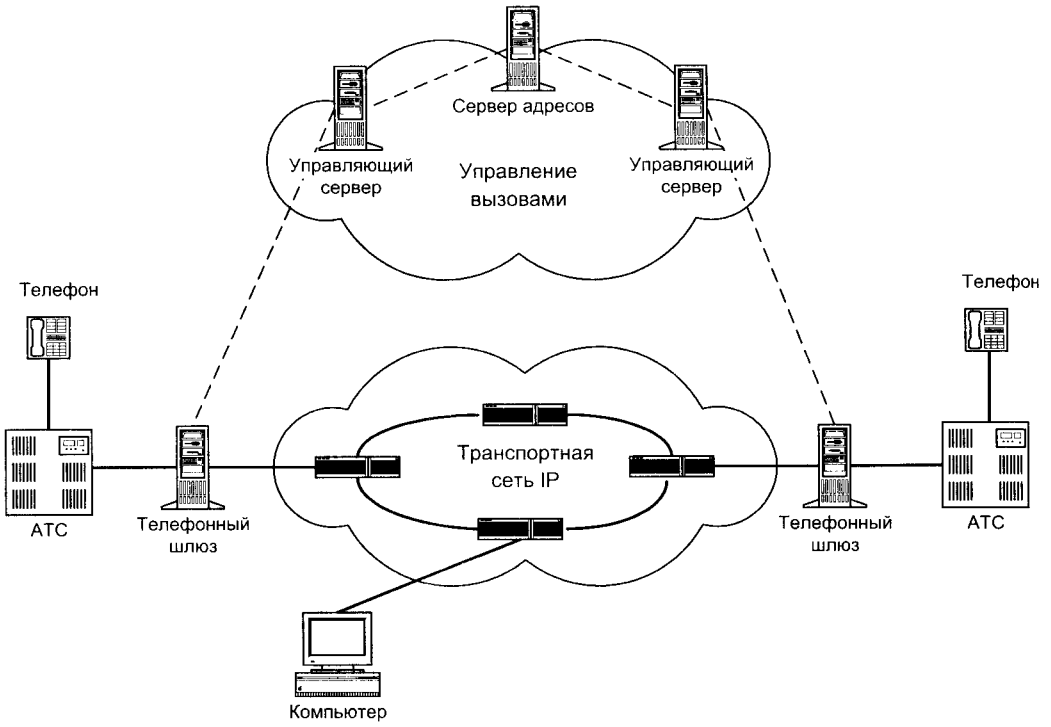


Рис. 4.1. Управление вызовами в сети IP-телефонии

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. Такие средства должны осуществлять контроль за доступом и использованием сетевых ресурсов и выполне-

нием соглашений по качеству обслуживания. При их отсутствии оператору может оказаться проблематичным гарантировать пользователю определенный класс обслуживания, если его трафик 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.

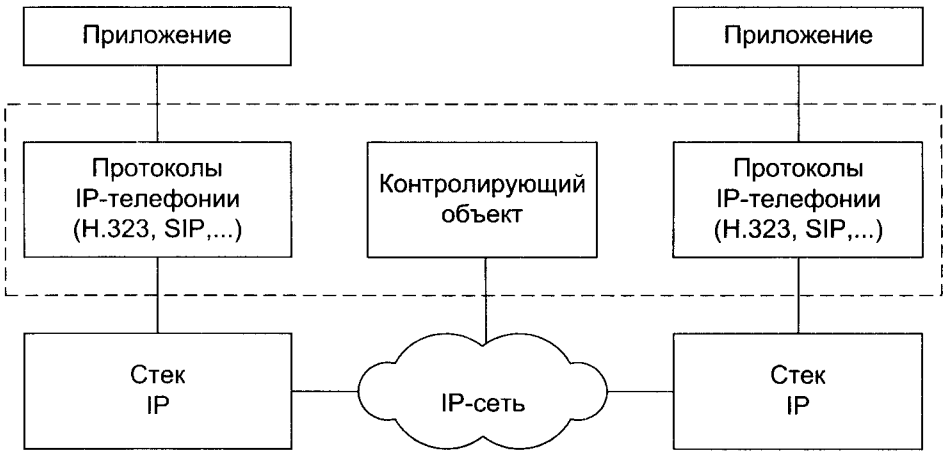


Рис. 4.2. Механизмы сигнализации IP-телефонии в протокольном стеке

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.323 (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 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.

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

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

Сигнализация RAS

Протокол сигнализации RAS (регистрации, подтверждения и состояния) применяется для передачи служебных сообщений между терминалами и контроллером зоны H.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 H.225.0. Канал сигнализации RAS не зависит от канала управления вызовом и канала управления H.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 сигнализации RAS).

Мнемонический адрес служит для адресации оконечного оборудования в удобной пользователю форме. Адресом может быть телефонный номер в формате E.164, телефонный

номер в корпоративной сети, адрес электронной почты и т.д. Gatekeeper не имеет мнемонического адреса.

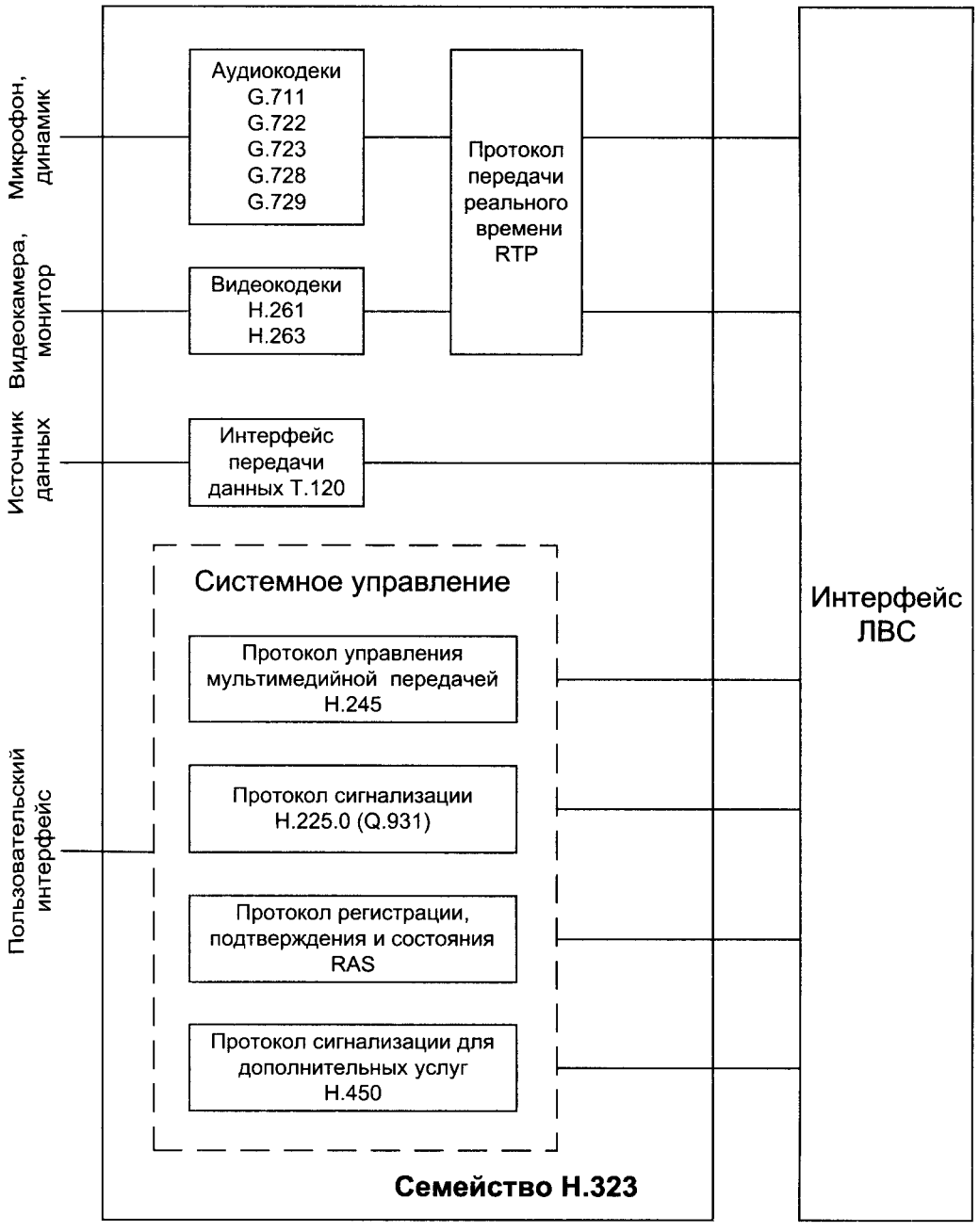


Рис. 4.3. Совокупность рекомендаций H.323

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 оконечного 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 оконечным 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 производителем 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 оставить его до конца сеанса связи, если поддерживаются дополнительные услуги.

* Почти не отличается от сигнализации Q.931
** Выдача адресов и номеров сеансов для RTP
*** Обеспечивается, в частности, контроль качества обслуживания

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

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.

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 трафика. Канал управления вызовами H.225.0 используется для установления и разрыва соединений между двумя терминалами H.323, а также между терминалом и шлюзом. Служебные сообщения этого протокола передаются поверх TCP или UDP (рис. 4.5). Соответствующий механизм H.225.0 основан на протоколе Q.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.

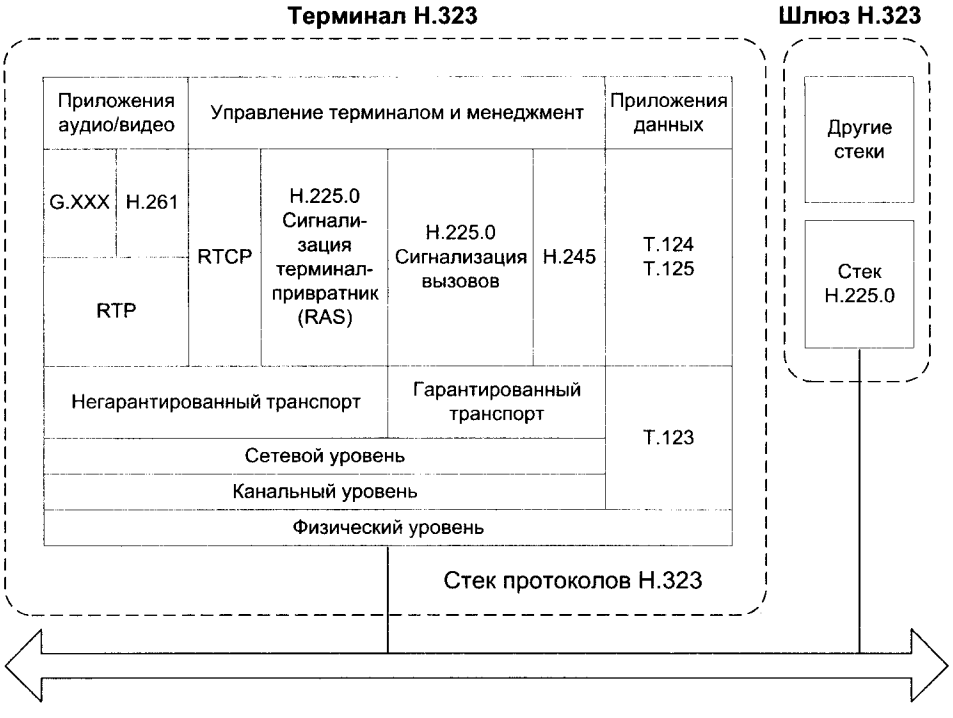


Рис. 4.5. Положение H.225.0 в стеке протоколов H.323

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 «0», 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 трафика.

С помощью сигнализации Q.931 согласно рекомендации МСЭ-Т H.225.0 и протоколу управления H.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 H.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 H.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 H.245, а открыт с новыми параметрами сообщением open Logical Channel.

Соединение разъединяется следующим образом:

- инициатор разъединения должен закрыть канал сообщением close Logical Channel, передаваемым по каналу управления H.245;
- инициатор разъединения должен передать сообщение end Session Command, передаваемым по каналу управления H.245;
- удаленное оборудование дожидается сообщения end Session Command, передаваемое по каналу управления H.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

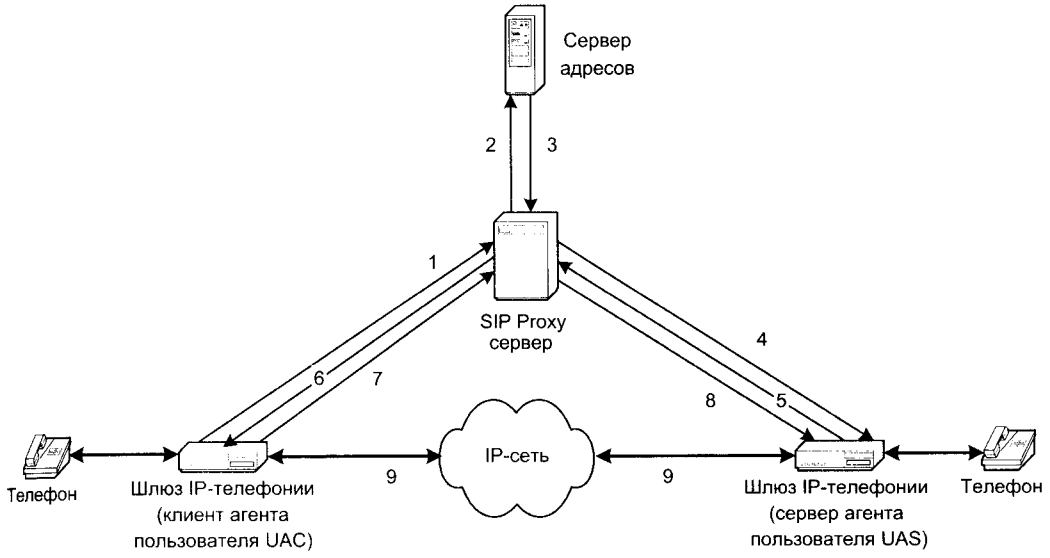
Протокол SIP (Session Initiation Protocol) является протоколом прикладного уровня, разработанным рабочей группой по управлению многоточечными сеансами мультимедиасвязи (MMUSIC) организации IETF (Рекомендация RFC 2543). Он позволяет организовать и провести такой сеанс, обеспечивая его установление, модификацию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



1. SIP INVITE
2. Поиск сервера адресов
3. Ответ сервера адресов
4. Пересылка INVITE
5. Ответ
6. Пересылка ответа
7. ACK
8. Пересылка ACK
9. Мультимедийный поток

Рис. 4.6. Схема сигнализации по протоколу SIP

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. 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@IPadress) 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 преобразование 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, описания канала мультимедийной связи и т.д. Для биллинга, например, может использоваться протокол Radius.

В работах над протоколом SIP участвуют ведущие производители сетевого и телекоммуникационного оборудования (Cisco Systems, Lucent Technologies, 3Com) и крупнейшие операторы (AT&T, MCI, 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 eConvergence 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.

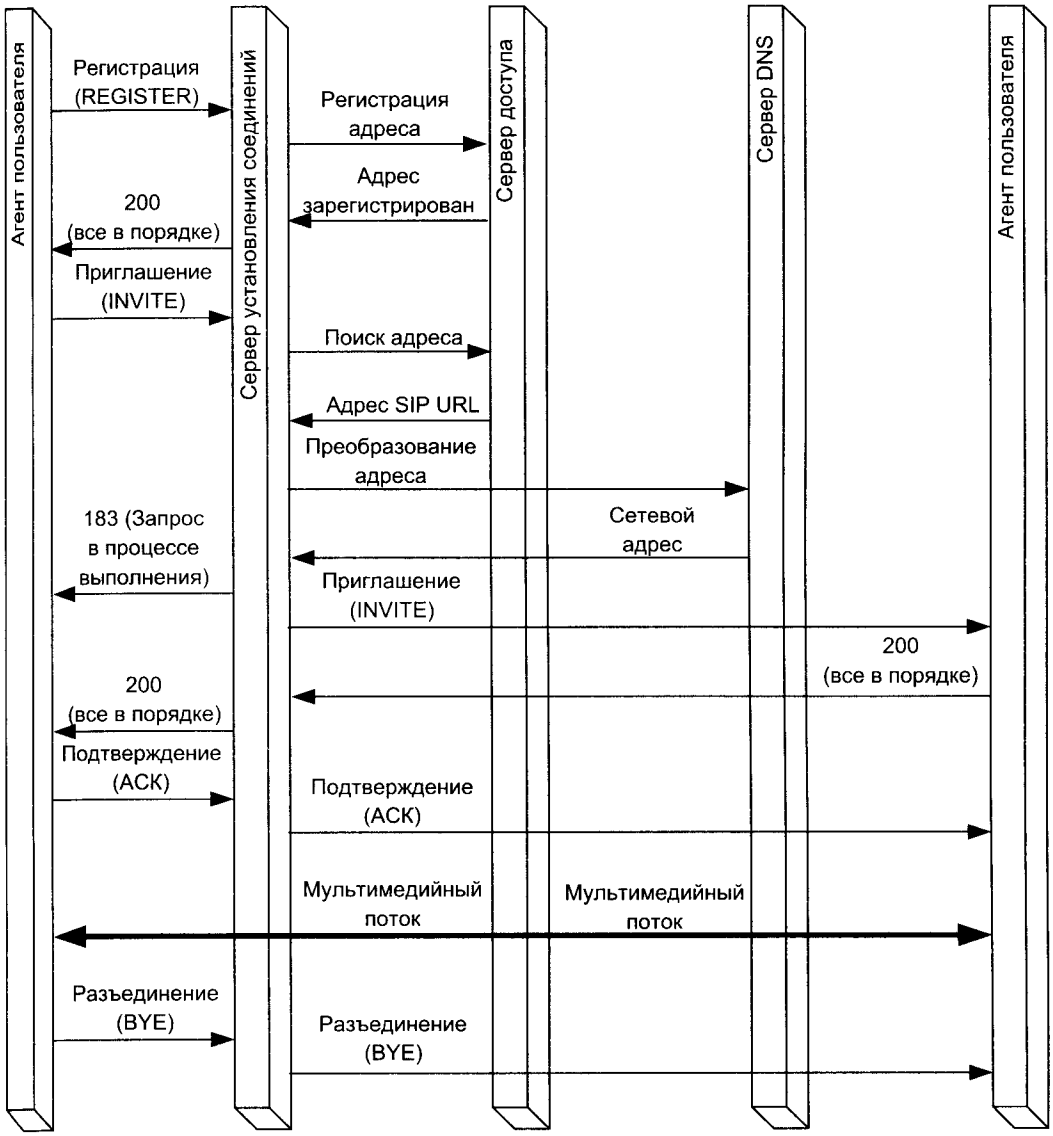


Рис. 4.7. Возможный сценарий установления и завершения сеанса связи по протоколу SIP

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 с 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.

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 аутентификация. 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 подходит 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 – Signalling Gate-

way), транспортный шлюз (MG – Media Gateway) и контроллер транспортного шлюза (MGC – Media Gateway Controller) (рис. 4.8).

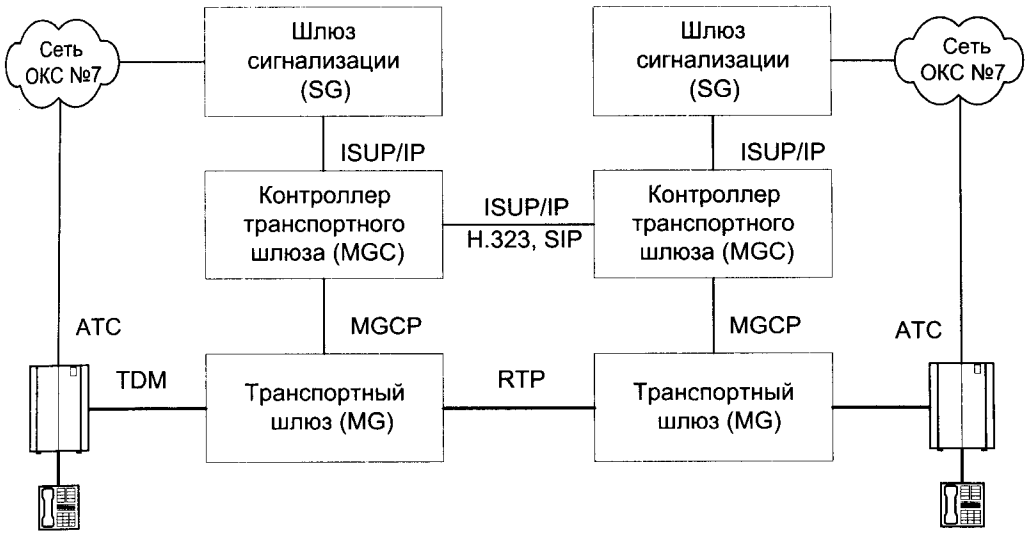


Рис. 4.8. Функциональная модель сети по проекту TIPHON

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 трафика, 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, фор-

мированием тональных сигналов (готовности к набору номера, контроля посылки вызова, «занято» и пр.), эхо-подавлением, использованием кодеков (G.711, G.723.1, G.729, GSM и 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 достаточно 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.

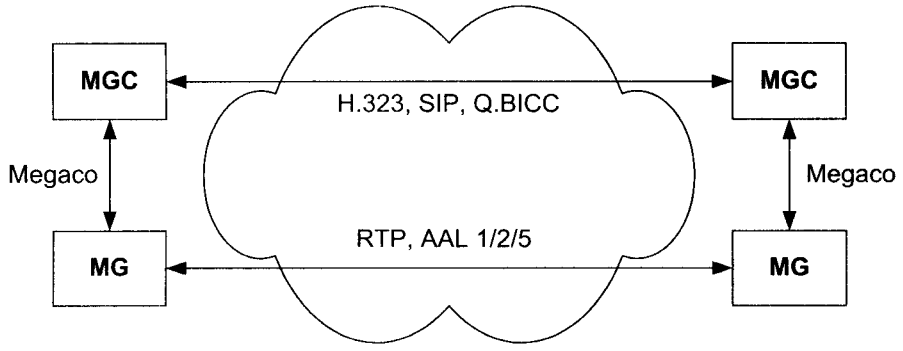


Рис. 4.9. Использование протокола Megaco в сети IP-телефонии

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, транспорт-

ным 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 [70].

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 планами 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.

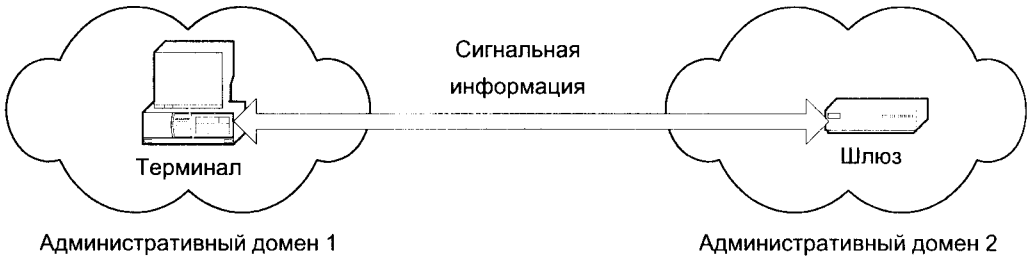


Рис. 4.10. Пример взаимодействия двух доменов

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) не 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:

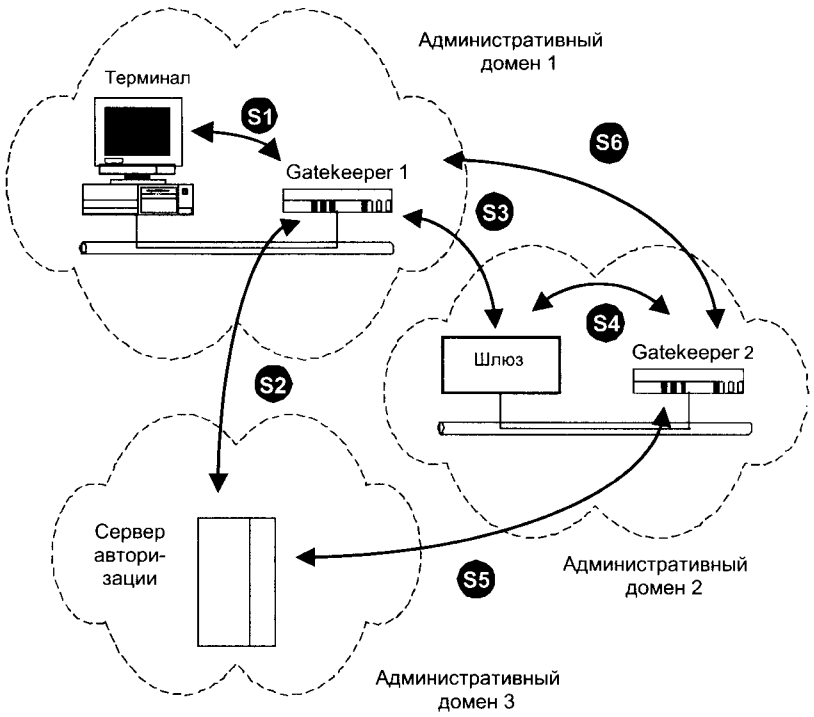


Рис. 4.11. Пример взаимодействия трех доменов

S1: 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.

Глава 5

ОБЕСПЕЧЕНИЕ КАЧЕСТВА IP-ТЕЛЕФОНИИ

5.1. Показатели качества IP-телефонии

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

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

Для приложений, где не важен порядок и интервал прихода пакетов, например, e-mail, время задержек между отдельными пакетами не имеет решающего значения. IP-телефония является одной из областей передачи данных, где важна динамика передачи сигнала, которая обеспечивается современными методами кодирования и передачи информации, а также увеличением пропускной способности каналов, что приводит к возможности успешной конкуренции IP -телефонии с традиционными телефонными сетями.

Основными составляющими качества IP -телефонии являются (рис. 5.1):

- Качество речи, которое включает:
  - *диалог* – возможность пользователя связываться и разговаривать с другим пользователем в реальном времени и полнодуплексном режиме;
  - *разборчивость* – чистота и тональность речи;
  - *эхо* – слышимость собственной речи;
  - *уровень* – громкость речи.
- Качество сигнализации, включающее:
  - *установление вызова* – скорость успешного доступа и время установления соединения;
  - *завершение вызова* – время отбоя и скорость разъединения;
  - *DTMF* – определение и фиксация сигналов многочастотного набора номера.

Факторы, которые влияют на качество IP-телефонии, могут быть разделены на две категории:

- Факторы качества IP-сети:
  - *максимальная пропускная способность* – максимальное количество полезных и избыточных данных, которая она передает;
  - *задержка* – промежуток времени, требуемый для передачи пакета через сеть;
  - *джиттер* – задержка между двумя последовательными пакетами;
  - *потеря пакета* – пакеты или данные, потерянные при передаче через сеть.

- Факторы качества шлюза:
  - *требуемая полоса пропускания* – различные вокодеры требуют различную полосу. Например, вокодер G.723 требует полосы 16,3 кбит/с для каждого речевого канала;
  - *задержка* – время, необходимое цифровому сигнальному процессору DSP или другим устройствам обработки для кодирования и декодирования речевого сигнала;
  - *буфер джиттера* – сохранение пакетов данных до тех пор, пока все пакеты не будут получены и можно будет передать в требуемой последовательности для минимизации джиттера;
  - *потеря пакетов* – потеря пакетов при сжатии и/или передаче в оборудовании IP-телефонии;
  - *подавление эхо* – механизм для подавления эхо, возникающего при передаче по сети;
  - *управление уровнем* – возможность регулировать громкость речи.

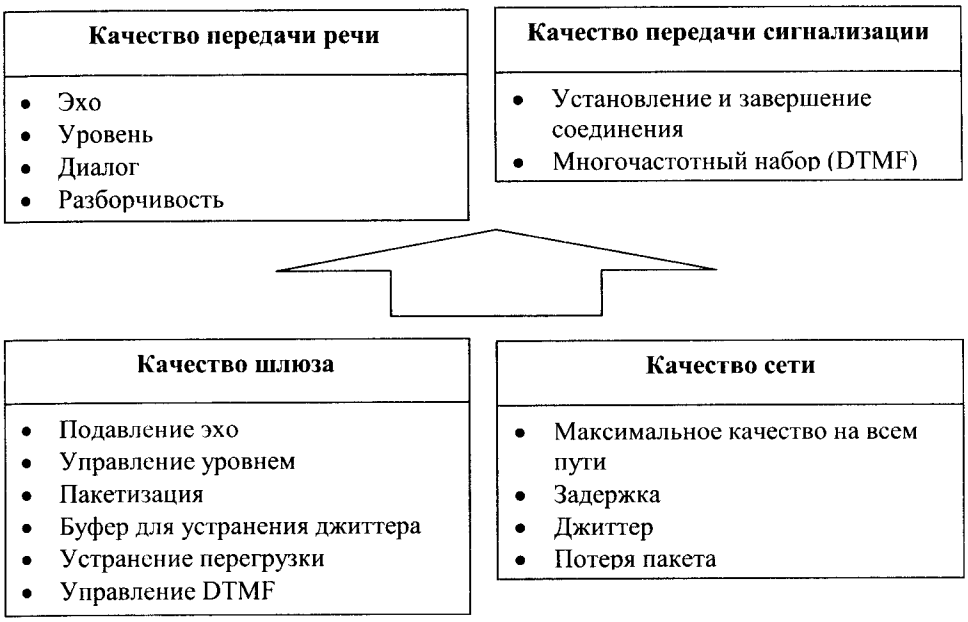


Рис. 5.1. Факторы, влияющие на качество IP-телефонии

5.2. Влияние сети на показатели качества IP-телефонии

Задержка

Задержка создает неудобство при ведении диалога, приводит к перекрытию разговоров и возникновению эхо. Эхо возникает в случае, когда отраженный речевой сигнал вместе с сигналом от удаленного конца возвращается опять в ухо говорящего. Эхо становится трудной проблемой, когда задержка в петле передачи больше, чем 50 мс. Так как эхо является проблемой качества, системы с пакетной коммутацией речи должны иметь возможность управлять эхо и использовать эффективные методы эхоподавления.

Затруднение диалога и перекрытие разговоров становятся серьезным вопросом качества, когда задержка в одном направлении передачи превышает 250 мс. Можно выделить следующие источники задержки при пакетной передачи речи из конца в конец (рис. 5.2).

- *Задержка накопления* (иногда называется алгоритмической задержкой): эта задержка обусловлена необходимостью сбора кадра речевых отсчетов, выполняемая в речевом кодере. Величина задержки определяется типом речевого кодера и изменяется от небольших величин (0,125 мкс) до нескольких миллисекунд. Например, стандартные речевые кодеры имеют следующие длительности кадров:

  G.729 CS-ACELP (8 кбит/с) – 10 мс
  G.723.1 –Multi Rate Coder (5,3; 6,3 кбит/с) – 30 мс.
- *Задержка обработки*: процесс кодирования и сбора закодированных отсчетов в пакеты для передачи через пакетную сеть создает определенные задержки. Задержка кодирования или обработки зависит от времени работы процессора и используемого типа алгоритма обработки. Для уменьшения загрузки пакетной сети обычно несколько кадров речевого кодера объединяются в один пакет. Например, три кадра кодовых слов G.729, соответствующих 30 мс речи, могут быть объединены для уменьшения размера одного пакета.
- *Сетевая задержка*: задержка обусловлена физической средой и протоколами, используемыми для передачи речевых данных, а также буферами, используемыми для удаления джиттера пакетов на приемном конце. Сетевая задержка зависит от емкости сети и процессов передачи пакетов в сети.

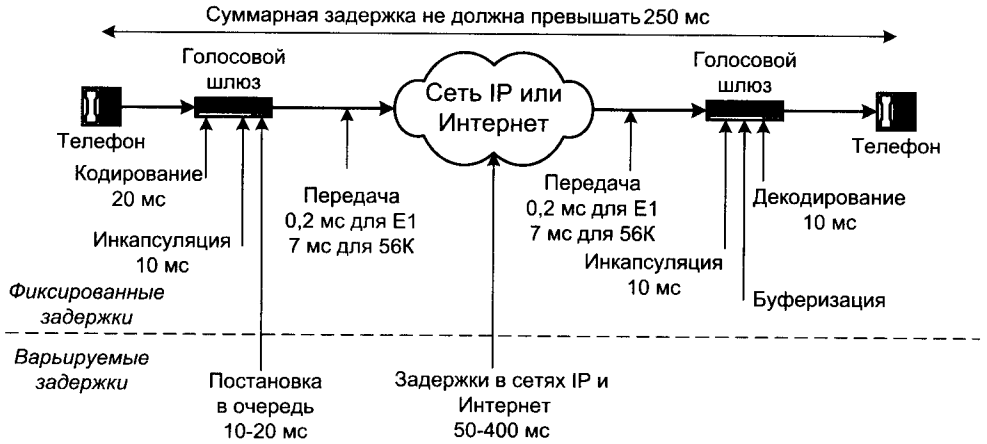


Рис. 5.2. Составляющие задержки в сети IP-телефонии

Время задержки при передаче речевого сигнала можно отнести к одному из трех уровней:

первый уровень до 200 мс – отличное качество связи. Для сравнения, в телефонной сети общего пользования допустимы задержки до 150-200 мс;

второй уровень до 400 мс – считается хорошим качеством связи. Но если сравнивать с качеством связи по сетям ТфОП, то разница будет видна. Если задержки постоянно удерживается на верхней границе 2-го уровня (на 400 мс), то не рекомендуется использовать эту связь для деловых переговоров;

третий уровень до 700 мс – считается приемлемым качеством связи для ведения неделовых переговоров. Такое качество связи возможно также при передаче пакетов по спутниковой связи.

Качество Интернет-телефонии попадает под 2-3 уровни, причем невозможно уверенно сказать, что тот или иной провайдер Интернет-телефонии работает по второму уровню, так как задержки в сети Интернет изменчивы. Более точно можно сказать о провайдерах IP-телефонии, работающих по выделенным каналам. Они попадают под 1-2 уровни. Также необходимо учитывать задержки при кодировании/декодировании голосового сигнала. Средние суммарные задержки при использовании IP-телефонии обычно находятся в пределах 150-250 мс.

В сети Интернет задержки пакетов существенно зависят от времени. Кривая этой зависимости имеет большой динамический диапазон и скорость изменения. Заметные изменения времени распространения могут произойти на протяжении одного непродолжительного сеанса связи, а колебания времени передачи могут быть в диапазоне от десятков до сотен миллисекунд и даже превышать секунду.

Важно отметить тот факт, что задержки в сетях с коммутацией пакетов влияют не только на качество передачи речевого трафика в реальном времени. Не менее важно и то, что данные задержки в определенных ситуациях могут нарушить правильность функционирования телефонной сигнализации в цифровых трактах E1/T1 на стыке голосовых шлюзов с оборудованием коммутируемых телефонных сетей. Причиной этого можно назвать тот факт, что набор рекомендаций H.323 в момент своего появления в 1997 г. был ориентирован на мультимедийные приложения, осуществляющие аудио и видеоконференцсвязь через сети IP. Данное решение позволяло значительно снизить стоимость таких систем по сравнению с их аналогами, работающими в сетях традиционной телефонии с коммутацией каналов. В процессе выделения IP-телефонии в самостоятельное направление и развития ее до услуги операторского уровня возникла необходимость соединения IP-шлюзов с телефонными станциями ТфОП по цифровым трактам E1/T1. При этом, шлюзы осуществляют взаимодействие с цифровыми АТС, используя стандартные механизмы телефонной сигнализации Q.931, интерпретированные через команды H.225 и транслируемые в IP-сети с использованием протокола TCP. Согласно рекомендации Q.931, при установлении телефонного соединения значения временных задержек между фазами выполнения команд сигнализации строго регламентированы. Однако, при интерпретации в IP-шлюзах команд телефонной сигнализации Q.931 стеком H.225/TCP/IP, задержки, возникшие на пути прохождения сигнала, увеличивают заданные временные интервалы между командами Q.931, и в большинстве случаев нарушают целостность функционирования данного протокола. Хотя версия 2 набора рекомендаций H.323 в фазе 2 предусматривает процедуру H.323v2 Fast Connect, ускоряющую обработку команд Q.931 стеком H.225/TCP, задержки IP-канала, особенно характерные для инфраструктуры Интернет, могут заведомо превышать все допустимые значения временных интервалов протокола Q.931. Данное обстоятельство можно расценивать как еще один аргумент в пользу использования выделенных каналов при построении сетей IP-телефонии.

Джиттер

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

1. джиттер, зависимый от данных (Data Dependent Jitter – DDJ) – происходит в случае ограниченной полосы пропускания или при нарушениях в сетевых компонентах;

2. искажение рабочего цикла (Duty Cycle Distortion – DCD) – обусловлено задержкой распространения между передачей снизу вверх и сверху вниз;
3. случайный джиттер (Random Jitter – RJ) – является результатом теплового шума.

На рис. 5.3 приведены гистограммы джиттера пакетов в локальной сети и в сети Интернет с различными скоростями работы, показывающие эмпирические распределения вероятностей задержек. На оси абсцисс отложена относительная задержка, характеризующая реальное положение пакета в последовательности на временной оси по отношению к идеальному в предположении, что первый пакет пришел без задержки.

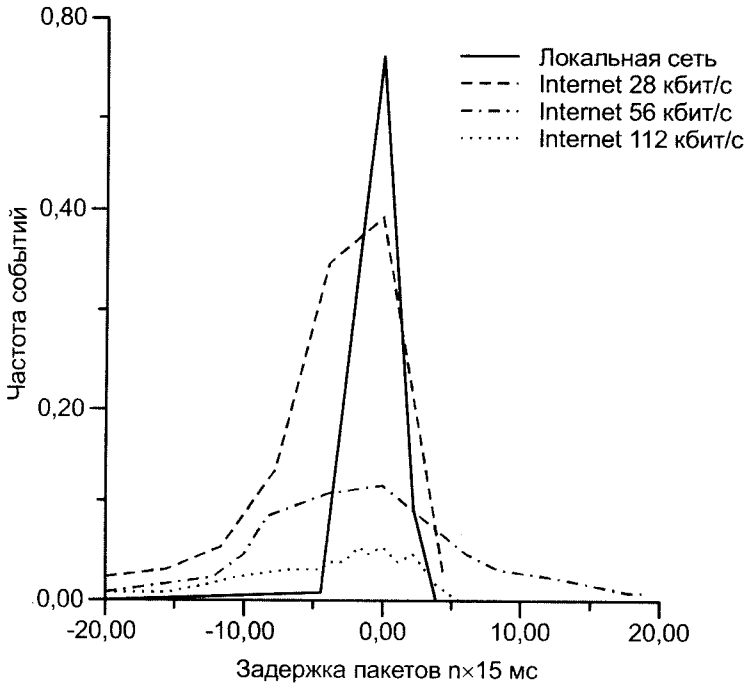


Рис. 5.3. Гистограммы джиттера пакетов

Величины возникающих задержек и их вероятности важны для организации процедуры обработки и выбора параметров обработки. Понятно, что временная структура речевого пакетного потока меняется. Возникает необходимость организации буфера для превращения пакетной речи, отягощенной нестационарными задержками в канале, возможными перестановками пакетов, в непрерывный естественный речевой сигнал реального времени. Параметры буфера определяются компромиссом между величиной запаздывания телефонного сигнала в режиме дуплексной связи и процентом потерянных пакетов. Потеря пакетов является другим серьезным негативным явлением в IP-телефонии.

Потеря пакетов

Потерянные пакеты в IP-телефонии нарушают речь и создают искажения тембра. В существующих IP-сетях все голосовые кадры обрабатываются как данные. При пиковых на-

грузках и перегрузках голосовые кадры будут отбрасываться, как и кадры данных. Однако кадры данных не связаны со временем и отброшенные пакеты могут быть успешно переданы путем повторения. Потеря голосовых пакетов, в свою очередь, не может быть восполнена таким способом и в результате произойдет неполная передача информации. Предполагается, что потеря до 5% пакетов незаметна, а свыше 10-15% – недопустима. Причем данные величины существенно зависят от алгоритмов компрессии/декомпрессии.

На рис. 5.4 представлены гистограммы потерь пакетов. По оси абсцисс отложено число подряд потерянных пакетов. Анализ гистограммы показывает, что наиболее вероятны потери одного, двух и трех пакетов. Потери больших пачек пакетов редки.

Рис. 5.4. Гистограммы потерь пакетов

Существенно, что потеря большой группы пакетов приводит к необратимым локальным искажениям речи, тогда как потери одного, двух, трех пакетов можно пытаться компенсировать.

Интуитивно ясно, что с повышением трафика возрастают задержки и потери в телефонном канале. В условиях ограниченных пропускных способностей это проявляется не только при интегральном увеличении загрузки каналов, например, в часы наибольшей нагрузки, но и при увеличении потока локального источника информации. Кривые графиков рис. 5.3 и 5.4, построенные для различных скоростей передачи информации, убедительно свидетельствуют о необходимости использования как можно более низких скоростей передачи речевой информации при естественном требовании обеспечения желаемого качества телефонной связи.

Взаимосвязь методов обеспечения качества IP-телефонии, показателей качества сети и качества вызова представлена на рис. 5.5.

5.3. Процедуры обработки речи в IP-телефонии

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

1. Устранение всех нежелательных компонентов из входного аудиосигнала. После оцифровки речи необходимо удалить эхо из динамика в микрофон, комнатное эхо и непрерывный фоновый шум (например, шум от вентиляторов), а также отфильтровать шумы переменного тока на низких частотах звукового спектра.

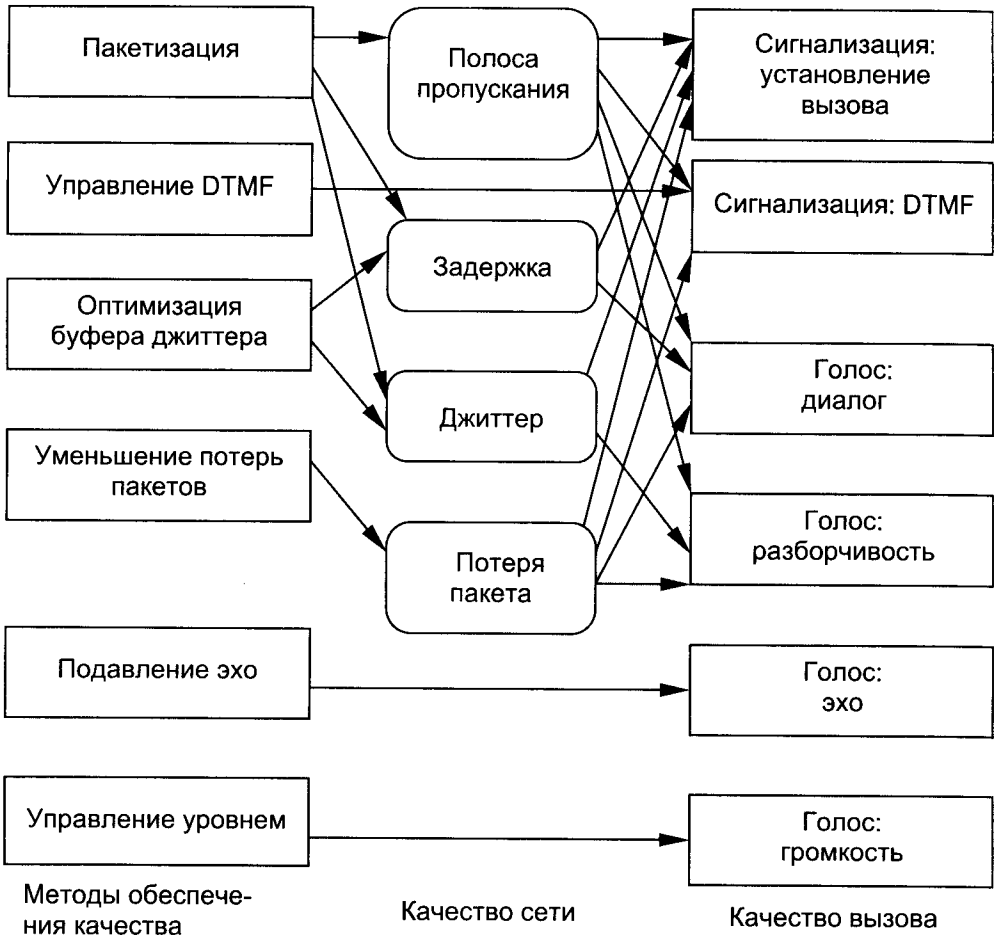


Рис. 5.5. Схема обеспечения качества IP-телефонии

Эффективное эхоподавление и уменьшение шумов абсолютно необходимо в любой конфигурации с «открытым микрофоном» и с громкоговорителем на базе персонального компьютера (ПК) для традиционной и IP-телефонии. Эти функции все в большей мере реализуются аудиокомпонентами ПК, так что сама система IP-телефонии может их и не иметь. Шлюзам IP-телефонии требуется выполнять меньший объем предварительной обработки, нежели конечным решениям, потому что УАТС и телефонная сеть обеспечивают фильтрацию и уменьшение шумов.

2. Подавление пауз в речи; распознавание остаточного фонового шума (внешних шумов) и кодирование для восстановление на дальнем конце; то же самое для опознаваемых сигналов. Паузы лучше всего полностью подавлять на ближнем конце. Для сохранения окружающих звуков необходимо смоделировать фоновые шумы, чтобы система на дальнем конце могла восстановить их для слушателя. Сигналы многочастотного набора номера DTMF и другие сигналы можно заменить на короткие коды для восстановления на дальнем конце (или для непосредственной обработки). Возможные проблемы: из-за того, что функция по-

давления пауз активизируется, когда громкость речи становится ниже определенного порога, некоторые системы обрезают начала и концы слов (в периоды нарастания и снижения энергии речи).

3. Сжатие голосовых данных. Сжать оцифрованный голос можно разными способами. В идеале решения, используемые для IP-телефонии, должны быть достаточно быстрыми для выполнения на недорогих цифровых сигнальных процессорах DSP, сохранять качество речи и давать на выходе небольшие массивы данных.

4. «Нарезание» сжатых голосовых данных на короткие сегменты равной длины, их нумерация по порядку, добавление заголовков пакетов и передача. Хотя стек протоколов TCP/IP поддерживает пакеты переменной длины, их использование затрудняет достижение устойчивой и предсказуемой межсетевой маршрутизации в голосовых приложениях. Маршрутизаторы быстро обрабатывают небольшие пакеты и рассматривают обычно все передаваемые по одному и тому же IP-адресу пакеты одного размера одинаковым образом. В результате пакеты проходят по одному маршруту, поэтому их не надо переупорядочивать.

5. Прием и переупорядочивание пакетов в адаптивном «буфере ресинхронизации» для обеспечения интеллектуальной обработки потерь или задержек пакетов. Главной целью здесь является преодоление влияния переменной задержки между пакетами. Решение этой проблемы состоит в буферизации достаточного числа поступающих пакетов (при отложенном их воспроизведении) с тем, чтобы воспроизведение было непрерывным, даже если время между поступлением пакетов сильно разнится. Лучшие продукты для IP-телефонии моделируют производительность сети и регулируют размер буфера ресинхронизации соответствующим образом – уменьшая его (сокращая задержку перед воспроизведением), когда сеть ведет себя предсказуемым образом, и увеличивая в противоположной ситуации.

5.4. Методы кодирования речевой информации

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

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

1. Кодеки с импульсно-кодовой модуляцией (ИКМ) и адаптивной дифференциальной импульсно-кодовой модуляцией (АДИКМ), появившиеся в конце 50-х годов и использующиеся сегодня в системах традиционной телефонии. В большинстве случаев, представляют собой сочетание АЦП/ЦАП.
2. Кодеки с вокодерным преобразованием речевого сигнала возникли в системах мобильной связи для снижения требований к пропускной способности радиотракта. Эта группа кодеков использует гармонический синтез сигнала на основании информации о его вокальных составляющих – фонемах. В большинстве случаев, такие кодеки реализованы как аналоговые устройства.
3. Комбинированные (гибридные) кодеки сочетают в себе технологию вокодерного преобразования/синтеза речи, но оперируют уже с цифровым сигналом посредством специализированных DSP. Кодеки этого типа содержат в себе ИКМ или АДИКМ кодек и реализованный цифровым способом вокодер.

На рис. 5.6 представлена усредненная субъективная оценка качества кодирования речи для вышеперечисленных типов кодеков.

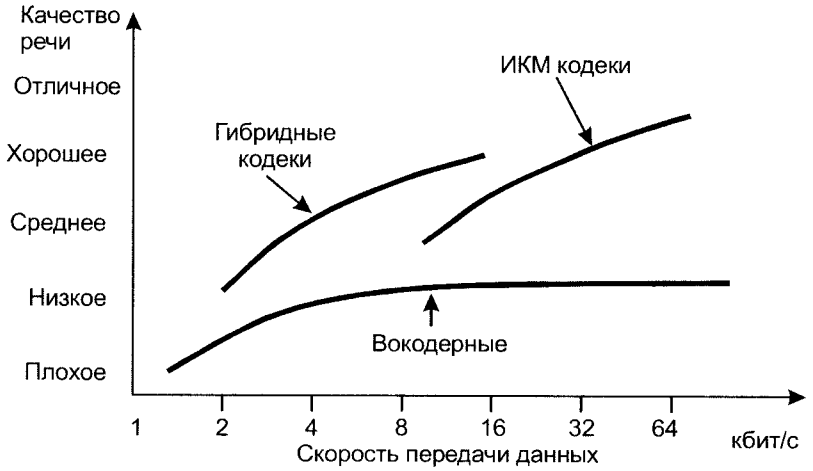


Рис. 5.6. Усредненная субъективная оценка качества кодирования речи для различных типов кодеков

В голосовых шлюзах IP-телефонии понятие кодека подразумевает не только алгоритмы кодирования/декодирования, но и их аппаратную реализацию. Большинство кодеков, используемых в IP-телефонии, описаны рекомендациями семейства «G» стандарта H.323 (рис. 5.7).

Рис. 5.7. Стандарты для кодирования речевых сигналов

Все методы кодирования, основанные на определенных предположениях о форме сигнала, не подходят при передаче сигнала с резкими скачками амплитуды. Именно такой вид имеет сигнал, генерируемый модемами или факсимильными аппаратами, поэтому аппаратура, поддерживающая сжатие, должна автоматически распознавать сигналы факс-аппаратов и модемов и обрабатывать их иначе, чем голосовой трафик. Многие методы кодирования берут свое начало от метода кодирования с линейным предсказанием LPC (Linear Predicative Coding). В качестве входного сигнала в LPC используется последовательность цифровых значений амплитуды, но алгоритм кодирования применяется не к отдельным цифровым значениям, а к определенным их блокам. Для каждого такого блока значений вычисляются его характерные параметры: частота, амплитуда и ряд других. Именно эти значения и передаются по сети. При таком подходе к кодированию речи, во-первых, возрастают требования к вычислительным мощностям специализированных процессоров, используемых для обработки сигнала, а во-вторых, увеличивается задержка при передаче, поскольку кодирование применяется не к отдельным значениям, а к некоторому их набору, который перед началом преобразования следует накопить в определенном буфере.

Важно, что задержка в передаче речи связана не только с необходимостью обработки цифрового сигнала (эту задержку можно уменьшать, увеличивая мощность процессора), но и непосредственно с характером метода сжатия. Метод кодирования с линейным предсказанием LPC позволяет достигать очень больших степеней сжатия, которым соответствует полоса пропускания 2,4 или 4,8 кбит/с, однако качество звука здесь сильно страдает. Поэтому в коммерческих приложениях он не используется, а применяется в основном для ведения служебных переговоров. Более сложные методы сжатия речи основаны на применении LPC в сочетании с элементами кодирования формы сигнала. В этих алгоритмах используется кодирование с обратной связью, когда при передаче сигнала осуществляется оптимизация кода. Закодировав сигнал, процессор пытается восстановить его форму и сличает результат с исходным сигналом, после чего начинает варьировать параметры кодировки, добиваясь наилучшего совпадения. Достигнув такого совпадения, аппаратура передает полученный код по линиям связи; на противоположном конце происходит восстановление звукового сигнала. Ясно, что для использования такого метода требуются еще более серьезные вычислительные мощности.

Одной из самых распространенных разновидностей описанного метода кодирования является метод LD-CELP (Low-Delay Code-Excited Linear Prediction). Он позволяет достичь удовлетворительного качества воспроизведения при пропускной способности 16 кбит/с. Алгоритм применяется к последовательности цифр, получаемых в результате аналого-цифрового преобразования голосового сигнала с 16-разрядным разрешением. Пять последовательных цифровых значений кодируются одним 10-битовым блоком – это и дает те самые 16 кбит/с. Для применения этого метода требуются большие вычислительные мощности; в частности, в марте 1995 г. ITU принял новый стандарт – G.723, который предполагается использовать при сжатии речи для организации видеоконференций по телефонным сетям. Этот стандарт представляет собой часть более общего стандарта H.324, описывающего подход к организации таких видеоконференций. Цель – организация видеоконференций с использованием обычных модемов. Основой G.723 является метод сжатия речи MP-MLQ (Multipulse Maximum Likelihood Quantization). Он позволяет добиться весьма существенного сжатия речи при сохранении достаточно высокого качества звучания. В основе метода лежит описанная выше процедура оптимизации; с помощью различных усовершенствований можно сжимать речь до уровня 4,8; 6,4; 7,2 и 8,0 кбит/с. Структура алгоритма позволяет на основе программного обеспечения изменять степень сжатия голоса в ходе передачи. Вносимая кодированием задержка не превышает 20 мс. Повышая эффективность использования полосы пропускания,

механизмы сжатия речи в то же время могут привести к ухудшению ее качества и увеличению задержек.

Далее рассмотрены некоторые основные кодеки, используемые в шлюзах IP-телефонии операторского уровня.

Кодек G.711

Рекомендация G.711, утвержденная МККТТ в 1984 г., описывает кодек, использующий ИКМ преобразование аналогового сигнала с точностью 8 бит, тактовой частотой 8 кГц и простейшей компрессией амплитуды сигнала. Скорость потока данных на выходе преобразователя составляет 64 кбит/с (8 бит×8 кГц). Для снижения шума квантования и улучшения преобразования сигналов с небольшой амплитудой при кодировании используется нелинейное квантование по уровню (рис. 5.8) согласно специальному псевдо-логарифмическому закону: А-закон для европейской системы ИКМ-30/32 или μ- закон для североамериканской системы ИКМ-24.

Первые ИКМ кодеки с нелинейным квантованием появились уже в 60-х годах. Кодек G.711 широко распространен в системах традиционной телефонии с коммутацией каналов. Несмотря на то, что рекомендация G.711 в стандарте H.323 является основной и первичной, в шлюзах IP-телефонии данный кодек применяется редко из-за высоких требований к полосе пропускания и задержкам в канале передачи (все-таки 64 кбит/с это много). Использование G.711 в системах IP-телефонии обосновано лишь в тех случаях, когда требуется обеспечить максимальное качество кодирования речевой информации при небольшом числе одновременных разговоров. Одним из примеров применения кодека G.711 могут послужить IP-телефоны компании Cisco.

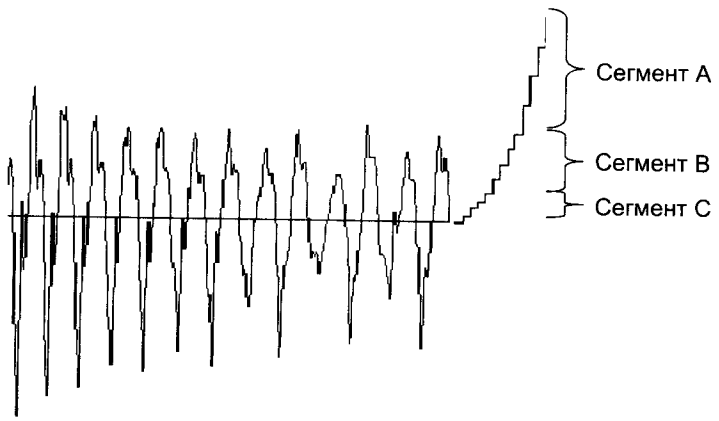


Рис. 5.8. Нелинейное квантование по уровню

Кодек G.726

Один из старейших алгоритмов сжатия речи ADPCM – адаптивная дифференциальная ИКМ (стандарт G.726 был принят в 1984 г.). Этот алгоритм дает практически такое же качество воспроизведения речи, как и ИКМ, однако для передачи информации при его использовании требуется полоса всего в 16-32 кбит/с. Метод основан на том, что в аналоговом сигна-

ле, передающем речь, невозможны резкие скачки интенсивности. Поэтому, если кодировать не саму амплитуду сигнала, а ее изменение по сравнению с предыдущим значением, то можно обойтись меньшим числом разрядов. В ADPCM изменение уровня сигнала кодируется четырехразрядным числом, при этом частота измерения амплитуды сигнала сохраняется неизменной. Процесс преобразования не вносит существенной задержки и требует от DSP 5,5-6,4 MIPS (Million Instructions Per Second). Кодек может применяться совместно с кодеком G.711 для снижения скорости кодирования последнего. Кодек предназначен для использования в системах видеоконференций.

Кодек G.723.1

Рекомендация G.723.1 описывает гибридные кодеки, использующие технологию кодирования речевой информации, сокращенно называемую – MP-MLQ (Multy-Pulse – Multy Level Quantization – множественная импульсная, многоуровневая квантизация), данные кодеки можно охарактеризовать, как комбинацию АЦП/ЦАП и вокодера. Своим возникновением гибридные кодеки обязаны системам мобильной связи. Применение вокодера позволяет снизить скорость передачи данных в канале, что принципиально важно для эффективного использования радиотракта и IP-канала. Основной принцип работы вокодера – синтез исходного речевого сигнала посредством адаптивной замены его гармонических составляющих соответствующим набором частотных фонем и согласованными шумовыми коэффициентами. Кодек G.723 осуществляет преобразование аналогового сигнала в поток данных со скоростью 64 кбит/с (ИКМ), а затем при помощи многополосного цифрового фильтра/вокодера выделяет частотные фонемы, анализирует их и передает по IP-каналу информацию только о текущем состоянии фонем в речевом сигнале. Данный алгоритм преобразования позволяет снизить скорость кодированной информации до 5,3-6,3 кбит/с без видимого ухудшения качества речи. Кодек имеет две скорости и два варианта кодирования: 6,3 кбит/с с алгоритмом MP-MLQ и 5,3 кбит/с с алгоритмом CELP. Первый вариант предназначен для сетей с пакетной передачей голоса и обеспечивает лучшее качество кодирования по сравнению с вариантом CELP, но менее адаптирован к использованию в сетях со смешанным типом трафика (голос/данные).

Процесс преобразования требует от DSP 16,4-16,7 MIPS и вносит задержку 37 мс. Кодек G.723.1 широко применяется в голосовых шлюзах и прочих устройствах IP-телефонии. Кодек уступает по качеству кодирования речи кодеку G.729a, но менее требователен к ресурсам процессора и пропускной способности канала.

Кодеки G.729

Семейство включает кодеки G.729, G.729 Annex A, G.729 Annex B (содержит VAD и генератор комфортного шума). Кодеки G.729 сокращенно называют CS-ACELP Conjugate Structure – Algebraic Code Excited Linear Prediction – сопряженная структура с управляемым алгебраическим кодом линейным предсказанием. Процесс преобразования использует DSP 21,5 MIPS и вносит задержку 15 мс. Скорость кодированного речевого сигнала составляет 8 кбит/с. В устройствах VoIP данный кодек занимает лидирующее положение, обеспечивая наилучшее качество кодирования речевой информации при достаточно высокой компрессии.

Кодек G.728

Гибридный кодек, описанный в рекомендации G.728 в 1992 г. относится к категории LD-CELP – Low Delay – Code Excited Linear Prediction – кодек с управляемым кодом линей-

ным предсказанием и малой задержкой. Кодек обеспечивает скорость преобразования 16 кбит/с, вносит задержку при кодировании от 3 до 5 мс и для реализации необходим процессор с быстродействием более 40 MIPS. Кодек предназначен для использования, в основном, в системах видеоконференций. В устройствах IP-телефонии данный кодек применяется достаточно редко.

Основные характеристики рассмотренных кодеков приведены в табл. 5.1.

Таблица 5.1. Характеристики кодеков

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

Количественными характеристиками ухудшения качества речи являются единицы QDU (Quantization Distortion Units): 1 QDU соответствует ухудшению качества при оцифровке с использованием стандартной процедуры ИКМ; значения QDU для основных методов компрессии приведены в табл. 5.2.

Таблица 5.2. Единицы ухудшения качества речи QDU для различных методов компрессии

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

Дополнительная обработка речи всегда ведет к дальнейшей потере качества. Согласно рекомендациям МСЭ-Т, для международных вызовов величина QDU не должна превышать 14, причем передача разговора по международным магистральным каналам ухудшает качество речи, как правило, на 4 QDU. Следовательно, при передаче разговора по национальным сетям должно теряться не более 5 QDU. Поэтому для качественной передачи речи процедуру компрессии/декомпрессии желательно применять в сети только один раз. В некоторых странах это является обязательным требованием регулирующих органов по отношению к корпоративным сетям, подключенным к сетям общего пользования. Подавление пауз (silence suppression) – важная функция АТМ-коммутаторов. Суть технологии подавления пауз заклю-

чается в определении различия между моментами активной речи и молчания в период соединения. В результате применения этой технологии генерация ячеек происходит только в моменты активного разговора. Поскольку в процессе типичного разговора по телефону тишина составляет до 60% времени, происходит двукратная оптимизация по количеству данных, которые должны быть переданы по линии. Объединение технологии сжатия речи и подавления пауз речи в коммутаторах приводит к уменьшению потока данных в канале до восьми раз.

Современные продукты для IP-телефонии применяют самые разные кодеки, стандартные и нестандартные. Конкурентами являются кодеки GSM (13,5 кбит/с) и кодеки МСЭ-Т серии G, использование которых предусматривается стандартом H.323 для связи по IP-сети. Единственным обязательным для применения кодеком в H.323-совместимых продуктах остается стандарт G.711: выдаваемые им массивы данных составляют от 56 до 64 кбит/с. В качестве дополнительных высокопроизводительных кодеков стандарт H.323 рекомендует G.723 и G.729 – последние способны сжимать оцифрованную 16-разрядную ИКМ-речь длительностью 10 мс всего в 10 байт. Стандарт G.729 уже получил широкое распространение в системах передачи голоса по IP; его поддерживают значительное число производителей продуктов для IP-телефонии.

5.5. Комплексная оценка качества IP-телефонии

Искажения от компрессии/декомпрессии оценивают путем опроса разных групп людей по пятибалльной шкале единицами субъективной оценки MOS (Mean Opinion Score). Оценки 3,5 баллов и выше соответствуют стандартному и высокому телефонному качеству, 3,0...3,5 – приемлемому, 2,5...3,0 – синтезированному звуку. Для передачи речи с хорошим качеством целесообразно ориентироваться на MOS не ниже 3,5 баллов. Значения MOS для различных стандартов кодеров приведены в табл. 5.3.

Таблица 5.3. Средние субъективные оценки качества различных методов кодирования

Кодек	Скорость передачи, кбит/с	MOS	Размер кадра, мс
G.711 PCM	64	4,3	0,125
G.726 Multi-rate ADPCM	16-40	2-4,3	0,125
G.723 MP-MLQ ACELP	5,3; 6,3	3,7; 3,8	30
G.728 LD-CEL	16	4,1	0,625
G.729 CS-ACELP	8	4,0	10
G.729a CS-ACELP	8	3,4	10
GSM RPE-LPC	13	3,9	30

Несмотря на большое разнообразие, характеризуемое пропускными способностями, числом маршрутизаторов, характеристиками физических линий и прочими характеристиками, реально действующие каналы Интернет характеризуются следующими параметрами:

- действительной пропускной способностью, определяемой наиболее «узким местом» в виртуальном канале в данный момент времени;
- трафиком, также являющимся функцией времени;

- задержкой пакетов, что определяется трафиком, числом маршрутизаторов, реальными физическими свойствами каналов передачи, образующими в данный момент времени виртуальный канал, задержками на обработку сигналов, возникающими в речевых кодеках и других устройствах шлюзов; все это также обеспечивает зависимость задержки от времени;
- потерей пакетов, обусловленной наличием «узких мест», очередями;
- перестановкой пакетов, пришедших разными путями.

Для провайдеров Интернет-телефонии очень привлекательна возможность предоставления услуг с разным уровнем качества (и соответствующими тарифами). Необходимым условием этого является поддержание определенного уровня качества предоставления услуг, причем не только в пределах одного оператора, но и между сетями разных операторов. Для этого в рамках проекта TIPHON определены четыре класса обслуживания (табл. 5.4), каждый из которых гарантирует определенное качество при установлении вызова и во время самого сеанса связи.

Качество обслуживания при установлении вызова характеризуется прежде всего временем его установления, т.е. временем между набором абонентом последней цифры номера (или, например, команды ввода при наборе адреса на компьютере) и получением им ответного тонального сигнала. Качество обслуживания во время сеанса связи определяется многими факторами, два основных – это сквозная временная задержка и качество сквозной передачи речи (оценивается параметрами субъективной оценки MOS).

Таблица 5.4. Характеристики классов обслуживания TIPHON

Характеристика	Классы обслуживания			
	Наилучший (4)	**Высокий (3)**	**Средний (2)**	**Низкий (1)**
Качество передачи речи[1]	Лучше, чем G.711	Не хуже, чем G.726 (32 кбит/с)	Не хуже, чем GSM-FR	Не определено
Сквозная задержка, мс	<150	<250	<350	<450
Время установления вызова, с:				
при прямой IP-адресации	<1,5	<4	<7	<7
при трансляции номера E.164 в IP-адрес[2]	<2	<5	<10	<10
при трансляции номера E.164 в IP-адрес через клиринговый центр или роуминг[2]	<3	<8	<15	<15
при трансляции номера E.164 в IP-адрес[3]	<4	<10	<20	<20
при трансляции номера E.164 в IP-адрес через клиринговый центр или роуминг[3]	<6	<15	<30	<30
при трансляции адреса электронной почты в IP-адрес	<4	<13	<25	<25

[1]В одном направлении, без интерактивных измерений
[2]Пользователь IP-сети вызывает абонента ТфОП
[3]Абонент ТфОП вызывает пользователя IP-сети

5.6. Обеспечение качества IP-телефонии на базе протокола RSVP

Одним из средств обеспечения качества IP-телефонии и особенно Интернет-телефонии является использование протокола резервирования ресурсов (Resource Reservation Protocol, RSVP), рекомендованного комитетом IETF. 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 и UDP – чтобы обеспечить качественную передачу видео- и аудиосигналов. Протокол RSVP предусматривает гарантированное QoS благодаря тому, что через каждый компьютер, или узел, который связывает между собой участников телефонного разговора, может передаваться определенное количество данных.

Протокол RSVP предназначен только для резервирования части пропускной способности. Используя RSVP, отправитель периодически информирует получателя о свободном количестве ресурсов сообщением RSVP Path (рис. 5.9). Транзитные маршрутизаторы по мере прохождения этого сообщения также анализируют имеющееся у них количество свободных ресурсов и подтверждают его соответствующим сообщением RSVP Resv, передаваемым в обратном направлении. Если ресурсов достаточно, то отправитель начинает передачу. Если ресурсов не достаточно, получатель должен снизить требования или прекратить передачу информации.

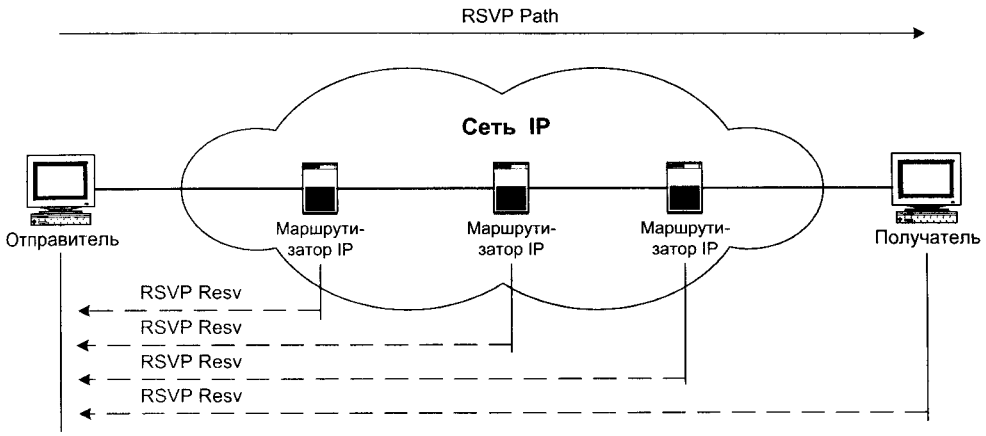


Рис. 5.9. Применение протокола RSVP

Одна из интересных особенностей RSVP заключается в том, что запросы на резервирование ресурсов направляются только от получателей данных отправителям, а не наоборот. Такой подход обусловлен тем, что лишь устройство-получатель знает, с какой скоростью оно должно получать данные, чтобы надежно декодировать аудио- или видеосигналы. Другая уникальная особенность RSVP состоит в том, что резервирование производится лишь для одного направления. Кроме того, RSVP не допускает смешения аудио- и видеосигналов на зарезервированном канале.

Когда RSVP-программы закончат сеанс связи, они должны вызвать функцию отмены, предусмотренную этим протоколом. Отмена аннулирует все запросы на ресурсы, сделанные

программой, и позволяет другим прикладным программам использовать коммуникационные возможности Internet. Если программе не удается выполнить отмену, то предусмотренные протоколом средства по истечении некоторого промежутка времени обнаружат это и автоматически отменят запрос на ресурсы.

Недостатком протокола RSVP является то, что полоса пропускания, выделяемая источнику информации, при снижении активности источника не может быть использована для передачи другой информации. Поскольку для реализации QoS протокол RSVP требует резервирования ресурсов или каналов связи, небрежные или безответственные пользователи могут захватить ресурсы сети, инициируя несколько сеансов QoS подряд. Как только канал зарезервирован, он становится недоступным для других пользователей, даже если тот, кто его затребовал, ничего не передает. К сожалению, в RSVP отсутствует четкий механизм предотвращения подобных ситуаций, и решение этой проблемы возлагается на сетевых администраторов. Очевидно, что необходимо предусмотреть более жесткий контроль, чтобы RSVP имел успех.

Как альтернатива этому способу может использоваться алгоритм управления потоками на основе системы приоритетов, однако в существующей версии IP этот механизм развит недостаточно. Механизм управления приоритетами должен быть реализован в следующей шестой версии IP, где предусматривается введение до 16 приоритетов, а также возможность организации нескольких логических потоков в рамках одного физического соединения. Однако в настоящее время аппаратура, реализующая IP версии 6, только начала появляться на рынке.

Ввиду зависимости RSVP от совместимости промежуточных узлов – в большинстве случаев маршрутизаторов – это влечет за собой неизбежные проблемы, в частности, в глобальных сетях. Если какой-либо маршрутизатор достиг предела своих возможностей, когда он не может гарантировать запрошенный уровень QoS, все последующие запросы будут игнорироваться и удаляться. При отказе только одного узла обслуживать запрос вся стройная система RSVP распадается на части.

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

5.7. Обеспечение качества IP-телефонии на базе протоколов RTP и RTCP

Для уменьшение значений джиттера и задержек на сетевом уровне применяются гарантирующие пользователю заданный уровень качества механизмы RSVP, MPLS, Diff-Serv, ATM и др. Они улучшают качество услуг, предоставляемых сетью, но не могут полностью устранить образование очередей в сетевых устройствах, а, следовательно, и совсем убрать джиттер. Компенсировать его негативное влияние позволяет разработанный IETF протокол прикладного уровня RTP (Real-time Transport Protocol), который используется технологиями H.323 и SIP.

Протокол RTP (RFC1889) предназначен для доставки чувствительной к задержкам информации с использованием сетевых служб одноадресной или групповой рассылки. Он не имеет собственных механизмов, гарантирующих своевременную доставку пакетов или другие параметры качества услуг – это осуществляют нижележащие протоколы. Он даже не

обеспечивает все те функции, которые обычно предоставляют транспортные протоколы, в частности, функции по исправлению ошибок или управлению потоком. Обычно RTP работает поверх UDP и использует его службы, но может функционировать и поверх других транспортных протоколов (рис. 5.10).

Служба RTP предусматривает указание типа полезной нагрузки и последовательного номера пакета в потоке, а также применение временных меток. Отправитель помечает каждый RTP-пакет временной меткой, а получатель извлекает ее и вычисляет суммарную задержку. Разница в задержке пакетов позволяет определить джиттер и смягчить его влияние – все пакеты будут выдаваться приложению с одинаковой задержкой.

Таким образом, главная особенность RTP – это вычисление средней задержки некоторого набора принятых пакетов и выдача их пользовательскому приложению с постоянной задержкой, равной этому среднему значению. Однако следует иметь ввиду, что временная метка RTP соответствует моменту кодирования первого дискретного сигнала пакета. Поэтому, если RTP-пакет, например, с видеоинформацией, разбивается на несколько пакетов нижележащего уровня, то временная метка уже не будет соответствовать истинному времени их передачи, поскольку они перед передачей могут быть организованы в очередь.

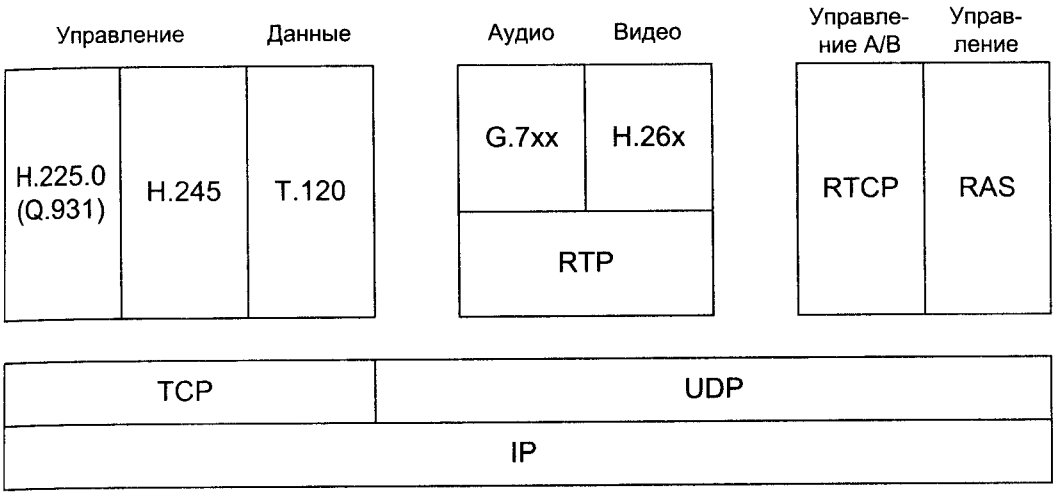


Рис. 5.10. Стек протоколов H.323

Еще одно преимущество RTP состоит в том, что его можно использовать с RSVP для передачи синхронизированной мультимедиаинформации с определенным уровнем качества обслуживания. Кроме того, разговоры передаются по сети Internet в незашифрованном виде. Поэтому любой узел, находящийся на пути следования данных, может подключиться к этой линии и прослушать ваш разговор. Чтобы решить эту проблему, в RTP предлагается механизм, до некоторой степени обеспечивающий защиту от несанкционированного доступа и конфиденциальность. Эти средства довольно ненадежны и могут рассматриваться лишь как временное решение проблемы – пока протоколы, поверх которых работает RTP, не будут располагать развитыми механизмами безопасности данных.

Возможности RTP можно расширить, объединив его с еще одним протоколом IETF, а именно с протоколом управления передачей в реальном времени (Real-time Transport Control Protocol, RTCP). С помощью RTCP контролируется доставка RTP-пакетов и обеспечивается

обратная связь с передающей стороной и другими участниками сеанса. RTCP периодически рассылает свои управляющие пакеты, используя тот же механизм распределения, какой применяется и для RTP-пакетов с пользовательской информацией.

Основной функцией RTCP является организация обратной связи с приложением для отчета в качестве получаемой информации. RTCP передает сведения (как от приемника, так и от отправителя) о числе переданных и потерянных пакетов, значении джиттера, задержке и т.д. Эта информация может быть использована отправителем для изменения параметров передачи, например, для уменьшения коэффициента сжатия информации с целью улучшения качества ее передачи. RTCP также предусматривает идентификацию пользователей-участников сеанса.

При всех своих достоинствах протокол RTP далеко не совершенен. Например, протокол никак не способен повлиять на задержку в сети, но он помогает сократить дрожание звука при воспроизведении при наличии задержек. Кроме того, хотя пакеты UDP получают порядковые номера, при этом принимающая станция может установить факт потери пакетов, RTP не предпринимает никаких мер для восстановления потерянных пакетов.

Один из способов расширения возможностей RTP состоит в использовании его совместно с протоколом RSVP, который официально не входит в комплект протоколов H.323, но поддерживается многими приложениями реального времени.

5.8. Обеспечение качества IP-телефонии на базе протокола IPv6

После нескольких лет тестирования организация Internet Assigned Numbers Authority приступила к развертыванию IPv6 (версии 6 протокола Internet Protocol) – системы цифровой адресации Internet нового поколения.

Начать разработку IPv6 организацию Internet Engineering Task Force побудили опасения, что Internet израсходует весь запас уникальных адресов. Первоначально сеть Internet была рассчитана на связь небольшого количества исследовательских сетей. Поэтому поле адреса в используемой в настоящее время системе адресации IPv4 может принимать около 4 млрд. уникальных значений. Число уникальных адресов, обеспечиваемых новой системой – десять в восемнадцатой степени, или миллиард миллиардов. Этого должно хватить на много лет вперед.

Переход на IPv6 начат с трех крупнейших региональных регистрационных каталогов, которые приступают к выдаче новым пользователям удлиненных адресов; полный перевод на новую систему всей сети может быть завершен, как ожидается, в течение 6-10 лет.

IPv6 включает следующие возможности, отсутствующие у IPv4:

- *расширенное адресное пространство*: IPv6 использует 128-битовые адреса вместо 32-битовых IPv4. В результате адресное пространство увеличивается в 2^{96} раз, что явно достаточно даже в случае неэффективного распределения сетевых адресов;
- *улучшенные возможности маршрутизации*: в связи с увеличением межсетевого трафика, связанного с обработкой больших объемов мультимедийной информации и расширением использования сети Интернет в различных сферах деятельности, весьма существенной является необходимость обеспечения высоких скоростей маршрутизации. Без применения эффективных алгоритмов обработки пакетов данных становится невозможным повысить скорости работы маршрутизаторов до уровня, сравнимого со скоростями передачи информации по каналам связи;

- *управление доставкой информации*: IPv6 позволяет отмечать соответствие конкретного пакета определенным условиям его передачи, заданным отправителем. В результате достигается регулирование скорости передачи определенных потоков данных, что позволяет обеспечивать эффективную поддержку специальных протоколов (например, видео в режиме реального времени и др.). За счет назначения приоритетов передачи данных по определенным протоколам, появляется возможность гарантировать первоочередность обработки наиболее критической информации и предоставления важным данным всей полосы пропускания канала связи. Другие особенности, имеющиеся у IPv6, позволяют протоколам этого семейства обеспечивать одновременную многоадресную доставку информации. Данная возможность находит свое применение в рассылке информации "по подписке" или "по требованию", а также в других приложениях;
- *средства обеспечения безопасности*: IPv6 предоставляет возможности защиты от атак, связанных с подменой исходных адресов пакетов, и от несанкционированного доступа к полям данных пакетов. Эти возможности достигаются за счет применения алгоритмов аутентификации и шифрования.

Не вызывает сомнений тот факт, что переход от IPv4 к IPv6 не может быть мгновенным. Долгое время две версии IP будут сосуществовать. Более того, поначалу узлы, реализующие IPv6, не будут предоставлять всех необходимых сервисов, а их расположение окажется напоминающим острова в океане IPv4. Следовательно, от узлов с IPv6 требуется выполнение двух свойств:

- возможность взаимодействовать с IPv4-узлами;
- возможность передавать пакеты IPv6 через существующую инфраструктуру IPv4.

Чтобы выполнить эти требования, рабочая группа по переходу на IP нового поколения предлагает два основных метода:

- одновременная поддержка в узлах (и в хостах, и в маршрутизаторах) IPv6 двух стеков протоколов (IPv6/IPv4);
- туннелирования пакетов IPv6 для их передачи через инфраструктуру IPv4.

5.9. Обеспечение качества IP-телефонии на базе дифференцированного обслуживания

Еще одна технология обеспечения QoS разработана рабочей группой IETF по дифференцированному обслуживанию (Differentiated Services, DiffServ). Эта группа выделилась из рабочей группы по интегрированному обслуживанию (Integrated Services, IntServ), задача которой состоит в разработке стандартов для поддержки трафика Internet реального времени.

Проводимая в рамках IntServ работа отражает некоторые из особенностей концепции RSVP. Интегрированное обслуживание предполагает сигнализацию из конца в конец и в действительности использует RSVP между отправителями и получателями.

IntServ определяет три класса обслуживания для IP-сетей:

- по мере возможности – то, что сейчас предлагает Internet;
- с контролируемой загруженностью – приложение получает тот уровень обслуживания, какой оно имело бы в слабо загруженной сети;
- гарантированным обслуживанием – необходимая пропускная способность в течение всего сеанса предоставляется с гарантией на параметры качества обслуживания.

Как и RSVP, интегрированное обслуживание имеет проблемы с масштабированием, поэтому данная технология вряд ли пробьется за пределы корпоративных сетей. И, как было отмечено, RSVP предполагает весьма значительные накладные расходы, так как каждый узел вдоль пути следования пакетов должен согласиться предоставить запрошенное качество услуг.

Дифференцированное обслуживание предлагает более простой и масштабируемый метод QoS для приложений реального времени. Одним из ключевых моментов в работе над DiffServ является переопределение 8-битного поля «Тип сервиса» в заголовке IPv4. Названное «Дифференцированным обслуживанием» (DS), это поле может содержать информацию, на основании которой узлы вдоль маршрута определяют, как им следует обрабатывать пакеты и передавать их следующему маршрутизатору.

В настоящее время только 6 из 8 бит в поле DS были определены, и только одно назначение было стандартизовано. Это назначение известно как принятое по умолчанию - Default (DE), – и оно определяет класс обслуживания по мере возможности. Другое предполагаемое назначение, срочная отправка (Expedited Forwarding, EF), должно обеспечить сокращение задержек и потерь пакетов.

При поступлении трафика в сеть краевой маршрутизатор классифицирует трафик в соответствии с информацией, содержащейся в поле DS. Он передает следующим за ним маршрутизаторам эту информацию, на основании которой они узнают, каким образом обрабатывать данный конкретный поток.

DiffServ, кроме того, сокращает служебный трафик по сравнению с RSVP и IntServ, опирающимися на сигнализацию из конца в конец. DiffServ классифицирует потоки в соответствии с предопределенными правилами и затем объединяет однотипные потоки. Подобный механизм делает DiffServ гораздо более масштабируемым, чем его предшественника IntServ. Весь трафик с одинаковыми метками рассматривается одинаковым образом, поэтому реализация DiffServ в сети крупного предприятия или по каналам глобальной сети оказывается более реальной задачей.

Как можно догадаться, преимущества DiffServ нельзя получить автоматически. Маршрутизаторы должны понимать «меченые потоки» и уметь соответствующим образом реагировать на них. Это потребует модернизации микропрограммного обеспечения маршрутизаторов. К счастью, с популяризацией DiffServ все большее число производителей намеревается поддерживать данную архитектуру в будущих версиях своих продуктов.

5.10. Обеспечение качества IP-телефонии на базе MPLS

Конкурентом DiffServ на роль протокола для обеспечения QoS является другой проект IETF под названием «Многопротокольная коммутация меток» (Multiprotocol Label Switching, MPLS).

При IP-коммутации узел анализирует первые несколько пакетов поступающего трафика и, в случае короткой посылки, например запроса DNS или SNMP, обрабатывает их как обычный маршрутизатор. Но если узел идентифицирует длительный поток – от трафика telnet или ftp до загрузки файлов через Web и мультимедийных приложений, то IP-коммутатор переключается на нижележащую структуру ATM и применяет сквозную коммутацию для быстрой доставки данных адресату.

IP-коммутация поддерживает различные уровни QoS и может использовать ATM, имеющий многочисленные встроенные средства поддержки QoS, и RSVP.

Конкуренцию IP-коммутации составила тег-коммутация. Как видно из названия, данная технология предполагает присоединение к пакетам меток для информирования коммутаторов и маршрутизаторов о природе трафика. Не углубляясь в анализ пакета, устройства просто считывают метку в заголовке для определения соответствующего маршрута потоку трафика.

Если DiffServ задействует заголовок DS, уже имеющийся в пакетах IPv4, то MPLS использует 32-разрядную информационную метку, добавляемую к каждому IP-пакету. Эта метка, добавляемая при входе в сеть с поддержкой MPLS, сообщает каждому маршрутизатору вдоль пути следования, как надо обрабатывать пакет. В частности, она содержит информацию о требуемом для данного пакета уровне QoS.

В отличие от поля DS, метка MPLS изначально не является частью пакета IP. Скорее, она добавляется при поступлении пакета в сеть и удаляется при выходе пакета из сети MPLS.

В обычной ситуации маршрутизаторы анализируют заголовок пакета для определения его адресата. Ввиду того, что такой анализ проводится на каждом транзитном узле независимо, предсказать, каким маршрутом будет следовать пакет, практически невозможно, поэтому обеспечение гарантированного уровня QoS оказывается невероятно сложной задачей.

При использовании меток MPLS маршрутизатор или коммутатор может присвоить метки записям из своих таблиц маршрутизации и в виде меток передать информацию о маршрутизации конкретным маршрутизаторам и коммутаторам. Считав метку, каждый коммутатор или маршрутизатор узнает информацию о следующем адресате на пути, не анализируя заголовок пакета. Это экономит время и ресурсы ЦПУ. Пакеты с метками MPLS могут, следовательно, передаваться от отправителя к получателю без задержек на обработку, причем все промежуточные узлы знают, как нужно обрабатывать каждый пакет.

По сути, MPLS привносит коммутацию каналов, какую мы имеем в ATM, в мир пакетных сетей, связанных с IP. На практике MPLS можно использовать для доставки IP-трафика по сетям IP.

Следует отметить, что DiffServ функционирует на третьем уровне, а MPLS – на втором, поэтому с технической точки зрения обе технологии могут мирно существовать друг с другом. Как уже упоминалось, DiffServ классифицирует пакеты при их поступлении на краевой маршрутизатор, поэтому данный стандарт, скорее всего, будет использоваться на границе сети, например, между компанией и ее сервис-провайдером.

А ввиду того, что MPLS предполагает включение дополнительных меток и использование маршрутизаторов/коммутаторов, способных интерпретировать данную информацию, он, вероятно, найдет применение исключительно внутри корпоративных сетей или базовой сети оператора, где требуется высокий уровень QoS для IP-трафика.

Если DiffServ требует некоторой настройки сетевых маршрутизаторов, то MPLS предполагает более серьезную модернизацию, чтобы маршрутизаторы могли читать метки и направлять пакеты по конкретным маршрутам.

В настоящее время DiffServ пользуется более широким вниманием, и он ближе к окончательной стандартизации, чем MPLS. Однако каждая из технологий имеет свои преимущества в конкретных областях сети, поэтому поставщики, скорее всего, будут поддерживать их обе.

5.11. Спецификация IEEE 802.1p

Рабочая группа IEEE 802.1 по высокоуровневым протоколам для локальных сетей разработала спецификацию 802.1p для приоритезации трафика в соответствии с восемью классами – от обработки по мере возможности до поддержки передачи голоса и видео в реальном

времени. Промежуточные уровни между ними занимают классы для потокового мультимедиа типа неинтерактивных видеоклипов и для важного трафика типа запросов к базам данных.

802.1p анализирует поля приоритета в заголовке пакета. Ей в помощь IEEE предложил спецификацию 802.1Q, предусматривающую 32-разрядный заголовок пакета, предшествующий адресам отправителя и получателя в кадре Ethernet. Этот 32-разрядный заголовок может быть определен маршрутизаторами, коммутаторами и даже станциями конечных пользователей. Он содержит информацию о группах виртуальных локальных сетей и сигнализации 802.1p.

На основании этого заголовка маршрутизаторы и коммутаторы (на втором и на третьем уровнях) могут принимать решения о приоритете трафика с учетом предопределенных правил, заданных администратором сети.

Стандарт 802.1p призван обеспечить QoS при коммутации в локальных сетях, поэтому он может быть не столь привлекательным, как рассмотренные выше технологии для глобальных сетей Интернет-телефонии.

5.12. Обеспечение качества IP-телефонии с помощью механизма управления на основе правил

Одним из перспективных направлений в реализации гарантированных уровней качества сервиса (QoS) в среде IP является разрабатываемая в настоящее время технология управления на основе правил.

Набор правил, или стратегия, описывает способ распределения ресурсов сети между ее клиентами – пользователями, приложениями или хост-машинами. Выделение этих ресурсов может происходить статически и динамически, в зависимости от разных факторов, например, времени дня, объема самих свободных ресурсов или наличия у клиентов подтвержденных авторизацией привилегий.

Высокоуровневые формулировки стратегии (например, «Предоставлять приоритет всем пакетам трафика voice-over-IP») преобразуются в структурированный набор правил вида «если <условие>, то <реакция>», который хранится в базе администратора, извлекается и интерпретируется различными сетевыми компонентами. Заметим, что системы первого поколения не могли сами интерпретировать высокоуровневые формулировки, а требовали от администратора формализованных условных операторов вида «если порт = HTTP (80), то установить приоритет трафика IP = 4».

Один из наиболее многообещающих проектов в области управления сетью на основе правил реализуется в настоящее время IETF: это исследования, связанные с определением стандартной инфраструктуры для применения данной методологии, а также набора необходимых протоколов и схем работы. Согласно уже имеющимся материалам IETF, в составе типичной сети, администрируемой по набору правил, должны присутствовать следующие элементы:

- консоль для задания стратегий – средство администрирования, с помощью которого сетевой администратор создает и редактирует набор правил управления;
- точка принятия решений (policy decision point, PDP) – сервер, обеспечивающий выборку правил из хранилища и выработку решений;
- точки реализации стратегий (policy enforcement point, PEP) – различные сетевые устройства (маршрутизаторы, коммутаторы и брандмауэры), претворяющие в жизнь решения PDP (т.е. правила управления сетью) с помощью списков доступа, алгоритмов управления очередями и других средств;

- хранилище стратегий – способный работать с протоколом LDAP сервер, на котором в специальном каталоге хранятся стратегии.

Связь между элементами PDP и PEP обеспечивает несложный протокол запросов/ответов Common Open Policy Service (COPS). Его преимущества перед SNMP состоят в ориентации на соединения (он охватывает процесс установления/разрыва соединения), большей надежности и наличии механизмов, предотвращающих попытки одновременного обновления данных одной точки PEP несколькими PDP.

Однако предложенная схема не определяет способов реализации означенной инфраструктуры. Возможны сосуществование на одном сервере различных компонентов или работа каждого из них на отдельном компьютере.

Типичная сеть с поддержкой администрирования на основе стратегий и механизмов обеспечения QoS показана на рис. 5.11. Ее построение потребует интеграции множества серверов, LDAP-каталогов, использования разных протоколов и сетевых устройств: коммутаторов/маршрутизаторов опорной сети PEP 1, коммутаторов/маршрутизаторов непосредственного подключения терминалов PEP 2, коммутаторов/маршрутизаторов территориально-распределенной сети PEP 3.

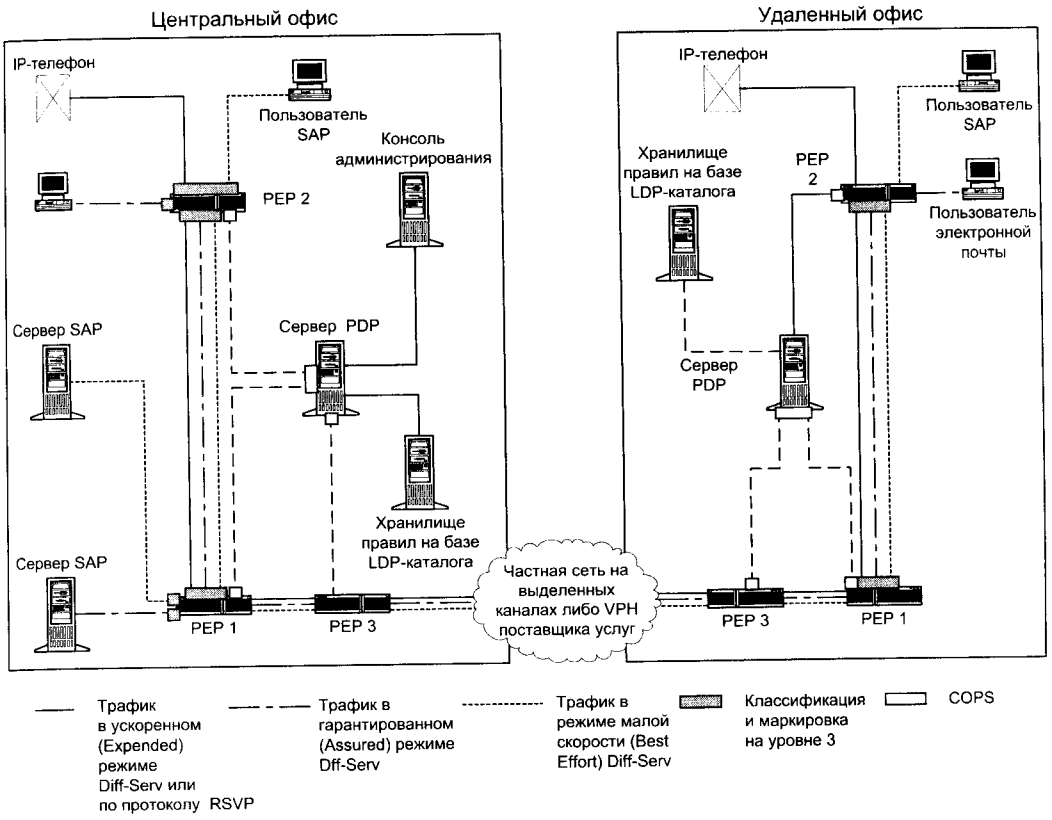


Рис. 5.11. Типичная сеть с поддержкой администрирования на основе стратегий и механизмов обеспечения QoS

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.

Уже сейчас между производителями существует соглашение, закрепляющее некоторые технические аспекты данной технологии. Так, информация о стратегиях должна храниться в LDAP-совместимом каталоге. Группа PFWG построила отображение модели Core Information Model на структуру каталога LDAP. Концепции, заложенные в эту модель, не только пользуются широкой поддержкой производителей, но и закреплены IETF в проектах нескольких стандартов. Хотя ни один из них еще не достиг стадии предложений по спецификациям (request for comments, RFC), они дают ясное представление о том, как построить сеть, управляемую по заданным правилам.

Ближайшие перспективы администрирования на основе стратегий в среде, состоящей из продуктов различных производителей, оставляют желать лучшего. К сожалению, реализации механизмов работы с набором правил и алгоритмы формирования трафика сильно различаются не только в продуктах разных производителей, но даже в пределах ассортимента одной компании. Чтобы добиться реальной совместимости устройств или их единого администрирования, нужны стандартные модели общих функций для задания и выполнения алгоритмов и формирования трафика. Необходимо также обеспечить единое представление схемы реализации QoS и информации о стратегиях в базе данных Policy Information Base (PIB), равно как и поддержку работы с PIB сетевыми устройствами.

Большинство производителей ограничивается рамками собственного оборудования и, по мере сил, реализацией совместимости с продукцией Cisco. Однако обширный список механизмов QoS, поддерживаемых устройствами этой компании, с каждым днем становится все длиннее. На начальном этапе все инициативы в области администрирования сетей на основе стратегий сосредоточены на обеспечении QoS, но в дальнейшем органы стандартизации и производители обратят внимание и на сетевую безопасность.

За последний год-полтора не осталось ни одного крупного производителя, не анонсировавшего решений для управления сетями на основе набора правил; однако пока лишь немногие из них довели дело до готового продукта.

5.13. Организационные аспекты обеспечения параметров качества IP-телефонии

Многие компании не имеют ресурсов или опыта управления сетью из конца в конец, поэтому они часто обращаются к сервис-провайдерам (первичным провайдерам) за услугами глобальных сетей. В прошлом провайдерам было достаточно поддерживать постоянную работоспособность своих сетей, чтобы абоненты могли передавать и получать информацию, когда им необходимо.

Но с распространением приложений реального времени, и, в частности, Интернет-телефонии, провайдеры все чаще сталкиваются с тем, что для сохранения своего бизнеса и привлечения клиентов им необходимо принять специальные меры для этих типов информационных потоков.

Один из способов сделать это – заключение соглашений об уровне сервиса (Service Level Agreement, SLA), т. е. контрактов, где четко указано, какого уровня доступность, сервисы и цены ожидает получить заказчик. В таком соглашении сервис-провайдеры должны гарантировать срок бессбойной работы и длительность задержки в конкретное время суток для конкретных видов приложений. Оно также может содержать информацию о доступности пользовательского соединения.

SLA должно также определять, какие сервисы и, что более важно, гарантии обслуживания предлагаются для каждого класса трафика. Кроме того, оно должно указывать пропускную способность (скорость, с которой пакеты передаются по сети), задержку (время между отправкой и приемом пакетов на конечных станциях), процент потерянных пакетов (максимально возможное число удаленных при передаче пакетов) и вариацию задержки (разницу во времени доставки пакетов из одного потока).

Сервис-провайдер может определить два или более уровней QoS и взимать за них соответствующую плату. Наинизший уровень QoS может использоваться для доставки данных по мере возможности по типу Internet. Более высокий уровень обслуживания – для критически важных данных, включая приложения ERP с низким процентом потерянных пакетов и контролируемой задержкой. Самый высокий уровень обслуживания – для приложений реального времени типа видеоконференции и видеосвязи; этот уровень должен характеризоваться очень малой задержкой и вариацией задержки, а также очень низким процентом потерянных пакетов.

Заказчики должны иметь способ мониторинга реального уровня QoS. Это может делаться посредством аудита журналов сетевых ресурсов. Сервис-провайдеры также должны вести учет, чтобы быть уверенными, что они выполняют условия контракта.

Качество услуг может являться ключевым дифференцирующим фактором между сервис-провайдерами в их борьбе за клиентуру. SLA представляют собой один из способов предложить определенный стандарт обслуживания, опираясь на который заказчики могли бы реализовать доставку трафика реального времени.

Глава 6

АДРЕСАЦИЯ В СЕТЯХ IP-ТЕЛЕФОНИИ

6.1. 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 нумерации 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. 6.1.

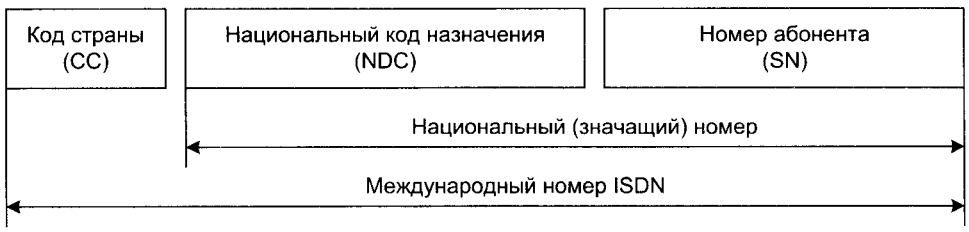


Рис. 6.1. Структура международного номера сети общего пользования

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.164. 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.160.

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.

6.2. 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-A0-17-3D-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 маши-

ны, 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:

128.10.2.30 - традиционная десятичная форма представления адреса,

10000000 00001010 00000010 00011110 – двоичная форма представления этого же адреса. На рис. 6.2 показана структура IP-адреса.

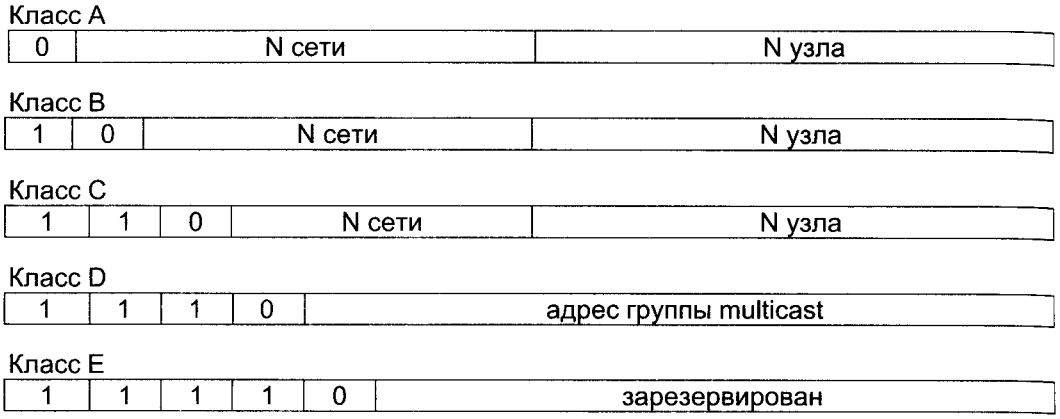


Рис. 6.2. Структура IP-адреса

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 зарезервирован для специальных целей, о чем будет сказано ниже.) В сетях класса A количество 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. 6.1 приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

Таблица 6.1. Диапазоны номеров IP-сетей

Класс	Наименьший адрес	Наибольший адрес
A	01.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0.	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	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 протокола ARP зависит от типа сети. На рис. 6.3 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}.

0 8 16 31

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)		

Рис. 6.3. Формат пакета протокола ARP

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 и 2 для 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.

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 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:

- com – 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 в 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 распределением. 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 DHCP 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, использованной 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 информацию, 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 и 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 позволит 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 с возможностью репликации.

Главная цель объединения серверов – дать пользователям возможность встраивать в их системы управления сетевыми адресами средства повышения надежности, безопасности и 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 соответствующим 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.164 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.

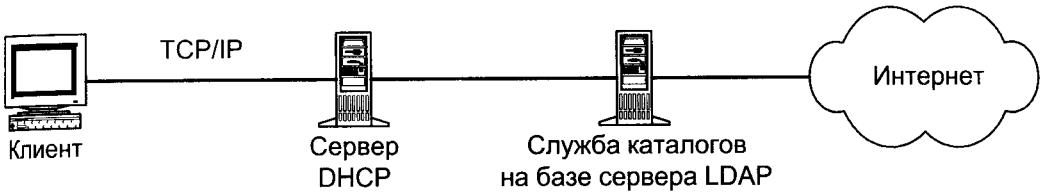


Рис. 6.4. Процесс взаимодействия серверов DHCP и LDAP

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:

010	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 имеется 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.

6.3. 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.164 используются конечными пользователями, чтобы идентифицировать вызов. В IP-системах, когда конечный пользователь идентифицируется терминалом, номер E.164 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.164). 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, ограничиваясь 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.164. 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.164 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 концепцией TIPHON и решениями по Интернет-телефонии, основанными на протоколе SIP.

Цель преобразования номера – замена цифр, набранных вызывающим пользователем, в имена E.164 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 иные 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 подстановочным номером 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.164 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.164 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.164. 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 7

СИСТЕМЫ БИЛЛИНГА И МЕНЕДЖМЕНТА ПОЛЬЗОВАТЕЛЕЙ IP-ТЕЛЕФОНИИ

7.1. Особенности систем биллинга и менеджмента пользователей IP-телефонии

Исходя из общих принципов реализации сети IP-телефонии ее пользователи должны получать те же услуги, что и при использовании традиционной телефонной связи. Однако использование IP-сети в качестве транспортной архитектуры позволяет провайдерам предоставлять пользователям целый набор услуг, основанных на протоколе IP (передача данных, факсимильных сообщений, электронной почты, видео и др.). Особенности предоставления услуг IP-телефонии и других видов IP-услуг выдвигают специфические требования к организации системы биллинга и менеджмента пользователей.

Традиционные пакетно-ориентированные биллинг-системы просто неспособны выполнить требования провайдеров IP-телефонии. Такие биллинг-системы первоначально разрабатывались для более медленных темпов расчетов и с пакетно-ориентированным составлением счетов для услуг телефонной связи, обеспечивали предоставление информации по запросу только в конце цикла расчетов или месяца (рис. 7.1, а). Эти системы обычно разрабатывались под конкретного заказчика, с длинными циклами развития и недостаточной гибкостью, которая требуется для быстро развивающихся услуг IP-телефонии.

Проблема заключается в том, что IP-телефония основывается на непосредственном взаимодействии с пользователями – поэтому провайдеры должны постоянно следить за каждым их действием. Информация об этих действиях не должна запаздывать, так как это может повлиять на действия пользователя. В конечном счете, провайдеры должны быть чрезвычайно гибки и оперативны при предоставлении услуг, которые они предлагают, они должны быстро предлагать новые услуги для продажи и эффективно управлять пользователями.

Таким образом, реализация услуг IP-телефонии требует нового подхода к построению систем менеджмента и биллинга. Провайдеры должны иметь такие системы, которые обеспечат комплексные возможности в реальном масштабе времени, неограниченную гибкость и масштабируемость для менеджмента и ускоренного внедрения мультисервисных IP-услуг (рис. 7.1, б). Это позволит им быстро разрабатывать новые услуги, снижать тарифы, эффективно управлять пользователями и осуществлять расчетные операции при сохранении достаточной гибкости в ответ на изменяющиеся требования рынка и запросы потребителей.

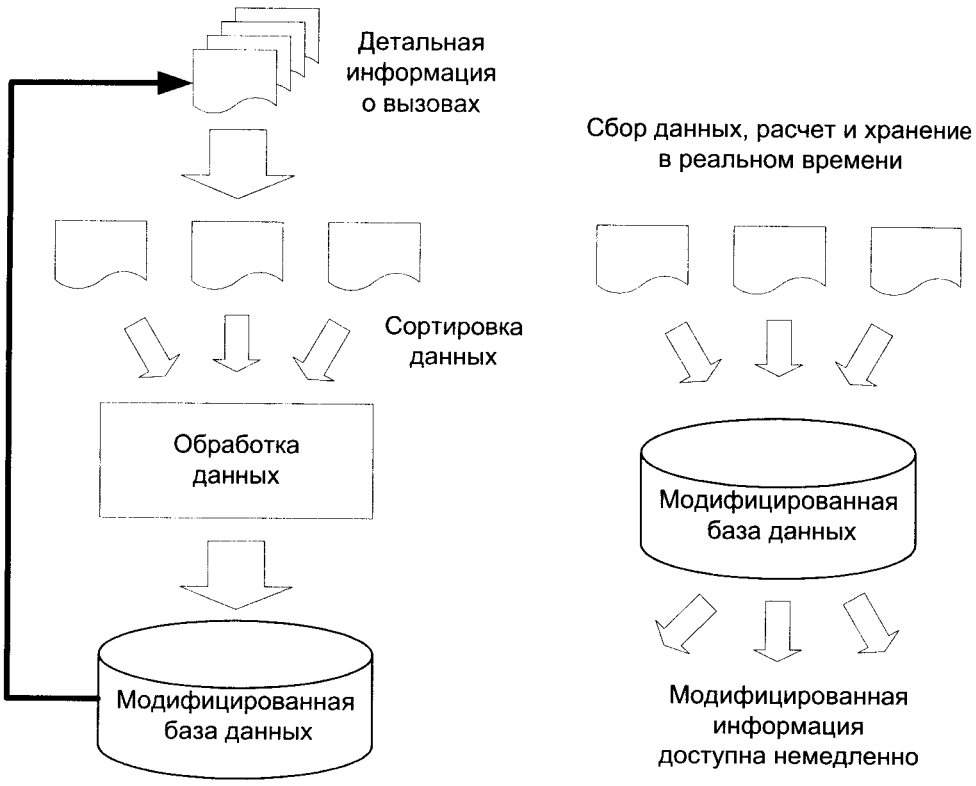


Рис. 7.1. Принципы функционирования системы менеджмента и биллинга: а) обычная телефония; б) IP-телефония

7.2. Требования к системе биллинга и менеджмента пользователей IP-телефонии

Работа в реальном масштабе времени

При традиционной телефонной связи программное обеспечение, которое выполняет расчеты за пользование услугами телефонной связи, не имеет непосредственного контакта с абонентом во время разговора. Детальная информация о вызовах (CDR) поступает от телефонных станций в течение месяца и только в конце месяца (или расчетного периода) вся собранная информация о вызовах передается в биллинг-систему.

Этот метод расчетов за услуги связи не подходит для рынка услуг IP-телефонии, который часто не регулируется и чрезвычайно конкурентный. Провайдеры IP-телефонии должны иметь возможность следить за любым действием каждого заказчика и информация о них должна поступать не в конце месяца, когда уже слишком поздно осуществлять воздействие.

Поэтому система менеджмента и биллинга, используемая для поддержки услуг IP-телефонии, должна быть способна отслеживать и управлять действиями абонентов в реальном времени (рис. 7.2). Система биллинга и менеджмента пользователей реального масштаба времени даст возможность провайдерам получать информацию немедленно и использовать ее в своей работе.

Рис. 7.2. Обслуживание вызова IP-телефонии при использовании комплексной системы биллинга и менеджмента реального масштаба времени

Кроме того, система биллинга и менеджмента пользователей должна не только обеспечивать расчеты в реальном масштабе времени, но и позволять развертывать новые услуги достаточно быстро, чтобы воспользоваться преимуществом появления их на рынке. При необходимости система должна рассчитывать, отслеживать и анализировать трафик и состояние счетов пользователей. Система должна быть гибкой, чтобы эффективно отвечать на конкурентное давление и удовлетворять требованиям провайдеров IP-телефонии.

Поддержка предоплаты

Опыт внедрения IP-телефонии показывает, что предоплаченные услуги составляют главную часть вызовов IP-телефонии. Предоплаченные телефонные карточки позволяют провайдерам IP-телефонии избегать неоплаты и задолженности по оплате. Система биллинга и менеджмента пользователей в реальном масштабе времени должна обеспечивать жесткие требования провайдеров по контролю за возможностями предоплаченных карт. В этом случае провайдеры могут предлагать любые предоплаченные услуги, включая дебетные карты, непополняемые и пополняемые предоплаченные счета. Система биллинга и менеджмента пользователей должна позволять строить комплексную архитектуру реального времени, которая обеспечит:

- поиск наилучшего пути для вызова;
- множественный доступ при одном предоплаченном счете;
- уведомление по электронной почте при уменьшении ниже нормы суммы на счету;
- пополнение счета через телефон или WEB-интерфейс;
- получение информации о зональных тарифах, остатках на счетах и другой информации по обработке и маршрутированию заранее оплаченных вызовов в реальном времени.

Поддержка вторичных провайдеров

Вторичные провайдеры (субпровайдеры) – быстро развивающийся и прибыльный сегмент бизнеса IP-телефонии. Это позволяет первичным провайдерам воспользоваться преимуществом модели бизнеса вне своей фирменной марки, когда их корпоративные пользователи становятся "виртуальными" провайдерами IP-телефонии или провайдерами фирменных услуг (Branded Service Provider – BSP). Такие вторичные провайдеры предлагают продукты или услуги Интернет-телефонии под их собственной корпоративной маркой без необходимости создания инфраструктуры менеджмента и поддержки услуг первичной сети.

Системы биллинга и менеджмента пользователей вторичных провайдеров должны поддерживаться подобной системой первичного провайдера для обеспечения всех услуг IP-телефонии. Это дает возможность первичным провайдерам предложить их вторичным провайдерам полный диапазон услуг по биллингу и менеджменту – создание счетов, тарификация, расчет, составление счетов, менеджмент пользователями и выписка счетов.

Система биллинга и менеджмента должна гарантировать абсолютную защиту данных пользователей, тарифных планов, счетов и сообщений и обеспечивать безопасный доступ вторичного провайдера к системе в реальном масштабе времени.

Идентификация в реальном масштабе времени

Идентификация означает проверку индивидуальной подлинности пользователя, однако при традиционной телефонной связи такая идентификация не требуется. Владелец телефонной линии ответственен за любые вызовы, сделанные с его телефона. Независимо от того, произведен вызов самим владельцем телефона, членом семьи, гостем или даже незнакомцем – телефонная компания связывает все вызовы с владельцем этого подключения.

Однако при услугах IP-телефонии – делает ли пользователь вызов из дома или офиса, с обычного телефона или компьютера – все вызовы должны быть связаны с определенным пользователем даже при его путешествии. Система биллинга и менеджмента пользователей IP-телефонии должна поддерживать надежные механизмы идентификации, чтобы опознавать пользователя уникально, и обеспечивать изменение этих механизмов в реальном времени.

Авторизация в реальном масштабе времени

Авторизация обеспечивает разрешение предоставления пользователю тех услуг, которые он требует. В традиционных биллинг-системах отсутствует взаимодействие с пользователями в реальном масштабе времени и в них нет никакой встроенной возможности обеспечения авторизации.

При IP-телефонии провайдеру услуг, как правило, требуется проверка по различным критериям, прежде чем он предоставит услугу пользователю. Каково текущее состояние кредита пользователя? Оплатил ли пользователь счета за прошедшие месяцы? Имеет ли пользователь приоритеты при международных вызовах? Подписывался ли пользователь на услуги факсимильной связи?

Такие запросы означают, что система биллинга и менеджмента, используемая для IP-телефонии, должна позволять провайдерам выполнять авторизацию в реальном масштабе времени перед тем, как услуга будет доступна пользователю (см. рис. 7.3).

Создание новых услуг и планов тарификации

На рынке услуг традиционной телефонной связи при отсутствии конкуренции провайдеры услуг телефонии могут достаточно медленно вводить новые услуги на рынок. Обычно проходят годы между концепцией построения и развертыванием новых услуг связи.

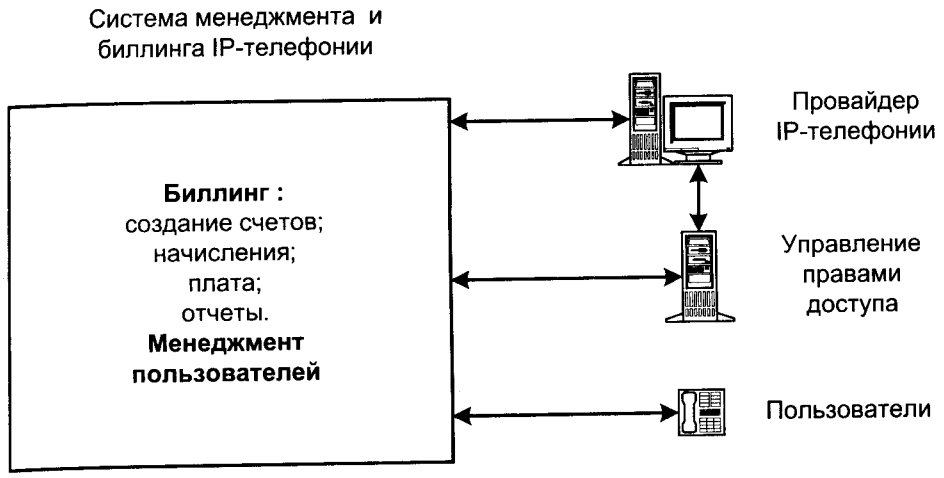


Рис. 7.3. Интеграция биллинг-системы с системой управления правами доступа

На высококонкурентном рынке IP-услуг провайдеры должны иметь возможность быстро отвечать на изменяющиеся рыночные условия. Таким образом, системы биллинга и менеджмента пользователей IP-телефонии должны позволять провайдеру быстро и легко создавать новые пакеты услуг телефонной связи, набор планов тарификации и быстро предлагать на рынок новые услуги.

Поддержка комплекса услуг

Провайдер, который предлагает услуги IP-телефонии, как правило, предлагает и другие услуги связи на рынок. Эти услуги могут включать традиционную модемную связь для доступа в Интернет и электронной почты, а также другие выгодные бизнес-услуги: предоставление необходимой полосы пропускания в сети, виртуальная частная сеть (VPN) и видеоконференцсвязь.

В результате, система биллинга и менеджмента пользователей в реальном времени должна быть приспособлена к любому число предложений IP-услуг. Это должно быть обеспечено централизованным менеджментом пользователей, управлением услугами, расчетами, трафиком в пределах единственной базы данных, которая, в конечном счете, обеспечит провайдерам более простое расширение спектра предлагаемых услуг.

Обеспечение качества обслуживания (QoS)

В IP-телефонии пакеты данных, которые содержат речевую информацию, передаются по IP-сети и проходят через множество путей до места назначения. Так как различные пакеты, содержащие сегменты одного и того же речевого сообщения, проходят различные маршруты, они имеют тенденцию прибывать в различном порядке к адресату, а некоторые пакеты могут даже потеряться и никогда не достигнут адресата. Эти факторы приводят к различной степени качества услуги передачи речи через IP-сеть.

Как правило, пользователи IP-телефонии требуют обеспечения определенного качества обслуживания, платя больше за более высокое качество и надежность или меньше – за

низкокачественные услуги, например, за одностороннюю связь. Система биллинга и менеджмента пользователей должна обеспечивать возможность провайдерам выбирать направление передачи вызовов: или через каналы сети Интернет с заранее определенной максимальной временной задержкой, или через частные IP-сети для самого высокого качества обслуживания, или через IP-сети общего пользования, когда стоимость, а не качество передачи речи является более существенным фактором.

Гибкость системы

Чтобы оставаться лидерами в предоставлении любых IP-услуг, провайдеры должны иметь возможность быстро добавить или изменить услуги, информацию о пользователе, тарифы и другие данные без прерывания выполняемых функций и без расходов на дополнительное программирование. Программное обеспечение системы биллинга и менеджмента пользователей IP-телефонии должно строится по блочно-функциональному принципу для обеспечения его быстрого внедрения у провайдера и возможностей масштабирования. Кроме этого, система должна работать с любым сетевым окружением для сбора детальной информации о вызовах (CDR) и интегрироваться с любыми прикладными системами финансовыми учета (рис. 7.4).

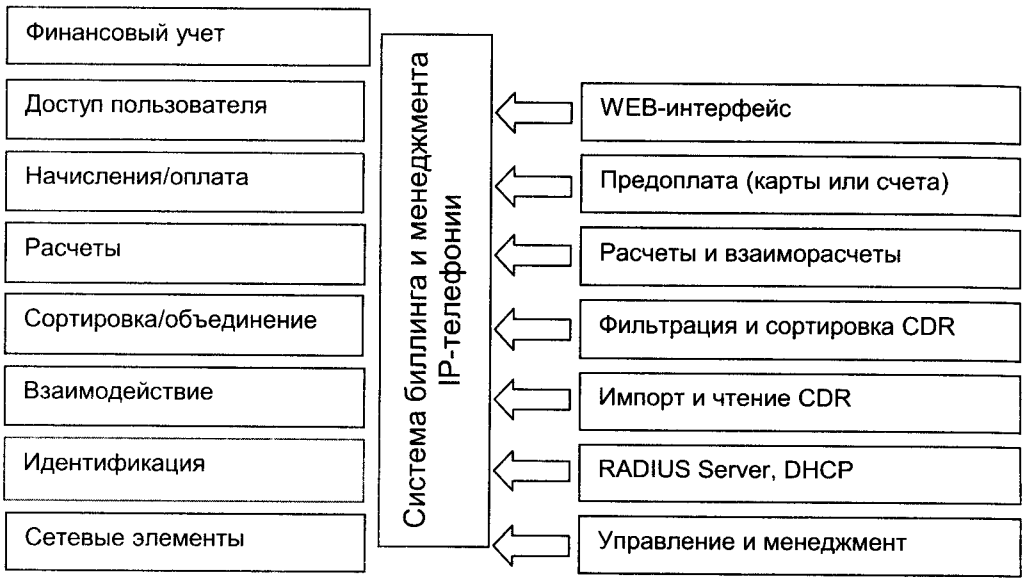


Рис. 7.4. Функциональные уровни системы биллинга и менеджмента IP-телефонии

Поддержка шлюзов IP-телефонии

В настоящее время переход речевого трафика из коммутируемых сетей общего пользования в IP-сети обеспечивает различное оборудование шлюзов VoIP. Этот подход становится все более критическим местом для системы биллинга и менеджмента пользователей, так как она должна работать с разнообразными шлюзами VoIP. Кроме этого постоянно идет развитие аппаратно-программных средств IP-телефонии. Следовательно, перспективная ар-

хитектура системы биллинга и менеджмента пользователей IP-телефонии должна обеспечивать быструю и легкую интеграцию с новыми шлюзами и другими компонентами телефонной связи в единую систему (рис. 7.5).

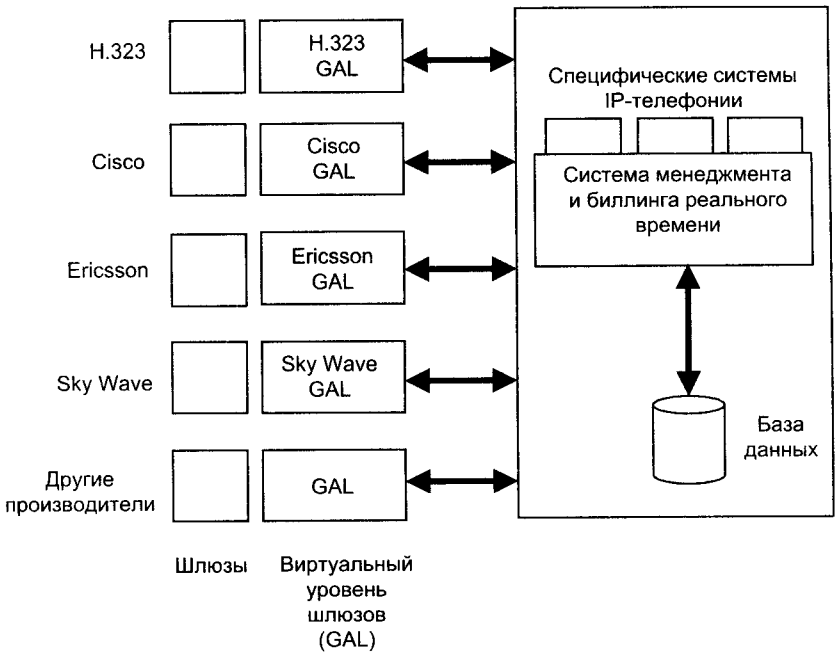


Рис. 7.5. Интеграция системы биллинга и менеджмента с системами IP-телефонии

7.3. Обзор систем биллинга и менеджмента пользователей IP-телефонии

Система Internet Management System

Система *Internet Management System (IMS 3.1)* фирмы *Belle Systems* является многофункциональной системой биллинга и менеджмента пользователей IP-телефонии, основанной на взаимодействии с сетевыми элементами. Данная система позволяет конфигурировать и управлять широким спектром сетевого оборудования, включая серверы доступа, маршрутизаторы и голосовые шлюзы фирмы Cisco. Интеграция с программным обеспечением фирм Atlantech Technologies и Orchestream, обеспечивает универсальный интерфейс для управления уровнем сетевых элементов. В систему встраивается сервер RADIUS для обеспечения идентификации пользователей при доступе через коммутируемую сеть. Система IMS обеспечивает гибкие схемы тарификации для пользователей, возможность контроля параметров QoS, поддержку систем финансового учета и бизнес-управления типа Oracle Financials и SAP. Для телефонных сетей общего пользования и мобильных сетей система IMS может интегрироваться с финансовыми системами фирм EHPT, Kenan и Saville на базе платформы CORBA. Система рассчитана на поддержку более 20 миллионов счетов и 1 миллиона пользователей и

предназначена для крупных операторов связи. Типовая архитектура системы IMS показана на рис. 7.6.

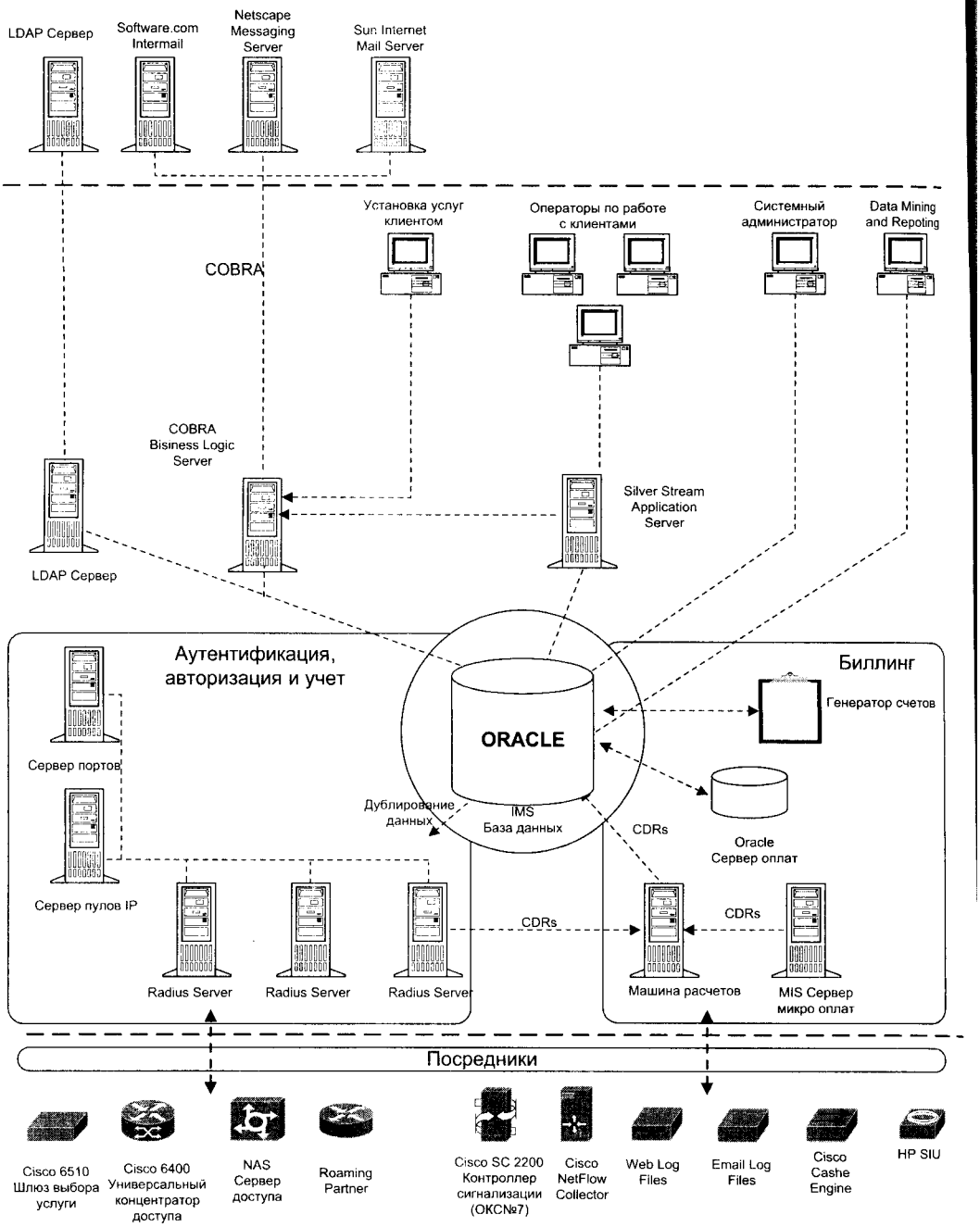


Рис. 7.6. Архитектура системы IMS

Система iPhoneEX

Система биллинга и менеджмента пользователей IP-телефонии *iPhoneEX* фирмы *MIND CTI* полностью интегрирована со всеми версиями шлюзов VocalTec, а также работает с оборудованием фирм Ascend, Lucent и Arelnet. Система может поддерживать от 100 до 100.000 пользователей. Составление счетов может выполняться из одного центрального пункта для всех узлов сети и в каждом узле сети.

Система IPhonEX обеспечивает четыре различных формы расчетов с пользователями.

- Неограниченный кредит – пользователи имеют неограниченную возможность получения услуг Интернет-телефонии.
- Ограниченный кредит – при достижении предела кредита учетная запись автоматически блокируется в реальном масштабе времени и пользователю дается отказ в предоставлении услуг до оплаты кредита.
- Дебетовая плата/Телефонные карточки – при достижении заранее оплаченного количества минут разговора дальнейшие запросы на услугу отвергаются и учетная запись блокируется.
- Дебетовая плата с пополнением – производится определенная предоплата, когда стоимость разговоров достигает оплаченного количества, учетная запись блокируется, но имеется возможность доплатить снова.

В состав системы IPhonEX входят следующие модули:

- *Модуль межсетевого биллинга Inter-Billing system* – обеспечивает взаиморасчеты между провайдерами Интернет-телефонии в сети. Модуль позволяет распределять затраты между различными узлами и различными операторами. Обеспечивает детальные сообщения данных по требованию для каждого провайдера.
- *Модуль управления вызовами Call Management Module* – обеспечивает пользователям большой набор сложных запросов сообщений управления. Система содержит мощный Генератор запросов, который позволяет пользователю генерировать настроенные сообщения с необходимой информацией. Все итоговые сообщения, созданные Генератором Запросов, могут быть представлены в графической форме.
- *Модуль безопасности Guard Module* – обеспечивает обнаружение несанкционированного доступа с помощью контроля за определенным набором параметров, задаваемых самим пользователем.
- *Модуль трафика Traffic* – является инструментом для анализа загрузок шлюза. Полученные данные могут служить основой для оптимального распределения ресурсов и наиболее эффективных мер экономии финансовых затрат. Возможна генерация сообщений, которые включают число вызовов в минуту для некоторой области, группу номеров, шлюзы и т.д.

Системные требования:

- Операционная система Windows NT 4;
- Процессор Pentium, оперативная память 64 Мбайт, жесткий диск 4 Гбайт.

Система Infranet IPT

Система *Infranet IPT* фирмы *Portal Software* объединяет управление всеми основными операциями бизнеса IP-телефонии, включая способность регистрировать, управлять пользователями и организовывать расчеты за предоставленные услуги. Ее архитектура функционирует в реальном масштабе времени и является открытой средой развития, обеспечивая платформу для создания службы управления телефонной связи в IP-сети.

Особенности работы системы Infranet IPT в реальном масштабе времени включают:

- регистрацию пользователя;
- идентификацию вызывающего абонента;
- проверку предела кредита;
- добавление к заранее оплаченной сумме и включение в учетную запись;
- работу с кредитными карточками;
- возможность выбора маршрута наименьшей стоимости;
- междоменное согласование и регулирование тарифов.

Система имеет специальную архитектуру абстрактного уровня шлюзов, которая позволяет настраивать работу со шлюзами IP-телефонии любого производителя. Infranet IPT может поддерживать обслуживание нескольких миллионов пользователей и ее программное обеспечение основывается на операционных системах HP UNIX, Microsoft Windows NT, SUN/Solaris и сервере Oracle или Microsoft SQL.

Система Talking NT Enterprise SQL

Система *Talking NT Enterprise SQL* фирмы *Telephony Experts* является мультимедийным приложением на основе операционной системы Windows NT, способным к обработке многих типов телефонных разговоров. Система интегрируется со шлюзом VocalTec для управления трафиком, который терминирует шлюз. Система Talking NT включает базу данных сервера MS SQL и обеспечивает составление счетов в реальном масштабе времени, гибкий выбор маршрута наименьшей стоимости, качество обслуживания по требованию, предупреждение об окончании предоплаты, автоматическое завершение вызова при окончании оплаты, управление вызовом со стороны пользователя.

Система Talking NT обеспечивает следующие дополнительные возможности:

- заранее оплаченная и без предварительной оплаты дебетовая карточка;
- международный обратный вызов;
- 1 + набор номера (группа особенностей D);
- заранее оплаченный беспроводный доступ;
- услуги 800/888;
- услуга персонального номера;
- речевая почта с пейджингом;
- пополняемая кредитная карточка.

Пример использования системы Talking NT на сети показан на рис. 7.7.

Система Telephony Gateway Billing Manager

Система *Telephony Gateway Billing Manager*™ фирмы *Telephony Experts* (рис. 7.8) может применяться в сети IP-телефонии, построенной на базе шлюза VocalTec Telephony Gateway™ Series 30™ и на VocalTec Ensemble Architecture™ (VEA), используя VocalTec Gatekeeper. Система является платформой аутентификации и биллинга, основанной на Windows NT ™ и SQL Microsoft ™ Server v. 6.5 или выше. Стандартные особенности включают средства контроля доступа к услугам и биллинг в реальном времени на базе предоплаты или постоплаты., а также различные средства управления учетными записями. Система может масштабироваться для обработки фактически неограниченного числа учетных записей и может быть сконфигурирована для защищенного доступа в любой точке через Интернет.

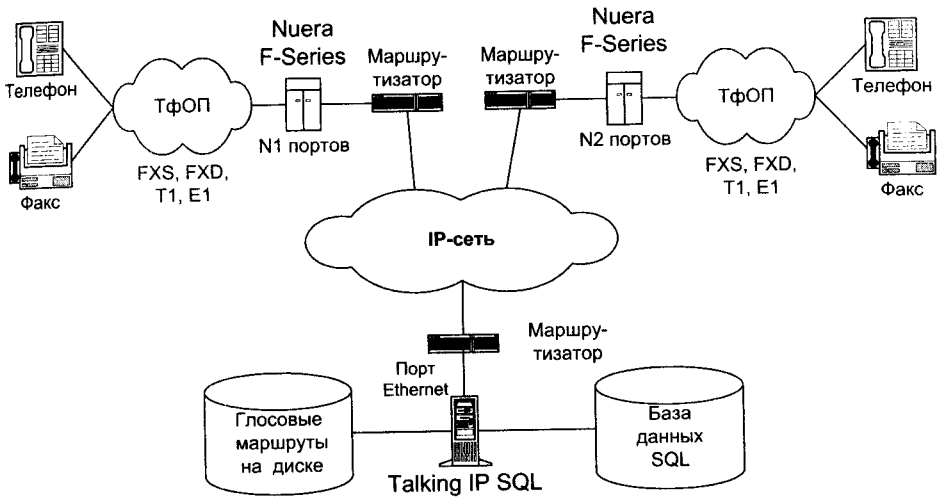


Рис. 7.7. Пример использования системы Talking NT Enterprise SQL

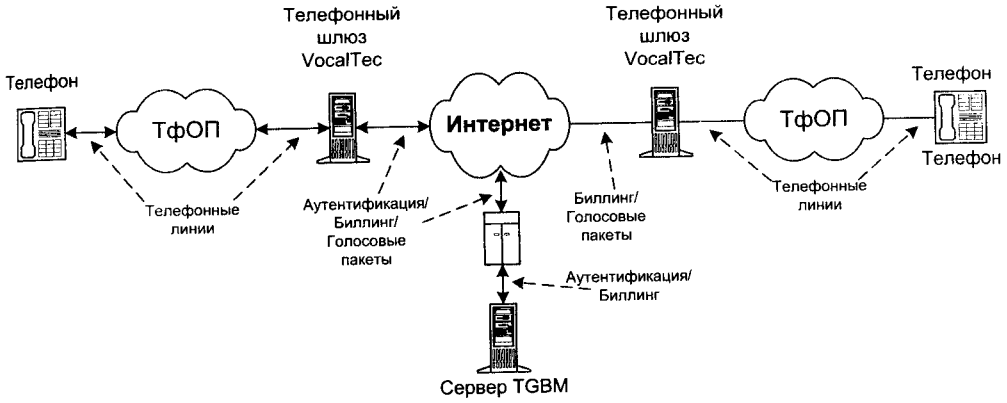


Рис. 7.8. Модель биллинга на базе системы Telephony Gateway Billing Manager

Система BizBill

Биллинговая система *BizBill* фирмы *Biztrans* позволяет провайдерам Интернет предоставлять услуги Интернет-телефонии через их узлы доступа и обеспечивает все расчетные операции в одном центре. Система BizBill обеспечивает интеграцию расчетов за Интернет и Интернет-телефонию, рассчитывает баланс и выдает необходимую информацию. Используемый в системе интерфейс Интернет дает возможность пользователю регистрироваться интерактивно. Система работает под управлением Windows NT/95 и предназначена для работы со шлюзами VocalTec.

Система IAF Horizon

Система *IAF Horizon* фирмы *Solect Technology Group* является многофункциональной платформой для поддержки IP-услуг. Система используется с оборудованием IP-телефонии

ведущих производителей: Cisco, Ericsson, Nokia и Telcordia Technologies. В дополнение к традиционным услугам тарификации IP-телефонии с предоплатой система IAF Horizon обеспечивает:

- предоставление услуг по заранее оплаченным телефонным карточкам с оценкой остатка в реальном масштабе времени;
- поддержку управления вызовом во время соединения;
- управление телефонной карточкой, включая создание размера оплаты и контроль оплаченного времени соединения;
- использование сообщений интерактивной системы ответа IVR, которые могут быть записаны и настроены на язык вызывающего пользователя;
- простоту создания и управления алгоритмами тарификации, включая создание различных вариантов тарификации применительно к географическим комбинациям;
- перенаправление вызова и блокирование номера;
- расширенные возможности составления счетов, например, с посекундной оплатой, со свободным периодом и с различными коэффициентами и параметрами дисконтирования.

Система IAF Horizon обеспечивает аутентификацию в реальном масштабе и расчет с абонентами сети Интернет-телефонии, построенной на базе оборудования фирм Cisco и Ericsson. Архитектура системы IAF Horizon показана на рис. 7.9.

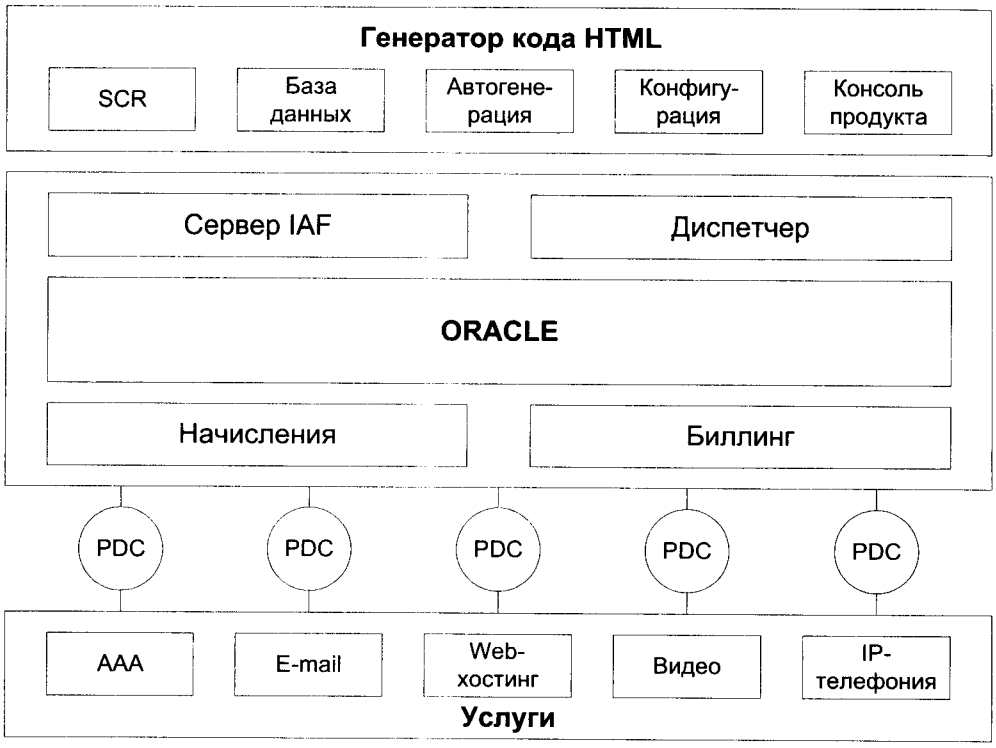


Рис. 7.9. Архитектура системы IAF Horizon

Основные технические характеристики систем биллинга и менеджмента пользователей IP-телефонии приведены в приложении 3.

Глава 8

БЕЗОПАСНОСТЬ IP-ТЕЛЕФОНИИ

8.1. Типы угроз в сетях IP-телефонии

Вопрос безопасности связи всегда был одним из важных в сетях телекоммуникаций. В настоящее время в связи с бурным развитием глобальных компьютерных сетей, и в том числе сетей Интернет-телефонии, обеспечение безопасности передачи информации становится еще более актуальным. Разработка мероприятий в области безопасности должна проводиться на основе анализа рисков, определения критически важных ресурсов системы и возможных угроз. Существует несколько основных типов угроз, представляющих наибольшую опасность в сетях IP-телефонии.

1. Подмена данных о пользователе

Подмена данных о пользователе означает, что один пользователь сети выдает себя за другого. При этом возникает вероятность несанкционированного доступа к важным функциям системы. Использование механизмов аутентификации и авторизации в сети повышает уверенность в том, что пользователь, с которым устанавливается связь, не является подставным лицом и что ему можно предоставить санкционированный доступ.

2. Подслушивание

Во время передачи данных о пользователях (пользовательских идентификаторов и паролей) или частных конфиденциальных данных по незащищенным каналам эти данные можно подслушать и впоследствии злоупотреблять ими. Методы шифровки данных снижают вероятность этой угрозы.

3. Манипулирование данными

Данные, которые передаются по каналам связи, в принципе можно изменить. Во многих методах шифрования используется технология защиты целостности данных, предотвращающая их несанкционированное изменение.

4. Отказ от обслуживания (Denial of Service – DoS)

Отказ от обслуживания (DoS) является разновидностью хакерской атаки, в результате которой важные системы становятся недоступными. Это достигается путем переполнения системы ненужным трафиком, на обработку которого уходят все ресурсы системной памяти и процессора. Система связи должна иметь средства для распознавания подобных атак и ограничения их воздействия на сеть.

Базовыми элементами в области безопасности являются аутентификация, целостность и активная проверка. *Аутентификация* призвана предотвратить угрозу обезличивания и несанкционированного доступа к ресурсам и данным. Хотя авторизация не всегда включает в свой состав аутентификацию, но чаще всего одно обязательно подразумевает другое. *Целостность* обеспечивает защиту от подслушивания и манипулирования данны-

ми, поддерживая конфиденциальность и неизменность передаваемой информации. И, наконец, *активная проверка* означает проверку правильности реализации элементов технологии безопасности и помогает обнаруживать несанкционированное проникновение в сеть и атаки типа DoS.

8.2. Методы криптографической защиты информации

Основой любой защищенной связи является *криптография*. Криптографией называется технология составления и расшифровки закодированных сообщений. Кроме того, криптография является важной составляющей для механизмов аутентификации, целостности и конфиденциальности. Аутентификация является средством подтверждения личности отправителя или получателя информации. Целостность означает, что данные не были изменены, а конфиденциальность создает ситуацию, при которой данные не может понять никто, кроме их отправителя и получателя. Обычно криптографические механизмы существуют в виде *алгоритма* (математической функции) и секретной величины (*ключа*). Алгоритмы широко известны, в секрете необходимо держать только криптографические ключи. Причем чем больше битов в таком ключе, тем менее он уязвим.

В системах обеспечения безопасности используются три основных криптографических метода:

- симметричное шифрование;
- асимметричное шифрование;
- односторонние хэш-функции.

Все существующие технологии аутентификации, целостности и конфиденциальности созданы на основе именно этих трех методов. Например, цифровые подписи можно представить в виде сочетания асимметричного шифрования с алгоритмом односторонней хэш-функции для поддержки аутентификации и целостности данных.

Симметричное шифрование, которое часто называют шифрованием с помощью секретных ключей, в основном используется для обеспечения конфиденциальности данных. При этом два пользователя должны совместно выбрать единый математический алгоритм, который будет использоваться для шифрования и расшифровки данных. Кроме того, им нужно выбрать общий ключ (секретный ключ), который будет использоваться с принятым ими алгоритмом шифрования/расшифровки.

В настоящее время широко используются алгоритмы секретных ключей типа Data Encryption Standard (DES), 3DES (или «тройной DES») и International Data Encryption Algorithm (IDEA). Эти алгоритмы шифруют сообщения блоками по 64 бита. Если объем сообщения превышает 64 бита (как это обычно и бывает), необходимо разбить его на блоки по 64 бита в каждом, а затем каким-то образом свести их воедино. Такое объединение, как правило, происходит одним из следующих четырех методов: электронной кодовой книги (ECB), цепочки зашифрованных блоков (CBC), x-битовой зашифрованной обратной связи (CFB-x) или выходной обратной связи (OFB).

Шифрование с помощью секретного ключа чаще всего используется для поддержки конфиденциальности данных и очень эффективно реализуется с помощью неизменяемых «вшитых» программ (firmware). Этот метод можно использовать для аутентификации и поддержания целостности данных, но метод цифровой подписи является более эффективным.

Метод секретных ключей имеет следующие недостатки:

- необходимо часто менять секретные ключи, поскольку всегда существует риск их случайного раскрытия;
- трудно обеспечить безопасное генерирование и распространение секретных ключей.

Асимметричное шифрование часто называют шифрованием с помощью общего ключа, при котором используются разные, но взаимно дополняющие друг друга ключи и алгоритмы шифрования и расшифровки. Этот механизм полагается на два взаимосвязанных ключа: общего ключа и частного ключа. Наиболее типичные примеры использования алгоритмов общих ключей:

- обеспечение конфиденциальности данных;
- аутентификация отправителя;
- безопасное получение общих ключей для совместного использования.

Важным аспектом асимметричного шифрования является то, что частный ключ должен храниться в тайне. Если частный ключ будет раскрыт, то человек, знающий этот ключ, сможет выступать от вашего имени, получать ваши сообщения и отправлять сообщения так, будто это сделали вы.

Механизмы генерирования пар общих/частных ключей являются достаточно сложными, но в результате получаются пары очень больших случайных чисел, одно из которых становится общим ключом, а другое – частным. Генерирование таких чисел требует больших процессорных мощностей, поскольку эти числа, а также их произведения должны отвечать строгим математическим критериям. Однако этот процесс генерирования абсолютно необходим для обеспечения уникальности каждой пары общих/частных ключей. Алгоритмы шифрования с помощью общих ключей редко используются для поддержки конфиденциальности данных из-за ограничений производительности. Вместо этого их часто используют в приложениях, где аутентификация проводится с помощью цифровой подписи и управления ключами.

Среди наиболее известных алгоритмов общих ключей можно назвать RSA и ElGamal.

Безопасной хэш-функцией называется функция, которую легко рассчитать, но обратное восстановление которой требует непропорционально больших усилий. Входящее сообщение пропускается через математическую функцию (хэш-функцию), и в результате на выходе получают некую последовательность битов. Эта последовательность называется «хэш» (или «результат обработки сообщения»). Этот процесс невозможно восстановить.

Хэш-функция принимает сообщение любой длины и выдает на выходе хэш фиксированной длины. Обычные хэш-функции включают:

- алгоритм Message Digest 4 (MD4);
- алгоритм Message Digest 5 (MD5);
- алгоритм безопасного хэша (Secure Hash Algorithm – SHA).

Технология шифрования часто используется в приложениях, связанных с управлением ключами и аутентификацией. Например, алгоритм Диффи-Хеллмана позволяет двум сторонам создать общий для них секретный ключ, известный только им двоим, несмотря на то, что связь между ними осуществляется по незащищенному каналу. Затем этот секретный ключ используется для шифрования данных с помощью алгоритма секретного ключа. Важно отметить, что на сегодня пока не создано средств для определения автора такого ключа, поэтому обмен сообщениями, зашифрованными этим способом, может подвергаться хакерским атакам. Алгоритм Диффи-Хеллмана используется для поддержки конфиденциальности данных, но не используется для аутентификации. Аутентификация в данном случае достигается с помощью цифровой подписи.

Цифровая подпись представляет собой зашифрованный хэш, который добавляется к документу. Она может использоваться для аутентификации отправителя и целостности документа. Цифровые подписи можно создавать с помощью сочетания хэш-функций и криптографии общих ключей.

Сообщение, которое отправляется по каналу связи, состоит из документа и цифровой подписи. На другом конце канала связи сообщение делится на оригинальный документ и цифровую подпись. Так как цифровая подпись была зашифрована частным ключом, то на приемном конце можно провести ее расшифровку с помощью общего ключа. Таким образом, на приемном конце получается расшифрованный хэш. Далее подается текст документа на вход той же функции, которую использовала передающая сторона. Если на выходе получится тот же хэш, который был получен в сообщении, целостность документа и личность отправителя можно считать доказанными.

Цифровым сертификатом называется сообщение с цифровой подписью, которое в настоящее время обычно используется для подтверждения действительности общего ключа. Цифровой сертификат в стандартном формате X.509 включает следующие элементы:

- номер версии;
- серийный номер сертификата;
- эмитент информации об алгоритме;
- эмитент сертификата;
- даты начала и окончания действия сертификата;
- информация об алгоритме общего ключа субъекта сертификата;
- подпись эмитирующей организации.

На практике часто используют совместно шифрование и цифровые сертификаты. Например, маршрутизатор и межсетевой экран имеют по одной паре общих/частных ключей (рис. 8.1). Предположим, что эмитирующей организации (CA) удалось получить сертификаты X.509 для маршрутизатора и межсетевого экрана по защищенным каналам. Далее предположим, что маршрутизатор и межсетевой экран тоже получили копии общего ключа CA по защищенным каналам. Теперь, если на маршрутизаторе имеется трафик, предназначенный для межсетевого экрана, и если маршрутизатор хочет обеспечить аутентификацию и конфиденциальность данных, необходимо предпринять следующие шаги.

1. Маршрутизатор отправляет в эмитирующую организацию CA запрос на получение общего ключа межсетевого экрана.
2. CA отправляет ему сертификат межсетевого экрана, зашифрованный частным ключом CA.
3. Маршрутизатор расшифровывает сертификат общим ключом CA и получает общий ключ межсетевого экрана.
4. Межсетевой экран направляет CA запрос на получение общего ключа маршрутизатора.
5. CA отправляет ему сертификат маршрутизатора, зашифрованный частным ключом CA.
6. Межсетевой экран расшифровывает сертификат общим ключом CA и получает общий ключ маршрутизатора.
7. Маршрутизатор и межсетевой экран используют алгоритм Диффи-Хеллмана и шифрование с помощью общих ключей для аутентификации.
8. С помощью секретного ключа, полученного в результате использования алгоритма Диффи-Хеллмана, маршрутизатор и межсетевой экран проводят обмен конфиденциальными данными.

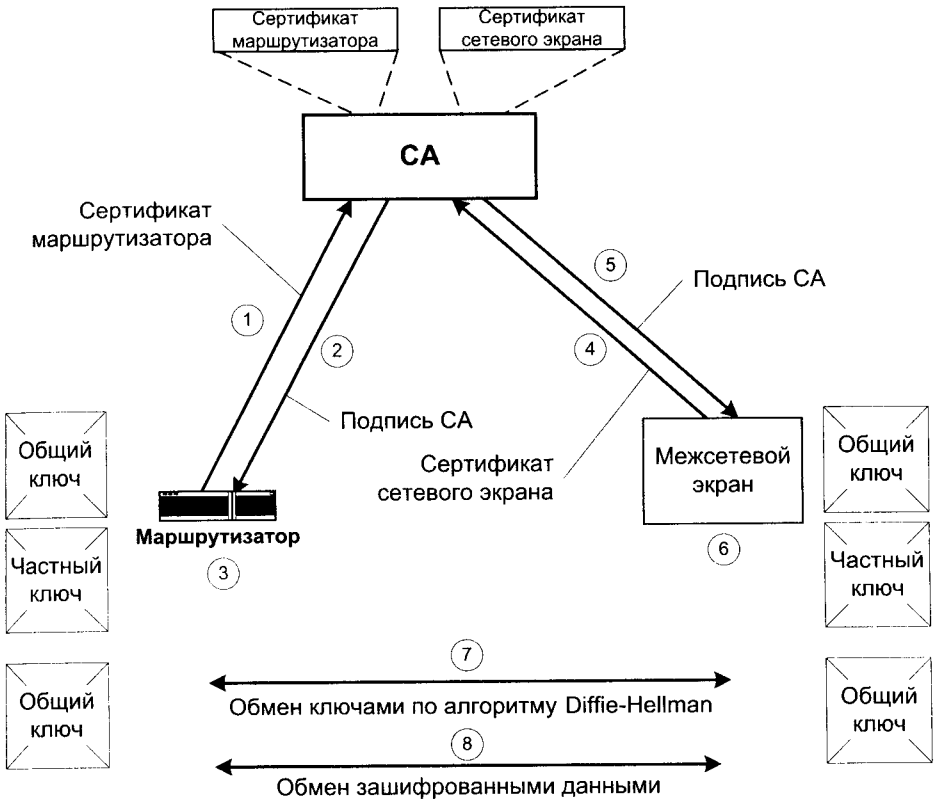


Рис. 8.1. Безопасная связь с использованием шифрования

8.3. Технологии аутентификации

Под *аутентификацией* понимается определение пользователя или конечного устройства (клиента, сервера, коммутатора, маршрутизатора, межсетевого экрана и т.д.) и его местоположения в сети с последующей авторизацией пользователей и конечных устройств. Наиболее простым способом аутентификации является использование паролей, но для поддержания высокого уровня безопасности пароли приходится часто менять. Методы использования одноразовых паролей применяются по-прежнему широко. Среди них можно отметить методы аутентификации по протоколу S/Key или при помощи специальных аппаратных средств (token password authentication). Механизм аутентификации по протоколу Point-to-Point Protocol (PPP) часто применяется в среде модемного доступа и включает использование протоколов *Password Authentication Protocol (PAP)*, *Challenge Handshake Protocol (CHAP)* и *Extensible Authentication Protocol (EAP)*. Разработка протокола EAP все еще продолжается, но уже сейчас он дает возможность более гибкого использования существующих и только появляющихся технологий аутентификации в каналах PPP. TACACS+ и Remote Access Dial-In User Service (RADIUS) – это протоколы, которые поддерживают масштабируемые решения в области аутентификации. Протокол Kerberos (Цербер) используется в ограниченных областях для поддержки единой точки входа в сеть.

Система одноразовых паролей S/Key, определенная в RFC 1760, представляет собой систему генерирования одноразовых паролей на основе стандартов MD4 и MD5. Она предназначена для борьбы «повторными атаками», когда хакер подслушивает канал, выделяет из трафика идентификатор пользователя и его пароль и в дальнейшем использует их для несанкционированного доступа.

Система S/Key основана на технологии клиент-сервер, где клиентом обычно является персональный компьютер, а сервером – сервер аутентификации. Вначале и клиента, и сервер нужно настроить на единую парольную фразу и счет итерации. Клиент начинает обмен S/Key, отправляя серверу пакет инициализации, а сервер в ответ отправляет порядковый номер и случайное число, так называемое «зерно» (seed). После этого клиент генерирует одноразовый пароль.

После создания одноразового пароля его нужно проверить. Для этого клиент передает одноразовый пароль на сервер, где он и проверяется. Для проверки аутентификации система однократно пропускает полученный одноразовый пароль через защищенную хэш-функцию. Если результат этой операции совпадает с предыдущим паролем, хранящимся в файле, результат аутентификации считается положительным, а новый пароль сохраняется для дальнейшего использования.

Аутентификация с помощью аппаратных средств работает по одной из двух альтернативных схем:

- по схеме запрос-ответ;
- по схеме аутентификации с синхронизацией по времени.

В схеме запрос-ответ пользователь подключается к серверу аутентификации, который, в свою очередь, предлагает ввести персональный идентификационный номер (PIN) или пользовательский идентификатор (user ID). Пользователь передает PIN или user ID на сервер, который затем делает «запрос» (передает случайное число, которое появляется на экране пользователя). Пользователь вводит это число в специальное аппаратное устройство, похожее на кредитную карточку, где число запроса шифруется с помощью пользовательского шифровального ключа. Результат шифрования отображается на экране. Пользователь отправляет этот результат на сервер аутентификации. В то время как пользователь подсчитывает этот результат, сервер аутентификации рассчитывает этот же результат самостоятельно, используя для этого базу данных, где хранятся все пользовательские ключи. Получив ответ от пользователя, сервер сравнивает его с результатом собственных вычислений. Если оба результата совпадают, пользователь получает доступ к сети. Если результаты оказываются разными, доступ к сети не предоставляется.

При использовании *схемы с синхронизацией по времени* на аппаратном устройстве пользователя и на сервере работает секретный алгоритм, который через определенные синхронизированные промежутки времени генерирует идентичные пароли и заменяет старые пароли на новые. Пользователь подключается к серверу аутентификации, который запрашивает у пользователя код доступа. После этого пользователь вводит свой PIN в аппаратное карточное устройство, и в результате на экран выводится некоторая величина, которая представляет собой одноразовый пароль. Этот пароль и отправляется на сервер. Сервер сравнивает его с паролем, который был вычислен на самом сервере. Если пароли совпадают, пользователь получает доступ к сети.

Протокол PPP

Аутентификация на основе протокола Point-to-Point Protocol (PPP) – это популярное средство инкапсуляции (упаковки), которое часто используется в глобальных сетях. В его состав входят три основных компонента:

- метод инкапсуляции дейтаграмм в последовательных каналах;
- протокол *Link Control Protocol (LCP)*, который используется для установления, конфигурирования и тестирования связи;
- семейство протоколов *Network Control Protocols (NCP)* для установки и конфигурирования различных протоколов сетевого уровня.

Чтобы установить прямую связь между двумя точками по каналу PPP, каждая из этих точек должна сначала отправить пакеты LCP для конфигурирования связи на этапе ее установления. После установления связи и прежде чем перейти к этапу работы на протоколах сетевого уровня, протокол PPP дает (при необходимости) возможность провести аутентификацию.

По умолчанию аутентификация является необязательным этапом. В случае, если аутентификация требуется, в момент установления связи система указывает дополнительную конфигурацию протоколов аутентификации. Эти протоколы используются, в основном, центральными компьютерами и маршрутизаторами, которые связаны с сервером PPP через коммутируемые каналы или линии телефонной связи, а, возможно, и через выделенные каналы. Во время согласования на сетевом уровне сервер может выбрать опцию аутентификации центрального компьютера или маршрутизатора.

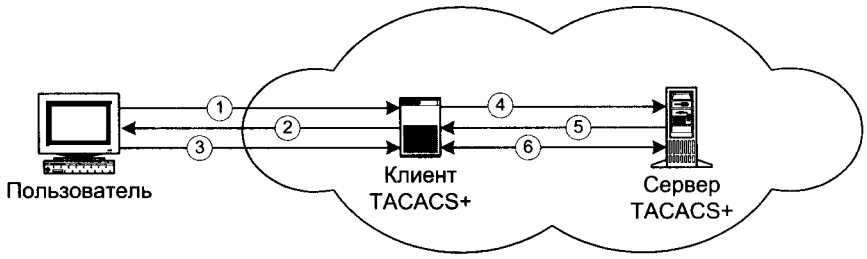
Протоколы EAP и CHAP представляют собой два метода аутентификации протокола PPP. EAP – это общий протокол аутентификации PPP, который поддерживает множество идентификационных механизмов. Этот протокол находится в процессе доработки, и в будущем он сможет поддерживать более современные механизмы аутентификации в рамках аутентификации PPP. Аутентификация происходит после согласования LCP и до согласования *IP Control Protocol (IPCP),* в ходе которого происходит обмен адресами IP. Этот процесс аутентификации проходит в автоматическом режиме и не требует от пользователей ввода в компьютер каких-либо данных при подключении PPP. Часто аутентификация PAP или CHAP занимает место переговорного сценария, который отвечает на запросы о вводе сетевого имени пользователя (login) и пароля. CHAP поддерживает более высокий уровень безопасности, поскольку не передает реальный пароль по каналу PPP. Однако PAP используется чаще.

Протокол TACACS

TACACS – это простой протокол управления доступом, основанный на стандартах User Datagram Protocol (UDP) и разработанных компанией Bolt, Beranek and Newman, Inc. (BBN). Компания Cisco несколько раз совершенствовала и расширяла протокол TACACS, и в результате появилась ее собственная версия TACACS, известная как TACACS+. TACACS+ пользуется транспортным протоколом TCP. Демон сервера «слушает» порт 49, который является портом протокола IP, выделенным для протокола TACACS. Этот порт зарезервирован для выделенных номеров RFC в протоколах UDP и TCP. Все текущие версии TACACS и расширенные варианты этого протокола используют порт 49.

Протокол TACACS+ работает по технологии клиент-сервер, где клиентом TACACS+ обычно является NAS, а сервером TACACS+, как правило, считается "демон" (процесс, запускаемый на машине UNIX или NT). Фундаментальным структурным компонентом протокола TACACS+ является разделение аутентификации, авторизации и учета (AAA – Authentication, Authorization, Accounting). Это позволяет обмениваться идентификационными сообщениями любой длины и содержания, и, следовательно, использовать для клиентов TACACS+ любой идентификационный механизм, в том числе PPP PAP, PPP CHAP, аппаратные карты и Kerberos (рис. 8.2). Аутентификация не является обязательной. Она рассматри-

вается как опция, которая конфигурируется на месте. В некоторых местах она вообще не требуется, в других местах она может применяться лишь для ограниченного набора услуг.



Клиент и сервер TACACS+ должны иметь общий секретный ключ

1. Пользователь инициирует соединение PPP с сервером доступа
2. Сервер доступа запрашивает у пользователя имя и пароль
3. Пользователь отвечает на запрос
4. Клиент TACACS+ посылает зашифрованный пакет серверу TACACS+
5. Сервер TACACS+ сообщает результаты идентификации
6. Клиент и сервер обмениваются авторизационной информацией
7. Клиент TACACS+ обрабатывает параметры, полученные во время авторизации

Рис. 8.2. Взаимодействие между пользователем и системой TACACS+

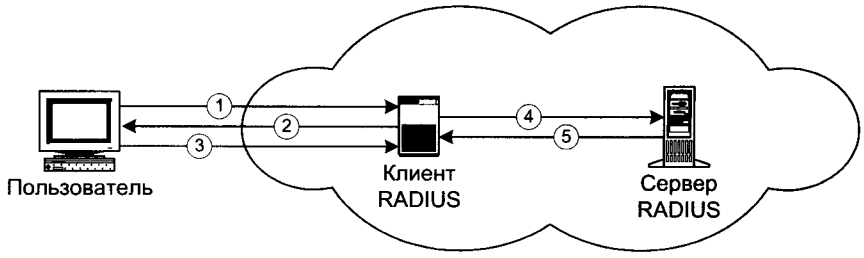
Авторизация – это процесс определения действий, которые позволены данному пользователю. Обычно аутентификация предшествует авторизации, однако это не обязательно. В запросе на авторизацию можно указать, что аутентификация пользователя не проведена (личность пользователя не доказана). В этом случае лицо, отвечающее за авторизацию, должно самостоятельно решить, допускать такого пользователя к запрашиваемым услугам или нет. Протокол TACACS+ допускает только положительную или отрицательную авторизацию, однако этот результат допускает настройку на потребности конкретного заказчика. Авторизация может проводиться на разных этапах, например, когда пользователь впервые входит в сеть и хочет открыть графический интерфейс или когда пользователь запускает PPP и пытается использовать поверх PPP протокол IP с конкретным адресом IP. В этих случаях демон сервера TACACS+ может разрешить предоставление услуг, но наложить ограничения по времени или потребовать список доступа IP для канала PPP.

Учет обычно следует за аутентификацией и авторизацией. *Учет* представляет собой запись действий пользователя. В системе TACACS+ учет может выполнять две задачи. Во-первых, он может использоваться для учета использованных услуг (например, для выставления счетов). Во-вторых, его можно использовать в целях безопасности. Для этого TACACS+ поддерживает три типа учетных записей. Записи «старт» указывают, что услуга должна быть запущена. Записи «стоп» говорят о том, что услуга только что окончилась. Записи "обновление" (update) являются промежуточными и указывают на то, что услуга все еще предоставляется. Учетные записи TACACS+ содержат всю информацию, которая используется в ходе авторизации, а также другие данные: время начала и окончания (если это необходимо) и данные об использовании ресурсов.

Транзакции между клиентом TACACS+ и сервером TACACS+ идентифицируются с помощью общего «секрета», который никогда не передается по каналам связи. Обычно этот секрет вручную устанавливается на сервере и на клиенте. TACACS+ можно настроить на шифрование всего трафика, который передается между клиентом TACACS+ и демоном сервера TACACS+.

Протокол RADIUS

Протокол RADIUS был разработан компанией Livingston Enterprises, Inc. в качестве протокола аутентификации серверного доступа и учета. В настоящее время спецификация RADIUS (RFC 2058) и стандарт учета RADIUS (RFC 2059) предложены для утверждения в качестве общепринятых стандартов IETF.



Клиент и сервер RADIUS должны иметь общий секретный ключ

1. Пользователь инициирует соединение PPP с сервером доступа

2. Сервер доступа запрашивает у пользователя имя и пароль

3. Пользователь отвечает на запрос

4. Клиент RADIUS посылает имя пользователя и зашифрованный пароль серверу RADIUS

5. Сервер RADIUS отвечает сообщениями Accept, Reject или Challenge

6. Клиент RADIUS обрабатывает параметры, полученные от сервера вместе с сообщениями Accept или Reject

Рис. 8.3. Взаимодействие между пользователем и системой RADIUS

Связь между NAS и сервером RADIUS основана на протоколе UDP. В целом считается, что протокол RADIUS не имеет отношения к подключению. Все вопросы, связанные с доступностью сервера, повторной передачей данных и отключениями по истечении времени ожидания, контролируются устройствами, работающими под управлением протокола RADIUS, но не самим протоколом передачи.

Протокол RADIUS основан на технологии клиент-сервер (рис. 8.3). Клиентом RADIUS обычно является NAS, а сервером RADIUS считается «демон», работающий на машине UNIX или NT. Клиент передает пользовательскую информацию на определенные серверы RADIUS, а затем действует в соответствии с полученными от сервера инструкциями. Серверы RADIUS принимают запросы пользователей на подключение, проводят идентификацию

пользователей, а затем отправляют всю конфигурационную информацию, которая необходима клиенту для обслуживания пользователя. Для других серверов RADIUS или идентификационных серверов других типов сервер RADIUS может выступать в роли клиента-посредника (proxy).

8.4. Особенности системы безопасности в IP-телефонии

В системе IP-телефонии должны обеспечиваться два уровня безопасности: системный и вызывной.

Для обеспечения системной безопасности используются следующие функции.

- Предотвращение неавторизованного доступа к сети путем применения разделяемого кодового слова. Кодовое слово одновременно вычисляется по стандартным алгоритмам на инициирующей и оконечной системах, и полученные результаты сравниваются. При установлении соединения каждая система IP-телефонии первоначально идентифицирует другую систему, в случае отрицательного результата связь прерывается и вносится соответствующая запись в журнал.
- Списки доступа, в которые вносятся все известные шлюзы IP-телефонии.
- Запись отказов в доступе.
- Функции безопасности интерфейса доступа, включая:
  - проверку идентификатора и пароля пользователя с ограничением доступа по чтению/записи;
  - проверку прав доступа к специальному WEB-серверу для администрирования.
- Функции обеспечения безопасности вызова включают:
  - проверку идентификатора и пароля пользователя (необязательно);
  - статус пользователя;
  - профиль абонента.

При установлении связи шлюза с другим шлюзом своей зоны производится необязательная проверка идентификатора и пароля пользователя. Пользователь в любое время может быть лишен права доступа.

Профили абонентов создаются для каждого пользователя, в них содержится информация о службах/приложениях, доступных данному абоненту. Возможные варианты:

- голос ТфОП – ТфОП;
- факс ТфОП – ТфОП;
- компьютер – ТфОП;
- службы, определенные пользователем (при помощи API).

Профиль абонента используется для проверки права доступа абонента к запрошенным службам.

8.5. Обеспечение безопасности в системах на базе стандарта H.323

Для систем IP-телефонии, построенных на базе Рекомендации ITU-T H.323, вопросы безопасности рассматриваются в Рекомендации H.235 (рис. 8.4). Эта рекомендация описыва-

ет ряд технических требований, включая вопросы безопасности: аутентификация пользователей и шифрование данных. Предложенная схема обеспечения безопасности применима и к простым двухточечным и к многоточечным конференциям для любых терминалов, которые используют протокол управления H.245. Если для IP-телефонии стандарта H.323 используются сети с пакетной коммутацией, не обеспечивающие гарантированного качества обслуживания QoS, то по тем же самым техническим причинам не обеспечивается и безопасное обслуживание. Для обеспечения гарантированной связи в реальном масштабе времени по опасным сетям необходимо рассматривать две главных области обеспечения безопасности – аутентификация и секретность.

Рис. 8.4. Область действия Рекомендации H.235 в серии Рекомендаций H.323

В соответствии с Рекомендацией H.235 в системе должны быть реализованы четыре основные функции безопасности:

- аутентификация;
- целостность данных;
- секретность;
- проверка отсутствия долгов.

Аутентификация пользователя обеспечивается управлением доступа в конечной точке сети и выполняется gatekeeper, являющимся администратором зоны H.323. Аутентификация основывается на использовании общих ключей с цифровым сертификатом. Для авторизации сертификатов они включают, например, идентификаторы провайдера услуг. Рекомендация H.235 не определяет содержание цифровых сертификатов, используемых соответствующим протоколом аутентификации, а также их генерацию, администрирование и распределение.

Целостность данных и секретность обеспечивается криптозащитой. Проверка отсутствия долгов гарантируется тем, что конечная точка может отказать в обслуживании вызова. Для обеспечения безопасности согласно рекомендации H.235 могут использоваться существующие стандарты: IP-безопасность (IP Security – IPSec) и безопасность транспортного уровня (Transport Layer Security – TLS).

Для обеспечения безопасной связи в системе на базе Рекомендации H.323 используются механизмы защиты информации канала управления вызовами Q.931, информации канала управления для мультимедиа коммуникаций H.245, информации каналов передачи мультимедиа. Канал управления вызовом (H.225.0) и канал сигнализации (H.245) должны оба работать в защищенном или незащищенном режимах, начинающимся с первой станции. Для канала управления вызовом защита сделана априорно (для систем в соответствии с Рекомендацией H.323 безопасность транспортного уровня обеспечивается соответствующим протоколом TSAP [порт 1300], который должен использоваться для Q.931 сообщений). Для канала сигнализации режим «защита» определяется информацией, переданной с помощью протокола начальной установки и подключения терминалов стандарта H.323.

В целом следует отметить, что все основные механизмы аутентификации, определенные в Рекомендации H.235, идентичны или получены из алгоритмов, разработанных Международной организации по стандартизации ISO, или основаны на протоколах IETF.

8.6. Механизмы безопасности в проекте TIPHON

В проект TIPHON включены следующие механизмы защиты для обеспечения безопасной телефонной связи с конечных устройств, основанные на приложении J Рекомендации ITU-T H.323:

- механизм защиты, основанный на цифровых сертификатах (CBSP);
- механизм защиты, основанный на паролях (PBSP);
- механизм защиты, основанный на шифровании информации.

Основным механизмом защиты является использование цифровых сертификатов. Реализация функций безопасности в данном механизме показана в табл. 8.1. В тех странах, где технология CBSP не реализована, должен использоваться механизм на базе паролей. Однако следует отметить, что PBSP является самым простым механизмом и не обеспечивает уровень защиты, реализуемый при использовании CBSP.

Криптографическая защита информации является необязательным требованием и используется только в сценариях, когда необходимо обеспечить секретность передаваемой информации. Оба механизма CBSP и PBSP используют модель безопасности при маршрутизации через шлюз на базе Приложения F Рекомендации H.323.

Таблица 8.1. Механизм безопасности TIPHON, основанный на сертификатах

Функции безопасности	Функции обслуживания вызовов		
	RAS	H.225.0	H.245
Аутентификация	Цифровая подпись SHA1/MD5 (Процедура А)	Цифровая подпись SHA1/MD5 (Процедура А)	Цифровая подпись SHA1/MD5 (Процедура А)
Отказ при наличии долгов	Цифровая подпись SHA1/MD5 (Процедура А)	Цифровая подпись SHA1/MD5 (Процедура А)	Цифровая подпись SHA1/MD5 (Процедура А)
Целостность информации	Цифровая подпись SHA1/MD5 (Процедура А)	Цифровая подпись SHA1/MD5 (Процедура А)	Цифровая подпись SHA1/MD5 (Процедура А)
Управление ключами	Распределение сертификата	Распределение сертификата и обмен ключами для аутентификации по алгоритму Диффи-Хеллмана	Управление общим ключом сеанса связи H.235 (распределение ключа, изменение ключа)

8.7. Обеспечение безопасности на базе протокола OSP

Компании 3Com, Cisco Systems, GRIC Communications, iPass и TransNexus сообщили о поддержке предварительного стандарта IP-телефонии – Open Settlement Protocol (OSP), – который предназначен для решения вопросов взаимодействия сетей различных провайдеров.

Это простой протокол, позволяющий различным компаниям – владельцам средств связи осуществлять коммуникации в пределах всей страны. К примеру, он позволяет устанавливать автора звонка, санкционировать обслуживание вызова и указывать расчетную информацию, которая будет включена в записи, содержащие подробные данные об этой транзакции (рис. 8.5).

Рабочая группа института European Telecommunications Standards Institute (ETSI) одобрила этот протокол, а производители в ближайшее время намерены провести его тестирование. Новый протокол был разработан в рамках проекта TIPHON. Протоколу OSP еще предстоит пройти процедуру окончательной ратификации. Однако ведущие компании, предоставляющие услуги IP-телефонии, включая Ascend, GTE, AT&T и Internet Telephony Exchange Carrier (ITXC), уже заявили о поддержке протокола OSP. В то же время компании Lucent и Nortel выразили свою заинтересованность и в целом готовы поддержать стандарты на IP-телефонию, но от окончательной оценки OSP пока воздержалась.

Основные характеристики спецификации Open Settlement Protocol (OSP):

- шифрование Secure Sockets Layer;
- безопасная аутентификация участников сеанса связи с помощью шифрования открытым и частным ключами;
- поддержка технологии цифровой подписи;
- обмен информацией с помощью XML.

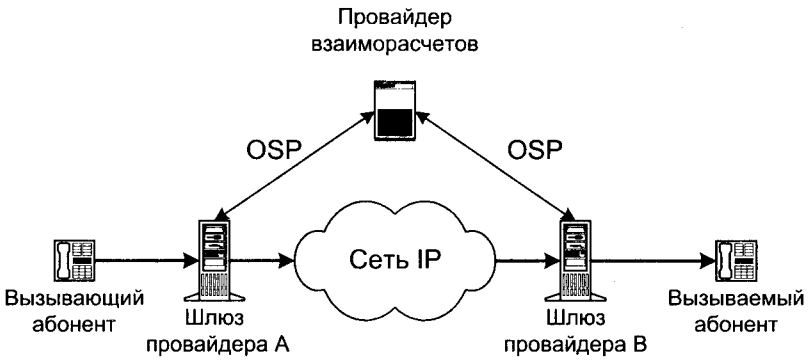


Рис. 8.5. Использование протокола OSP

При условии внедрения единого способа выполнения аутентификации и обеспечения взаимосвязи различных сетей значительно упростится задача выбора провайдера услуг IP-телефонии. В настоящее время ни один провайдер не может пока предлагать свои услуги во всех регионах, а стандартный подход позволит им обеспечить более «прозрачные» службы и в более широкой географической области. Однако при этом возникает целый ряд вопросов. В частности, пока не установлено, каким образом сети будут взаимодействовать друг с другом на уровне расчетов, то есть не определено, как именно передавать между сетями данные о распределении прибыли при обмене.

8.8. Обеспечение безопасности IP-телефонии на базе VPN

Одним из механизмов обеспечения безопасности IP-телефонии может быть использование виртуальных частных сетей (Virtual Private Network, VPN).

Сети VPN создаются, как правило, для решения двух задач. Во-первых, они служат для организации взаимодействия индивидуальных пользователей с удаленной сетью через Интернет, а во-вторых, – для связи двух сетей. В первом случае, они используются в качестве альтернативы удаленному доступу. Вместо того, чтобы устанавливать соединение с корпоративной средой по междугородной или международной связи, пользователи локально подключаются к Интернет и связываются с сетью компании. Во втором – они часто применяются для организации так называемых виртуальных выделенных линий.

Виртуальная частная сеть (VPN) создается между инициатором туннеля и терминатором туннеля. Обычная маршрутизируемая сеть IP (она не обязательно включает в себя общедоступную сеть Интернет) определяет маршрут между инициатором и терминатором. Инициатор туннеля инкапсулирует пакеты в новый пакет, содержащий наряду с исходными данными новый заголовок с информацией об отправителе и получателе. Хотя все передаваемые по туннелю пакеты являются пакетами IP, в принципе, инкапсулируемые пакеты могут принадлежать к протоколу любого типа, включая пакеты немаршрутизируемых протоколов, например, NetBEUI. Терминатор туннеля выполняет процесс, обратный инкапсуляции, удаляя новые заголовки и направляя исходный пакет в локальный стек протоколов или адресату в локальной сети.

Сама по себе инкапсуляция никоим образом не повышает конфиденциальности или целостности туннелируемых данных. Конфиденциальность обеспечивается с помощью шифрования. Поскольку методов шифрования данных существует множество, очень важно, чтобы инициатор и терминатор туннеля использовали один и тот же метод. Кроме того, для успешного дешифрования данных они должны иметь возможность обмена ключами. Чтобы туннели создавались только между уполномоченными пользователями, конечные точки требуется идентифицировать. Целостность туннелируемых данных можно обеспечить с помощью некоей формы выборки сообщения или хэш-функции для выявления изменений или удалений.

Для реализации унифицированного способа инкапсуляции трафика третьего уровня (и более высоких уровней) на клиентах и серверах Windows компании Microsoft, Ascend Communications и 3Com разработали туннельный протокол между двумя точками (Pointto-Point Tunneling Protocol, PPTP), представляющий собой расширение протокола PPP. В PPTP не специфицируется конкретный метод шифрования, однако, клиенты удаленного доступа в Windows NT 4.0 и Windows 95 с Dial-Up Networking 1.2 поставляются с версией шифрования DES компании RSA Data Security, получившей название «шифрование двухточечной связи Microsoft» (Microsoft Point-to-Point Encryption, MPPE).

Компания Cisco Systems разработала протокол пересылки на втором уровне модели OSI (Layer-2 Forwarding, L2F), с помощью которой удаленные клиенты могут связаться по каналам провайдера Internet и быть идентифицированы. При этом ISP не нужно осуществлять конфигурацию адресов и выполнять идентификацию. Протокол L2F стал компонентом операционной системы IOS (Internetwork Operating System) компании Cisco и поддерживается во всех выпускаемых ею устройствах межсетевого взаимодействия и удаленного доступа.

Оба этих тесно связанных друг с другом протокола IETF были объединены, и получившийся в результате протокол, включивший лучшее из PPTP и L2F, называется *протоколом туннелирования второго уровня* (Layer-2 Tunneling Protocol, L2TP). Его поддерживают компании Cisco, Microsoft, 3Com, Ascend и многие другие производители. Как и предшествующие протоколы второго уровня, спецификация L2TP не описывает методы идентификации и шифрования.

Спецификацией IETF, где описаны стандартные методы для всех компонентов VPN, является протокол Internet Protocol Security, или IPSec, – иногда его называют *туннелированием третьего уровня* (Layer-3 Tunneling). IPSec предусматривает стандартные методы идентификации пользователей или компьютеров при инициации туннеля, стандартные способы использования шифрования конечными точками туннеля, а также стандартные методы обмена и управления ключами шифрования между конечными точками. Этот гибкий стандарт предлагает несколько способов для выполнения каждой задачи. Выбранные методы для одной задачи обычно не зависят от методов реализации других задач. Идентификацию можно выполнять с помощью спецификации IPSec, причем она является обязательным компонентом протокола IPv6.

IPSec может работать совместно с L2TP, в результате эти два протокола обеспечивают более надежную идентификацию, стандартизованное шифрование и целостность данных. Следует отметить, что спецификация IPSec ориентирована на IP и, таким образом, бесполезна для трафика любых других протоколов сетевого уровня. Туннель IPSec между двумя локальными сетями может поддерживать множество индивидуальных каналов передачи данных, в результате чего приложения данного типа получают преимущества с точки зрения масштабирования по сравнению с технологией второго уровня.

Некоторые поставщики VPN используют другой подход под названием «посредники каналов» (circuit proxy), или VPN пятого уровня. Этот метод функционирует над транспорт-

ным уровнем и ретранслирует трафик из защищенной сети в общедоступную сеть Internet для каждого сокета в отдельности. (Сокет IP идентифицируется комбинацией TCP-соединения и конкретного порта или заданным портом UDP. Протокол IP не имеет пятого – сеансового - уровня, однако ориентированные на сокеты операции часто называют операциями сеансового уровня.)

Шифрование информации, передаваемой между инициатором и терминатором туннеля, часто осуществляется с помощью защиты транспортного уровня (Transport Layer Security, TLS), ранее протокола защищенных сокетов (Secure Sockets Layer, SSL). Для стандартизации аутентифицированного прохода через брандмауэры IETF определил протокол под названием SOCKS, и в настоящее время SOCKS 5 применяется для стандартизованной реализации посредников каналов.

В SOCKS 5 клиентский компьютер устанавливает аутентифицированный сокет (или сеанс) с сервером, выполняющим роль посредника (proxy). Этот посредник – единственный способ связи через брандмауэр. Посредник, в свою очередь, проводит любые операции, запрашиваемые клиентом. Поскольку посреднику известно о трафике на уровне сокета, он может осуществлять тщательный контроль, например, блокировать конкретные приложения пользователей, если они не имеют необходимых полномочий. Для сравнения, виртуальные частные сети уровня 2 и 3 обычно просто открывают или закрывают канал для всего трафика по аутентифицированному туннелю. Это может представлять проблему, если нет гарантии защиты информации на другом конце туннеля.

Следует отметить на наличие взаимосвязи между брандмауэрами и VPN. Если туннели завершаются на оборудовании провайдера Интернет, то трафик будет передаваться по вашей локальной сети или по линии связи с провайдером Интернет в незащищенном виде. Если конечная точка расположена за брандмауэром, то туннелируемый трафик можно контролировать с помощью средств контроля доступа брандмауэра, но никакой дополнительной защиты при передаче по локальной сети это не даст. В этом случае конечную точку будет связывать с брандмауэром незащищенный канал.

Расположение конечной точки внутри защищаемой брандмауэром зоны обычно означает открытие прохода через брандмауэр (как правило, через конкретный порт TCP). Некоторые компании предпочитают применять реализуемый брандмауэром контроль доступа ко всему трафику, в том числе и к туннелируемому, особенно если другую сторону туннеля представляет пользователь, стратегия защиты которого неизвестна или не внушает доверия. Одно из преимуществ применения тесно интегрированных с брандмауэром продуктов туннелирования состоит в том, что можно открывать туннель, применять к нему правила защиты брандмауэра и перенаправлять трафик на конечную точку на конкретном компьютере или в защищаемой брандмауэром подсети.

Как и любая другая вычислительная функция, работа по созданию сетей VPN проводится с помощью программного обеспечения. Между тем программное обеспечение для VPN может выполняться на самых разных аппаратных платформах. Маршрутизаторы или коммутаторы третьего уровня могут поддерживать функции VNP по умолчанию (или в качестве дополнительной возможности, предлагаемой за отдельную плату). Аппаратно и программно реализуемые брандмауэры нередко предусматривают модули VPN со средствами управления трафиком или без них. Некоторые пограничные комбинированные устройства включают в себя маршрутизатор, брандмауэр, средства управления пропускной способностью и функции VPN (а также режим конфигурации). Наконец, ряд чисто программных продуктов выполняется на соответствующих серверах, кэширует страницы Web, реализует функции брандмауэра и VPN.

Механизм VPN немыслим без идентификации. Инфраструктура с открытыми ключами (Public Key Infrastructure, PKI) для электронной идентификации и управления открытыми ключами является в настоящее время основной. Данные PKI целесообразнее всего хранить в глобальном каталоге, обращаться к которому можно по упрощенному протоколу доступа к каталогу (Lightweight Directory Access Protocol, LDAP).

В табл. 8.2 представлены некоторые системы для организации взаимодействия между пользователями VPN в сети Интернет-телефонии.

Таблица 8.2. Категории систем VPN

Категория системы	Достоинства	Недостатки
Программное обеспечение VPN для брандмауэров	Общее администрирование VPN. Если VPN должны завершаться вне брандмауэра, то канал между окончанием туннеля и брандмауэром может стать уязвимым звеном в системе защиты. При повышении производительности серверных продуктов аппаратное обеспечение потребуется модернизировать.	Операции, связанные с шифрованием данных, могут чрезмерно загружать ЦП и снижать производительность брандмауэра. В случае интегрированных продуктов VPN и брандмауэра оба они могут оказаться не лучшими в своем классе.
VPN на базе маршрутизатора или коммутатора	Интегральные сети VPN могут не потребовать дополнительных расходов на приобретение. Упрощение администрирования VPN.	Функционирование VPN может отрицательно повлиять на другой трафик.
VPN на базе автономного программного обеспечения	Завершение VPN нередко представляет собой сложную задачу. При повышении производительности серверных продуктов аппаратное обеспечение может потребоваться модернизировать. Старые аппаратные средства могут послужить для решения новых задач.	Администрирование VPN может потребовать отдельного приложения, возможно, выделенного каталога.
VPN на базе аппаратных средств	Многофункциональные устройства облегчают конфигурацию и обслуживание в удаленных офисах. Однофункциональные устройства допускают тонкую настройку для достижения наивысшей производительности.	В многофункциональных блоках производительность одного приложения повышается зачастую в ущерб другому. Однофункциональные устройства могут требовать отдельных инструментов администрирования и каталогов. Модернизация для повышения производительности нередко оказывается слишком дорогостоящей или невозможной.

8.9. Реализация функций СОРМ в IP-телефонии

Так как в сетях IP-телефонии используется передача речевой информации между абонентами, то такие сети подпадают под действие системы оперативно-разыскных мероприятий (СОРМ). Для реализации необходимых функций СОРМ необходимо обеспечить возможность фиксации не только всей справочной информации о телефонных вызовах (источник и получатель вызова, дата и время разговора и др.), но и возможность полной записи разговора.

В сети IP-телефонии реализация функций СОРМ может быть выполнена различными способами. В том случае, когда вызывающий абонент включен в телефонную сеть общего пользования (например, сценарии 2 и 3 проекта TIPHON), то функции СОРМ реализуются существующими средствами на телефонных станциях.

При включении исходящих терминалов (например, терминалов H.323 на базе персональных компьютеров) непосредственно в IP-сеть вопросы реализации функций СОРМ должны решаться в оборудовании доступа сети с пакетной коммутацией (серверы доступа, маршрутизаторы, коммутаторы и др.).

Глава 9

МОБИЛЬНОСТЬ В СЕТЯХ IP-ТЕЛЕФОНИИ

9.1. Разновидности мобильности

Сети IP-телефонии должны поддерживать следующие четыре типа мобильности.

1. Мобильность пользователя – способность пользователя соединяться с сетью IP телефонии, используя для соединения различные терминалы и типы терминалов.

2. Мобильность терминала – способность терминала менять физическое местонахождение, сохраняя возможность соединения с сетью. В свою очередь мобильность терминала подразделяется на два вида.

- *Дискретная мобильность терминала* (roaming) – изменение физического местонахождения терминала за пределами сеанса связи с сетью.
- *Непрерывная мобильность терминала* (handover) – изменение физического местонахождения терминала в пределах сеанса связи с сетью с потерей или без потери передаваемых данных.

3. Мобильность обслуживания – предоставляет абоненту возможность воспользоваться услугой, на которую он подписался, вне зависимости от местонахождения и типа терминала.

4. Режим виртуальной домашней сети – то же самое, что и мобильность обслуживания, но касается не одной услуги, а пакета услуг. При этом, в зависимости от конкретной услуги, предоставляемой абоненту, в его обслуживание может быть вовлечен только сервер домашней сети или необходимо взаимодействие сервера домашней сети с сервером визитной сети.

Поддержка того или иного типа мобильности зависит, прежде всего, от протокола, который применяется в IP-сети. Далее будут рассмотрены возможности мобильности в сетях IP-телефонии, использующих протоколы IPv4, IPv6 и SIP, а также в сетях стандарта H.323.

Кроме того, доступ к сетям IP-телефонии могут получить и абоненты сотовых сетей. Одной из перспективных технологий, обеспечивающих доступ мобильного абонента сотовой связи к сетям передачи данных, является *система пакетной радиосвязи общего пользования* (GPRS). Эта технология первоначально разработана для стандарта сотовой связи GSM, однако она уже адаптирована для третьего поколения стандартов сотовой связи, например UMTS.

9.2. Идентификация терминала и пользователя

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

Терминал имеет следующие идентификаторы:

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

Полный адрес терминала на транспортном уровне должен содержать IP адрес, тип транспортного протокола, номер порта и тип прикладного протокола. Подробно вопросы идентификации в сетях IP-телефонии на базе различных протоколов рассмотрены в главе 6.

Для определения пользователя используются следующие идентификаторы:

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

Роуминговый идентификатор используется только один раз. Оператор формирует множество роуминговых идентификаторов, которые применяются последовательно. Таким образом, чтобы достичь требуемого абонента, в IP-телефонии используются адреса транспортного уровня и временные идентификаторы.

Ко всем идентификаторам предъявляются особые требования по безопасности, и они не должны передаваться в открытом виде.

9.3. Сценарии мобильности в сетях IP-телефонии

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

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

Функциональные элементы сети IP-телефонии, участвующие при реализации функций мобильности, показаны на рис. 9.1.

В сетях IP-телефонии возможны следующие четыре сценария мобильности.

1. Мобильность между подсетями.
2. Мобильность между зонами обслуживания.
3. Мобильность между подсетями и зонами обслуживания одновременно.
4. Мобильность между подсетями, находящимися в разных зонах обслуживания.

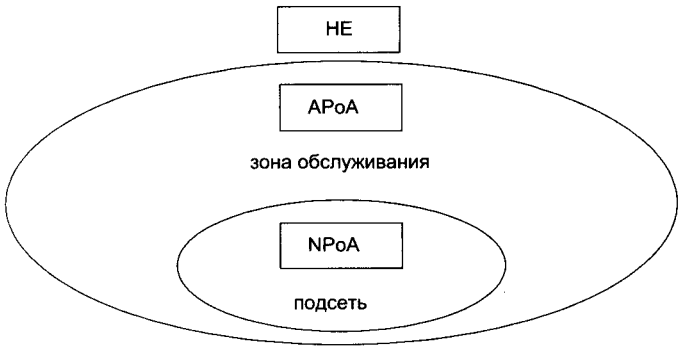


Рис. 9.1. Функциональные элементы, вовлеченные в обслуживание абонента при мобильности

На рис. 9.2-9.5 показаны различные сценарии мобильности абонента в сети IP-телефонии.

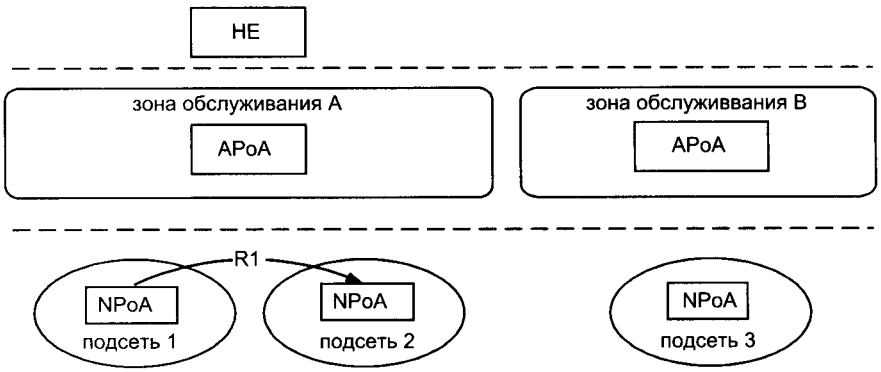


Рис. 9.2. Мобильность между подсетями в пределах одной зоны обслуживания

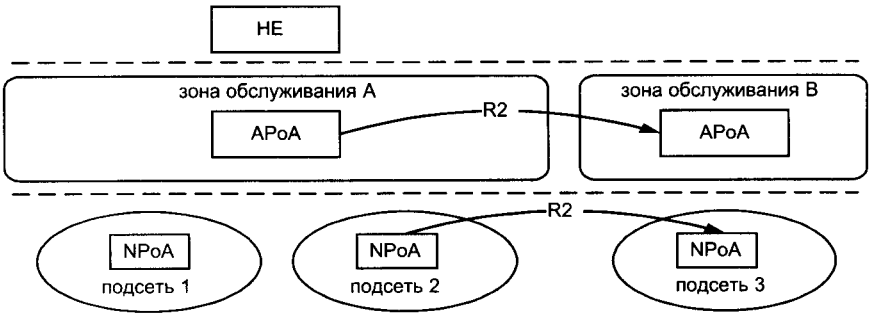


Рис. 9.3. Мобильность между подсетями и между зонами обслуживания одновременно

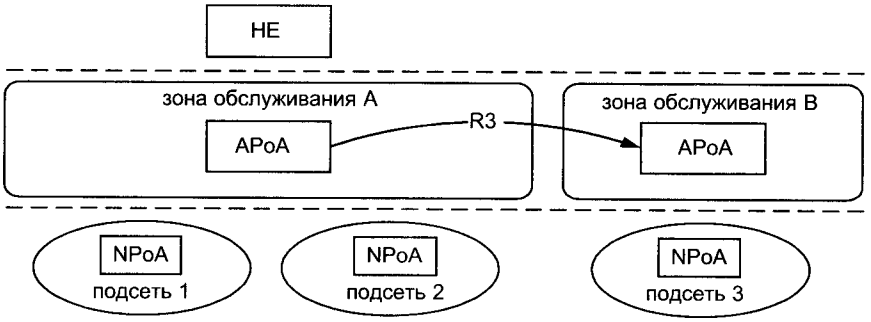


Рис. 9.4. Мобильность между зонами обслуживания

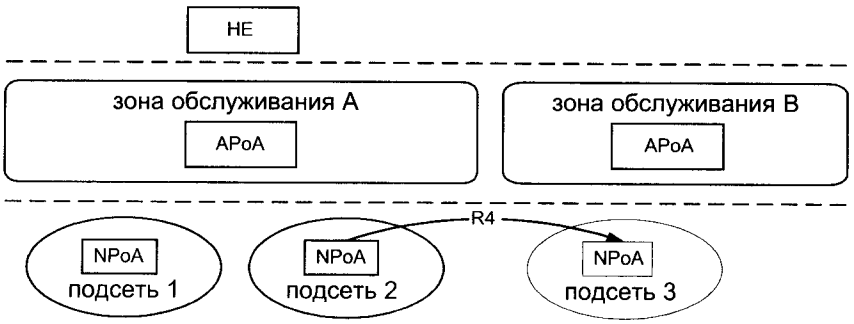


Рис. 9.5. Мобильность между подсетями, находящимися в разных зонах обслуживания

9.4. Мобильность в сети IP-телефонии на базе протокола IPv4

В сетях IP-телефонии, построенных на базе протокола IPv4, терминал перемещается из одной сети в другую не меняя своего IP адреса.

В процедуре мобильности участвуют три компонента: мобильный терминал (MT), домашний регистр и визитный регистр (рис. 9.6).

Мобильный терминал – это терминал, который перемещается из одной сети в другую.

Домашний регистр – это регистр, который хранит всю необходимую информацию о мобильном терминале.

Визитный регистр – это регистр, обслуживающий зону, отличную от зоны домашнего регистра.

Функции домашнего и визитного регистров обычно выполняются маршрутизаторами.

Корреспондентский узел – узел в сети IP-телефонии, обменивающийся данными с мобильным терминалом.

В протоколе IP мобильный терминал может использовать два IP адреса: один для идентификации – домашний адрес (*home address)* и один для маршрутизации – адрес обслуживания (*care-of address).* Существует два типа адреса обслуживания: совмещенный адрес обслуживания (*co-located care-of address)* и адрес обслуживания визитного регистра (*foreign agent*

care-of address). Совмещенный адрес обслуживания представляет собой временный адрес, который присваивается самостоятельно узлом или получается непосредственно из PPP или DHCP сервера. Адрес обслуживания визитного регистра – это адрес регистра, в котором зарегистрирован мобильный терминал. В процедурах регистрации мобильный терминал может использовать совмещенный адрес обслуживания или адрес обслуживания визитного регистра, однако использование совмещенного адреса приводит к уменьшению дефицитных ресурсов, а именно адресов IP, поэтому обычно используется адрес обслуживания визитного регистра.

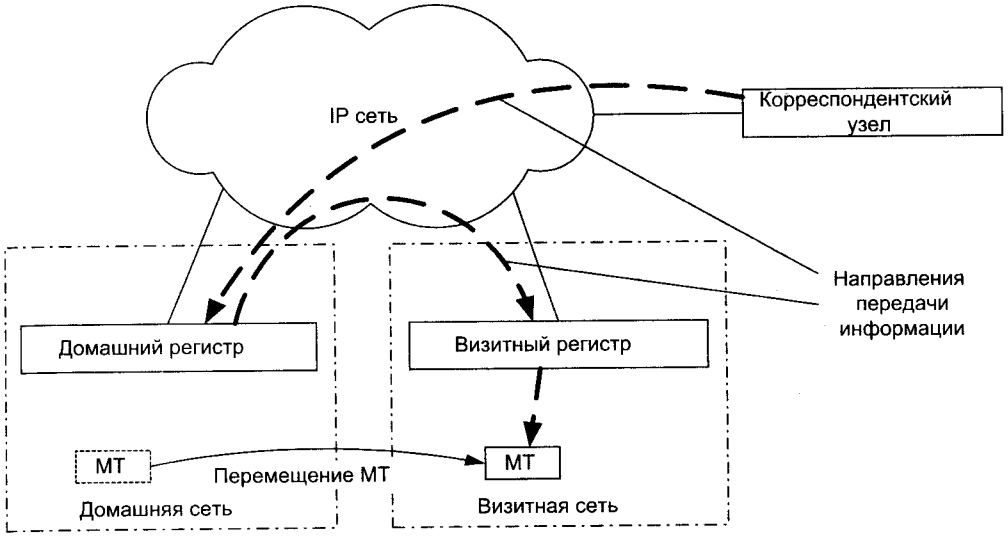


Рис. 9.6. Пример передачи информации для мобильного терминала в сети на базе протокола IPv4

После того как мобильный терминал зарегистрируется в новой сети, он посылает данные об адресе обслуживания домашнему регистру. Домашний регистр обновляет свои таблицы маршрутизации, создает или изменяет уже существующие биллинговые записи и ассоциирует домашний адрес мобильного терминала с его текущим адресом обслуживания.

Когда домашний регистр получает данные, предназначенные для мобильного терминала, он перенаправляет их по адресу обслуживания этого терминала, используя метод инкапсулирования, также известный как метод туннелирования. В обратном направлении мобильный терминал обычно посылает пакеты через маршрутизатор визитной сети. Таким образом, в протоколе IPv4 отсутствует оптимизация маршрута к мобильному терминалу при его роуминге.

В табл. 9.1 приведена характеристика мобильности для протокола IPv4.

9.5. Мобильность в сети IP-телефонии на базе протокола IPv6

В отличие от сетей, построенных на базе протокола IPv4, в сетях на базе протокола IPV6 есть возможность оптимизировать маршрут передачи информации от корреспондент-

ского узла к мобильному терминалу. Корреспондентские узлы, поддерживающие протокол IPv6, способны запоминать связь между домашним адресом мобильного терминала и его адресом обслуживания. В случае передачи информации мобильному терминалу они используют адрес его обслуживания (рис. 9.7).

Таблица 9.1. Характеристика мобильности для протокола IPv4

Критерии		Мобильность IP (v4)
Идентификаторы	пользователей	NAI, домашний адрес IP
	терминала	MAC адрес
	приложений	
	местоположения	адрес обслуживания
Критичные элементы протокола		мобильный терминал, домашний регистр, визитный регистр
Возможность Handover		
Механизм достижения терминала		посылка датаграммы
Индикации состояния		если узел не доступен, то могут быть посланы ICMP сообщения
Дополнительные возможности	QoS	RSVP
	кодек	не применяется
	безопасность	IP Sec
	другое	
Оптимизация маршрута		необязательна, требует поддержки от корреспондентского узла
Мобильность услуг		не применяется

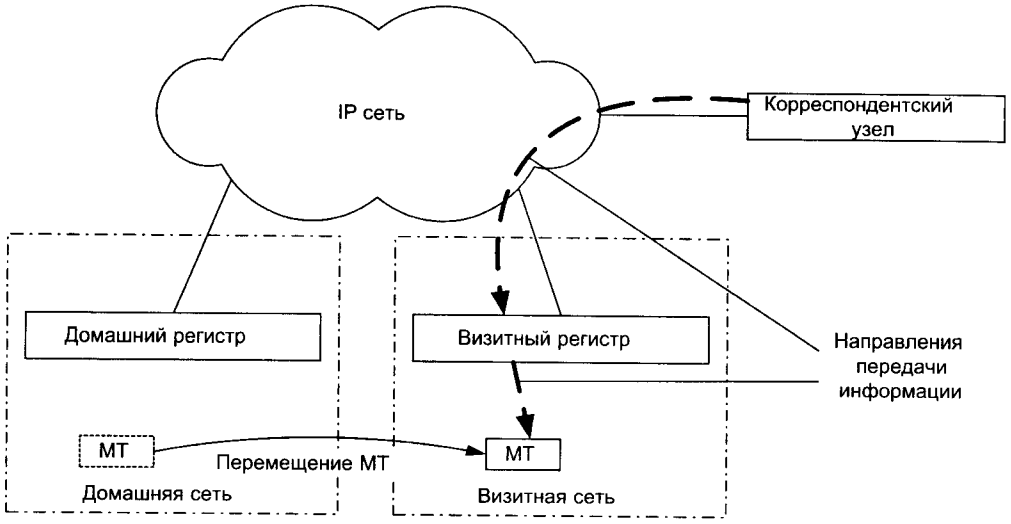


Рис. 9.7. Пример передачи информации для мобильного терминала в сети на базе протокола IPv6

В таблице 9.2. приведена характеристика мобильности для протокола IPv6.

Таблица 9.2. Характеристика мобильности для протокола IPv6

Критерии		Мобильность IP (v6)
Идентификаторы	пользователей	NAI, домашний адрес IP
	терминала	MAC адрес
	приложений	
	местоположения	адрес обслуживания
Критичные элементы протокола		мобильный узел, домашний агент, корреспондентский узел
Возможность Handover		да
Мобильные элементы, вовлеченные в Handover		мобильный узел, корреспондентский узел
Механизм достижения терминала		посылка датаграммы
Индикации состояния		если узел не доступен, то могут быть посланы ICMP сообщения
Дополнительные возможности	QoS	RSVP
	кодек	не применяется
	безопасность	IP Sec
	другое	
Оптимизация маршрута		да
Мобильность услуг		не применяется

9.6. Мобильность в сети IP-телефонии на базе протокола SIP

В настоящее время, в рамках исследований IETF, разрабатываются новые протоколы, которые поддерживают персональную мобильность. Одним из таких протоколов является *протокол инициирования сеанса связи* (SIP). SIP – это прикладной протокол, который может устанавливать сеансы связи мультимедиа или телефонные соединения и управлять ими. Мобильность пользователя в этом протоколе основана на использовании уникального персонального идентификатора.

Пользователь вносится в список сервера-регистратора, после того как он присылает запрос о регистрации. Далее сервер-регистратор сообщает домашнему серверу пользователя, где тот зарегистрирован.

Вызывающий пользователь посылает сообщение-приглашение для вызываемого абонента на ближайший прокси-сервер, который запрашивает у домашнего сервера текущее местоположение вызываемого абонента и, получив необходимую информацию, посылает сообщение-приглашение на сервер-регистратор, в котором зарегистрирован вызываемый пользователь. Вызываемый абонент подтверждает получение сообщения-приглашения, после чего прокси-сервер устанавливает соединение между пользователями.

Протокол SIP не рассматривает мобильность терминального оборудования.

9.7. Реализация функций мобильности в стандарте H.323

Мобильность пользователя IP-телефонии в стандарте H.323 возможна, но до конца не определена. В соответствие с процедурами стандарта сначала устанавливается сигнальное соединение с gatekeeper зоны H.323, следовательно, адрес вызываемого абонента может быть определен перед установлением соединения, а, поэтому, возможно перенаправление с полной обработкой на прикладном уровне.

Современное состояние разработок позволяет говорить о том, что поддержка мобильности возможна и без добавления новых компонентов, и с минимальными модификациями самого стандарта H.323. При этом услуги мобильности IP-телефонии могут быть дополнительным сервисом в существующих, поддерживающих H.323 системах телефонной связи Internet.

В текущей версии H.323 мобильность хост-машин запрещается, исходя из основного механизма IP, который неявно предполагает, что хост-машина стационарна.

9.8. IP-телефония для пользователей сетей сотовой подвижной связи

Для того, чтобы абоненты сотовых сетей могли воспользоваться услугами сетей передачи данных, была разработана новая технология GPRS, которая является составной частью системы GSM, однако может быть адаптирована и под другие технологии.

Инфраструктура сети GSM/GPRS состоит из инфраструктуры сети GSM и двух дополнительных элементов: SGSN (узел, поддерживающий услуги GPRS) и GGSN (узел, выполняющий функции шлюза GPRS).

SGSN выполняет функции управления мобильностью и функции регистрации абонентских данных, включая идентификаторы и местонахождение пользователя.

GGSN – это шлюз между системой GPRS и IP-сетью, который управляет взаимодействием между мобильным пользователем и сетью.

Прежде, чем получить доступ к услугам, мобильный пользователь должен зарегистрироваться в SGSN. При регистрации пользователя SGSN запрашивает его данные из HLR (домашнего регистра) или SGSN, где он был зарегистрирован ранее.

Для передачи или приема информации мобильной станции необходимо активное PDP (Packet Data Protocol) соединение, которым управляет GGSN. При взаимодействии GGSN с мобильной станцией используются PDP адреса.

При обмене информацией, предназначенной для пользователя, между SGSN и GGSN используется GPRS Tunnelling Protocol (GTP).

Кроме того, в стандарте GRPS, как и в GSM, поддерживается идентификация доступности мобильной станции и мобильность обслуживания между сетями, поддерживающими GPRS. Как только мобильная станция перемещается в другую сеть, информация о профиле её обслуживания передается в SGSN визитной сети.

В табл. 9.3 приведена характеристика мобильности для GPRS.

Таблица 9.3. Характеристика мобильности для технологии GPRS

Критерии		Мобильность GPRS
Идентификаторы	пользователей	IMSI
	терминала	IMEI
	приложений	PDP адрес
	местоположения	RAI, Cell ID
Критичные элементы протокола		MS, SGSN, GGSN, HLR (VLR)
Возможность Handover		Да
Мобильные элементы, вовлеченные в Handover		MS, SGSN (VLR)
Индикации состояния		Да
Дополнительные возможности	QoS	PDP
	кодек	
	безопасность	
	другое	
Оптимизация маршрута		Да
Транспортабельность услуг		Да

Глава 10

ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ СЕТЕЙ IP-ТЕЛЕФОНИИ

10.1. Классификация сетей IP-телефонии

Сеть IP-телефонии представляет собой совокупность оконечного оборудования, каналов связи и узлов коммутации. Сети IP-телефонии строятся по тому же принципу, что и сети Интернет. Однако в отличие от сетей Интернет, к сетям IP-телефонии предъявляются особые требования по обеспечению качества передачи речи. Одним из способов уменьшения времени задержки речевых пакетов в узлах коммутации является сокращение количества узлов коммутации, участвующих в соединении. Поэтому при построении крупных транспортных сетей в первую очередь организуется магистраль, которая обеспечивает транзит трафика между отдельными участками сети, а оконечное оборудование (шлюзы) включается в ближайший узел коммутации (рис. 10.1). Оптимизация маршрута позволяет улучшить качество предоставляемых услуг. При подключении к сети других операторов их оборудование также подключается к ближайшему узлу коммутации.

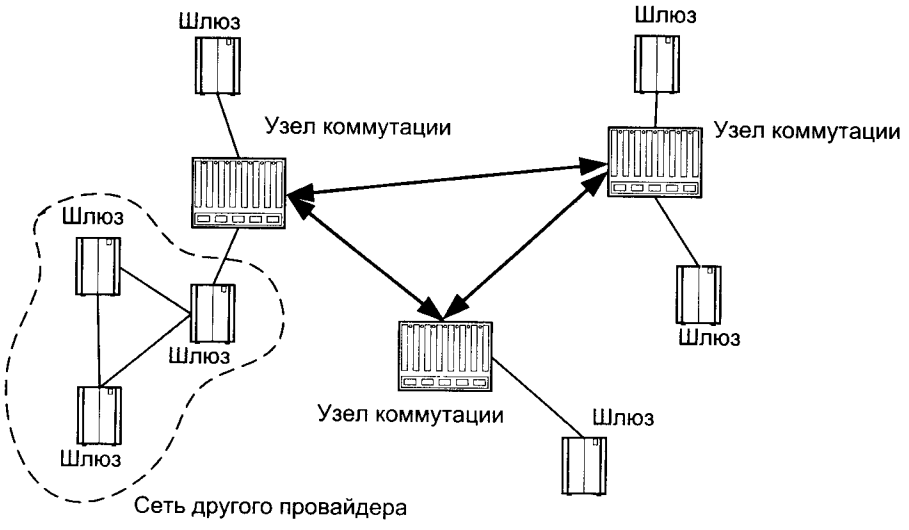


Рис.10.1. Пример построения сети IP-телефонии с использованием магистрали

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

В *выделенных сетях* (рис. 10.2) связь между оконечными устройствами осуществляется по выделенным каналам и пропускная способность этих каналов используются только для передачи речевых пакетов. Чаще всего провайдеры IP-телефонии не строят собственную сетевую инфраструктуру, а арендуют каналы у провайдеров первичной сети. Это позволяет уменьшить затраты на эксплуатацию сети и увеличить окупаемость вложений.

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

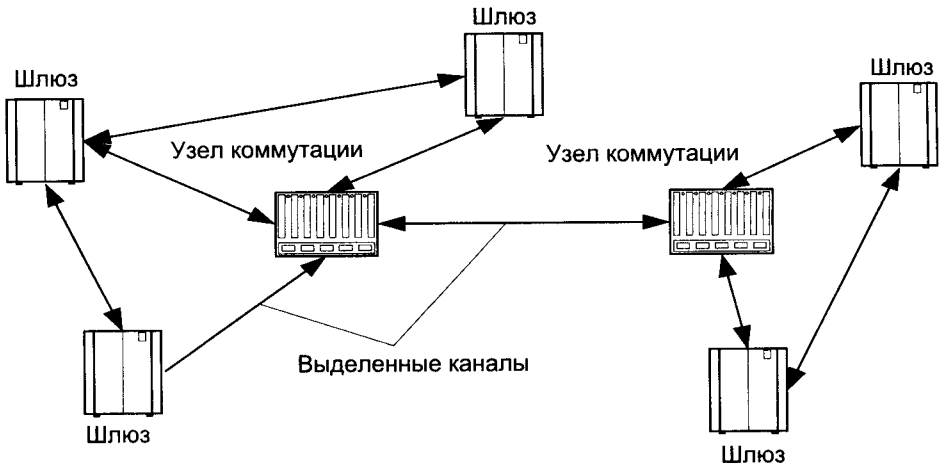


Рис.10.2. Пример построения выделенной сети IP-телефонии

В *интегрированных* сетях IP-телефонии для связи между устройствами используется глобальная сеть Интернет (рис. 10.3). Это может быть уже существующая собственная сеть или доступ к сети Интернет через провайдеров. Если оператор имеет собственную сеть Интернет, то для предоставления услуг IP-телефонии он лишь устанавливает дополнительное оборудование, которое обеспечивает преобразование речи в данные и наоборот, и модернизирует уже имеющееся оборудование, чтобы обеспечить качество предоставляемых услуг. Если оператор IP-телефонии пользуется услугами провайдеров Интернет, то качество услуг такой сети может быть низким, так как обычные сети Интернет не рассчитаны на передачу информации в реальном масштабе времени.

По разным причинам операторы сетей IP-телефонии для объединения своих устройств в сети могут использовать выделенные каналы и сеть Интернет. Такие сети можно назвать сетями *смешанного* типа (рис. 10.4). Вопрос о том, какие каналы использовать для связи устройств между собой, решается оператором индивидуально в зависимости от возможностей.

Если оператор, обычно использующий выделенные каналы, по каким-либо причинам не может арендовать канал до оконечного устройства, он прибегает к услугам провайдеров Интернет. Если оператор IP-телефонии, использующий сеть Интернет, не имеет возможности полу-

чить доступ в Интернет в конкретной точке, или качество услуг через сеть Интернет очень низкое, то для подключения оконечного устройства к сети используется выделенный канал. К построению сети по смешанному типу прибегают редко, только когда нет другого варианта. Чаще всего, таким способом более крупные операторы подключают к себе более мелких операторов.

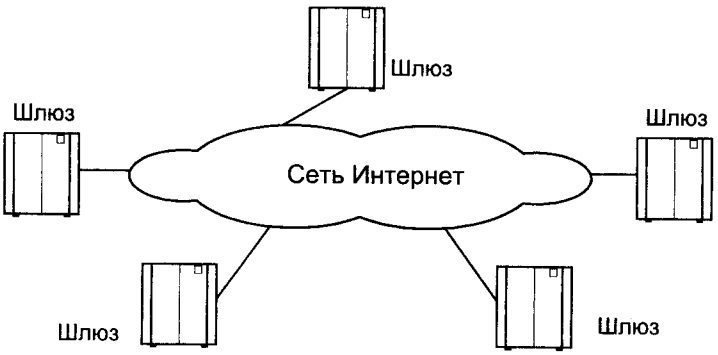


Рис.10.3. Пример построения интегрированной сети IP-телефонии

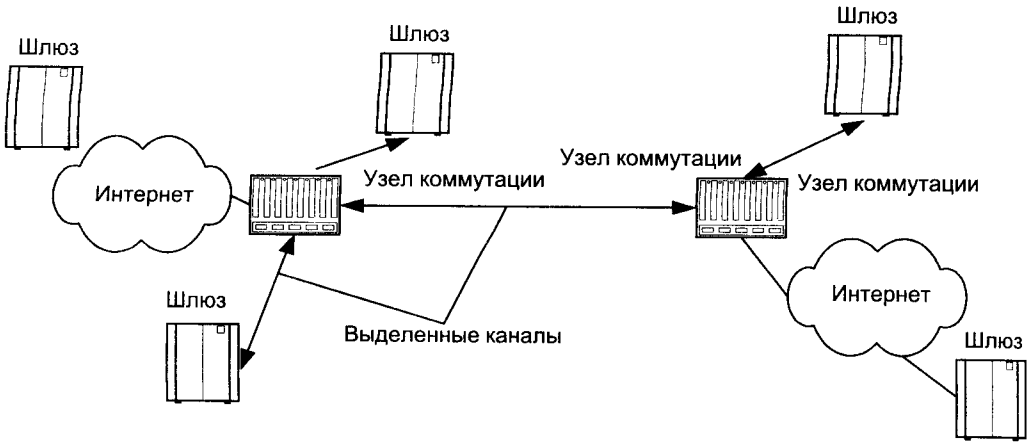


Рис.10.4. Пример построения смешанной сети IP-телефонии

По своему масштабу все сети IP-телефонии можно разделить на *международные, региональные и местные.*

Международная сеть IP-телефонии имеет точки своего присутствия в нескольких странах и обеспечивает терминацию трафика практически в любую точку мира при минимальном использовании телефонной сети общего пользования. Чаще всего, международные сети не работают с конечными пользователями, а предоставляют свою пропускную способность другим сетям. Главной задачей международных сетей является транзит трафика между сетями различного уровня. Кроме того, операторы международной сети организуют международные клиринг-центры, которые упрощают процедуры взаиморасчетов между операторами. При построении международной сети в первую очередь строится мощная магистраль, имеющая большую пропускную способность. Международные сети строятся с использованием выделенных каналов и на базе уже существующих сетей Интернет.

Яркими примерами выделенных международных сетей являются сети компаний ITXC, iBasis и DeltaThree. Среди провайдеров Интернет, предоставляющих услуги международной IP-телефонии, можно отметить компании Carrier1, GRIC, GTE Internetworking и Equant.

В отличие от международной сети *национальная сеть* имеет точки своего присутствия в одной или, в крайнем случае, в нескольких близлежащих странах и обслуживает абонентов и местных операторов только этого региона. С помощью заключения договоренности с международными сетями национальная сеть предоставляет своим абонентам и другим местным сетям возможность терминации вызовов в любую точку мира.

Чаще всего, национальные сети строятся национальными телекоммуникационными компаниями с использованием уже существующей инфраструктуры, поэтому большая часть национальных сетей IP-телефонии являются *интегрированными* сетями. Крупные национальные операторы проводят дооборудование своих сетей передачи данных для предоставления услуг IP-телефонии. Прежде всего, оператор заботится об обеспечении качества передачи речи по сети с помощью модернизации имеющегося оборудования или приобретении нового. Также, в зависимости от имеющегося на сети оборудования, оператор или приобретает дополнительное шлюзовое оборудование, или дооборудует уже используемое на сети оборудование передачи данных функциями шлюза. Примерами телекоммуникационных компаний, имеющих национальную сеть IP-телефонии, могут служить Deutsche Telecom, France Telecom, Telecom Finland, Japan Telecom и многие другие.

Операторы IP-телефонии, не имеющие собственной инфраструктуры, строят свои сети с использованием провайдеров Интернет или провайдеров первичной телекоммуникационной сети и стараются выйти за рамки национальной сети, так как особенно выгодно предоставлять услуги IP-телефонии на большие расстояния. Поэтому операторы, имеющие достаточно средств на строительство сети, предпочитают строить международные сети, причем они располагают точки своего присутствия в тех странах, куда больше всего тяготеет международный телефонный трафик. Примерами национальных выделенных сетей можно считать сети компаний Innofone (Канада) и Liberty One (Австралия, Новая Зеландия).

Местная сеть IP-телефонии предоставляет возможность абонентам местной телефонной сети и частным компаниям воспользоваться услугами IP-телефонии. В основном, операторы местных сетей являются провайдерами доступа к сети IP-телефонии. Чаще всего, их сети имеют всего один шлюз, подключенный к более крупным сетям через сеть Интернет или по выделенным каналам. Таких операторов часто называют перепродавцами, так как они просто перепродают услуги других сетей абонентам местной телефонной сети. Для большинства операторов местная сеть является лишь промежуточным этапом развития и они стремятся выйти на международный или национальный уровень.

10.2. Классификация провайдеров услуг IP-телефонии

При предоставлении услуг в рамках сети IP-телефонии участвует большое количество субъектов, выполняющие различные организационно-технические функции. В рекомендациях TIPHON, разработанных ETSI, определена следующая классификация для субъектов IP-телефонии.

1. Конечный пользователь IP (IPEU) – пользователь, соединенный с IP-сетью.
2. Провайдер доступа IP (IPAP) – компания или организация, предоставляющая доступ к IP-услугам, который может быть или доступом к частной IP-сети, или к сети Интернет.

3. Провайдер IP-сети (IPNP) – компания или организация, которой принадлежит IP-сеть.
4. Провайдер услуг Интернет-телефонии (ITSP) – компания или организация, которая предлагает услуги телефонии через сеть Интернет.
5. Провайдер взаимодействия (ICP) – компания или организация, которая предлагает услуги по взаимодействию между IP-сетями и сетями с коммутацией каналов для телефонного соединения.
6. Провайдер услуг сети с коммутацией каналов (SCNP) – компания или организация, которой принадлежит сеть с коммутацией каналов.
7. Провайдер доступа к сети с коммутацией каналов (SCAP) – компания или организация, которая предоставляет доступ к сети с коммутацией каналов.
8. Конечный пользователь сети с коммутацией каналов (SCEU) – пользователь, соединенный с сетью коммутации каналов.
9. Провайдер информационных услуг (DSP – directory service provider) – провайдер справочной информации, например, предоставляет номер E.164 на основе Email-адреса.
10. Провайдер дополнительных услуг (VASP) – провайдер, который предоставляет дополнительные услуги, помимо услуг традиционной телефонии.
11. Брокер – провайдер делового обслуживания, который обеспечивает возможность межсетевого обмена между провайдерами IP услуг и операторами сетей с коммутацией каналов, включая урегулирование расчетов.

На рис. 10.5 показано взаимодействие некоторых из этих субъектов для базового телефонного соединения между сетью с коммутацией каналов и IP-сетью.

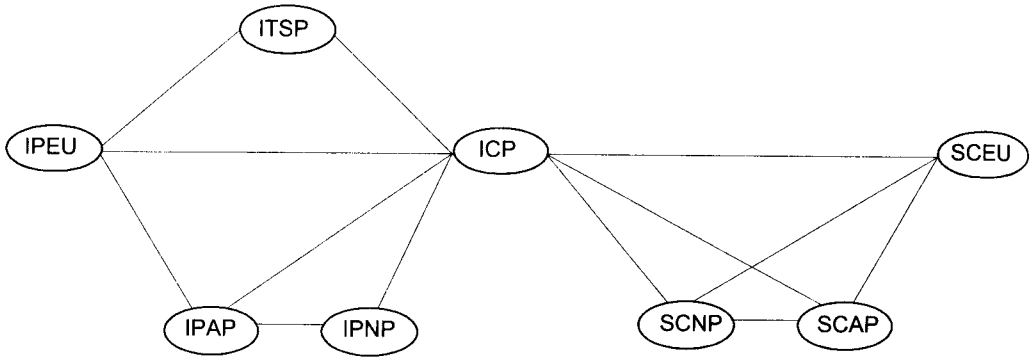


Рис. 10.5. Взаимодействие субъектов сети IP-телефонии при обслуживании телефонного вызова

Ниже приведена классификация бизнес-ролей для провайдеров IP-телефонии, которые вовлечены в обслуживание базового вызова.

1. Локальный оператор IP-телефонии

Локальный оператор действует как провайдер услуг IP-телефонии только внутри своей сети. Для взаимодействия с другими операторами он пользуется услугами сетей с коммутацией каналов.

2. Зональные операторы IP-телефонии (на основе двухсторонних соглашений)

По предварительной договоренности один оператор IP-телефонии может расширить зону своего обслуживания за счет другого оператора. В этом случае, операторы просто разрешают устройствам, принадлежащим разным сетям, взаимодействовать между собой. Такие

операторы для физической связи между устройствами должны использовать общего провайдера IP-сети.

3. Магистральный оператор

Сеть магистрального оператора обеспечивает физические соединения между сетями других операторов IP-телефонии. Магистральный оператор действует как провайдер IP-сети и, потенциально, как провайдер информационных услуг и провайдер дополнительных услуг. Магистральный оператор может также предоставлять услуги авторизации между операторами.

4. Ассоциация операторов

Ассоциация операторов предоставляет операторам возможность расширить зону обслуживания без физического расширения сети. Вступая в ассоциацию, оператор получает доступ к оконечным устройствам, принадлежащим другим членам. Хотя эта бизнес-роль аналогична бизнес-роли брокера (см. п. 5), но членство в ассоциации накладывает на операторов некоторые ограничения. Один оператор, например, может купить права привилегии для некоторой области запроса. Такая закупка запрещает ассоциации поддерживать других операторов в этой области запроса, поэтому все запросы должны направляться только на сеть назначенного оператора.

5. Брокер

Брокер предоставляет услуги по урегулированию взаимодействия между операторами, предлагающими услуги IP-телефонии. Его функции могут быть ограничены только урегулированием расчетов или включать в себя помощь при маршрутизации, урегулирование совместного использования ресурсов, обмен учетными записями и т.д. Воспользовавшись услугами брокера, оператор получает доступ к другим обслуживаемым операторам. Брокер накладывает на операторов меньше ограничений, чем ассоциация, однако его системные службы могут требовать более строгих мер защиты. Примером бизнес-роли брокера является провайдер услуг клиринг-центра (Clearing House Service Provider).

В реальности некоторые операторы могут исполнять несколько бизнес-ролей одновременно. Так, чаще всего, магистральный оператор может играть роль брокера или ассоциации. Это совмещение более привлекательно для локальных операторов, которые стремятся заключать соглашения с крупными альянсами.

Так, в настоящее время на рынке сформировалась определенная иерархия поставщиков услуг IP-телефонии.

1. Компании первого уровня – крупные международные узлы обмена трафиком IP-телефонии, терминирующие вызовы в любую точку мира

2. Компании второго уровня – сети IP-телефонии, которые охватывают нескольких регионов в пределах одного государства, и, как правило, имеют один-два международных выхода на узлы первичных провайдеров для терминации международных вызовов

3. Компании третьего уровня – дилеры, продающие услуги сетей IP-телефонии вторичных компаний в точках присутствия

К компаниям-поставщикам услуг IP-телефонии первого уровня относятся компании ITXC (www.itxc.com), GRIC Communications (www.gric.com), DeltaThree (www.deltathree.com), AT&T Global Clearinghouse (www.ap.att.com), Arbinet (www.arbinet.com), Net2Pnone (www.net2phone.com).

Эти компании позиционируются на рынке следующими особенностями.

- Стремятся к *повсеместному охвату*. Осуществляют терминацию вызовов в любую точку мира. Для тотального охвата компании первого уровня строят широкую партнерскую сеть мирового масштаба в сотрудничестве со вторичными провайдерами ITSP в разных странах мира. Для глобального охвата практикуются гибридные звонки по IP

и традиционным телефонным сетям. Если в вызываемой точке нет совместимого шлюза IP-телефонии, то на узле обмена трафиком IP-телефонии первого уровня, который размещается, как правило, на площадке в США, вызов маршрутизируется из IP в традиционную телефонную сеть, по которой вызов коммутируется до вызываемого абонента. Используется известный факт, что звонки по традиционным телефонным сетям из США в третьи страны дешевле, чем напрямую между этими странами.

- Добиваются *совместимости* шлюзов IP-телефонии основных производителей. Например, компания GRIC оперирует шлюзами Cisco, Lucent и Siemens. Вторичные провайдеры, строящие свои сети на оборудовании данных производителей, могут присоединяться к одному из нескольких узлов обмена трафиком GRIC, расположенных в разных странах мира.
- Осуществляют *сеттлемент и биллинг* вызовов вторичных провайдеров ITSP через свои узлы. Обеспечивают маршрутизацию вызовов по наиболее дешевому маршруту Best Value Routing (BVR), обеспечивают авторизацию, роуминг и биллинг услуг IP-телефонии.
- *Управляют сетью* и контролируют качество обслуживания вызовов на своей сети передачи данных между первичными узлами IP-телефонии, гарантируя качество обслуживания, оговариваемое в договоре со вторичным провайдером IP-телефонии.

К провайдерам IP-телефонии второго уровня можно отнести большинство компаний, предлагающих услуги IP-телефонии на российском рынке (www.comptek.ru/iptelephony/itsp_list). К ним относятся компании MTU-Inform (www.mtu.ru), IncomTel TG (www.incomtel.ru), Elvis Telecom (www.elvis-telecom.ru), Sitek (www.sitek.ru) и другие. Следует выделить сеть TarioNet (www.tario.net) компании Tario Trading, которая одной из первых вышла на российский рынок с услугами IP-телефонии, наиболее широко охватывает российские регионы (более 50 точек присутствия) и имеет собственные выходы на международные узлы IP-телефонии. В мировом масштабе компанию Tario Trading можно отнести ко вторичным поставщикам услуг IP-телефонии, которая строит свою дилерскую сеть TarioNet на территории РФ с наиболее широким охватом регионов.

Сети вторичных провайдеров ITSP по соображениям совместимости и единообразия системы управления строятся на оборудовании одного производителя. По историческим причинам вначале подавляющее большинство ITSP развивали свои сети на шлюзах VocalTec Telephony Gateway (VTG) компании VocalTec – пионера в производстве оборудования для IP-телефонии. В настоящее время на рынке имеется большой выбор шлюзов и специализированного ПО для построения сетей IP-телефонии от разных производителей. Многие компании ITSP, начавшие строить свои сети на VTG, продолжают их развивать на оборудовании других производителей. Например, TarioNet постепенно переходит от шлюзов VTG к шлюзам, разработанным специально для сети TarioNet, на базе платформы DM3 IP-Link известного производителя hardware для предоставления услуг компьютерной телефонии компании Dialogic (с лета 1999 года подразделение корпорации Intel). Продукты компании Dialogic – одни из наиболее популярных для создания платформ IP-телефонии, за счет поставки компанией вместе с hardware набора библиотек с открытым интерфейсом программирования, что позволяет на основе этой базы гибко разрабатывать требуемую систему с учетом потребностей конкретной сети и провайдера ITSP.

Помимо решений VocalTec и Dialogic, среди провайдеров IP-телефонии в настоящее время пользуются популярностью и начинают играть все более ведущую роль решения для предоставления услуг IP-телефонии индустриальных гигантов, прежде всего, компаний Cisco, Lucent и других. Их решения отличаются высокой производительностью и масштаби-

руемостью, позиционируются как решения для крупных провайдеров ITSP, новых New World (решения Cisco) и традиционных Old World (решения Lucent, Nortel, Ericsson, Siemens) операторов связи. Решения последних отличаются возможностью интеграции в существующие у операторов технологические процессы предоставления традиционных телефонных услуг и направлены на создание интегрированных узлов, которые позволят этим операторам осуществить постепенный эволюционный переход к услугам мультисервисных сетей, продолжая оказывать традиционные телефонные услуги.

10.3. Услуги сетей IP-телефонии

Речевые соединения

Сети IP-телефонии любого уровня могут предоставлять конечным пользователям следующие виды речевых соединений:

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

Кроме того, часть сетей IP-телефонии предоставляет услуги по передачи факсов.

Практически все крупные *выделенные сети* предоставляют полный набор услуг своим клиентам. Набор приложений остальных компаний зависит от оборудования, которое используется на их сети, однако большинство провайдеров заявляют о поддержке в будущем всех соединений IP-телефонии.

Конечно же, самой распространенной услугой на выделенных сетях является услуга связи между двумя телефонными аппаратами.

Интегрированные сети, организованные уже существующими провайдерами сети Интернет и работающие на рынке много лет, предоставляют услуги IP-телефонии как дополнительный сервис в своем пакете услуг по передаче данных. В этом случае компания использует собственную сеть, дооборудовав ее и обеспечив необходимое качество передачи речи. Однако на первом этапе провайдеры Интернет для выхода на рынок IP-телефонии предлагают своим клиентам бесплатное программное обеспечение для связи компьютер-компьютер и компьютер-телефон, поэтому эта услуга является самой распространенной для сетей провайдеров Интернет. Например, подобные услуги предоставляют сети компаний DotCom и Net2Phone.

Связь с любой точкой мира

Для конечного пользователя услуга IP-телефонии привлекательна, прежде всего, низкой стоимостью разговора по сравнению с традиционной телефонной связью. Однако, это справедливо только при связи на большие расстояния (для России более 100 км), именно поэтому конечный пользователь заинтересован более всего в междугородной и международной связи через сеть IP-телефонии.

В настоящее время большинство международных операторов IP-телефонии декларируют предоставление связи с любой точкой мира. Эта возможность является основным требованием к провайдерам IP-телефонии. Однако, чтобы реализовать это требование в одиночку, только с использованием собственной сети, операторам IP-телефонии пришлось бы вкладывать огромные средства в развертывание сети по всему миру. Чтобы избежать этого, провайдеры заключают соглашения с другими сетями IP-телефонии.

Если до местной телефонной сети вызываемого абонента нельзя проключить соединение через IP-сети, то провайдеры используют междугородные и международные телефонные сети (рис. 10.6). Это целесообразно в тех случаях, когда строительство шлюза, расположенного в сети вызываемого абонента, невыгодно из-за малого тяготения. Вызовы в эту сеть маршрутизируются на ближайший к месту назначения шлюз, который устанавливает соединение с вызываемым абонентом через телефонные сети различного уровня.

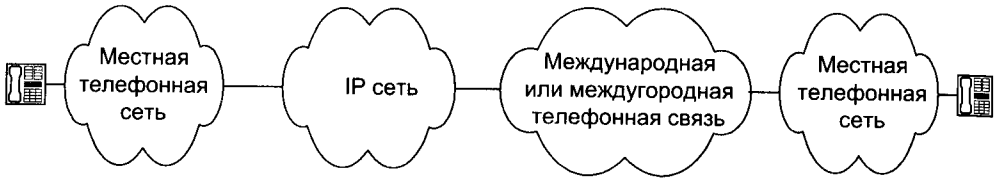


Рис.10.6. Организация связи с удаленным абонентом через телефонную сеть общего пользования

Если провайдер IP-телефонии использует не только местные, но и международные телефонные сети, то это приводит к увеличению себестоимости разговора и, соответственно, к увеличению тарифа на этот разговор, так как оператору приходится оплачивать более дорогие междугородные и международные телефонные соединения. В некоторых случаях стоимость телефонного разговора через сеть Интернет может быть незначительно меньше, чем через традиционную телефонную сеть. Если же качество связи через сеть Интернет-телефонии плохое, то длительность разговора может увеличиться, и стоимость одного и того же разговора через такую сеть может быть даже больше, чем через традиционную телефонную сеть. Поэтому, чем более развита сеть оператора, чем больше у нее заключено соглашений с другими сетями, тем выгодней пользоваться её услугами.

Подвижность (роуминг) пользователя

Одной из перспективных услуг IP-телефонии является роуминг абонента. При этом абонент одной сети может воспользоваться услугами IP-телефонии, находясь в другой сети. Для этого необходимо, чтобы при перемещении пользователя в другую сеть, визитная сеть могла получить данные этого абонента из его домашней сети. Функционирование такой услуги возможно при использовании соответствующей системы биллинга и менеджмента абонентов.

Организация доступа к сети IP-телефонии конечных пользователей

При организации узла IP-телефонии, прежде всего, определяется зона оригинации вызовов, то есть часть телефонной сети, абоненты которой смогут воспользоваться услугами этого узла. Для выхода на сеть IP-телефонии абонент может использовать телефонный аппарат или персональный компьютер.

Для доступа к сети IP-телефонии с телефонного аппарата на местной телефонной сети выделяется номер, по которому абонент может выйти на сеть IP-телефонии с любого телефонного аппарата. Далее, после аутентификации и авторизации, абонент набирает нужный ему телефонный номер.

Пользователь персонального компьютера может получить доступ к сети IP-телефонии, так же как и к сети Интернет, с помощью модема через местную телефонную сеть или по выделенной линии (рис. 10.7).

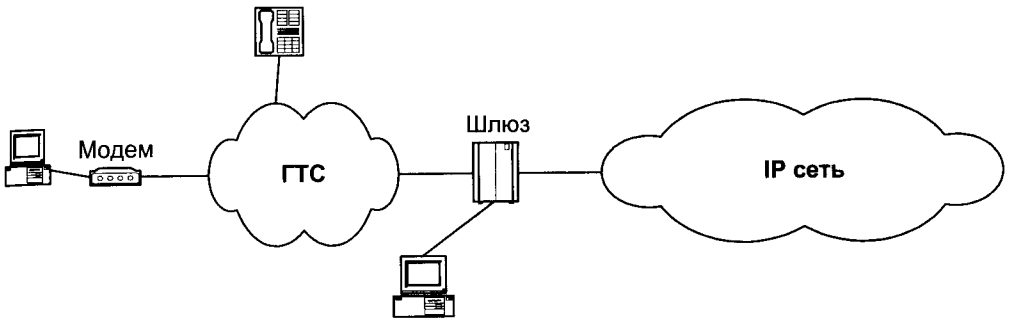


Рис.10.7. Варианты организации доступа конечных пользователей к сети IP-телефонии

Организация доступа к сети IP-телефонии частных сетей

IP-телефония является привлекательным продуктом не только для отдельных пользователей, но и для частных фирм, имеющих собственные телефонные станции. Частная компания может воспользоваться услугами провайдеров IP-телефонии как для ведения международных переговоров, так и для связи между удаленными друг от друга отделениями компании. Возможны два способа организации выхода на сеть IP-телефонии для частной компании.

В первом случае, телефонная станция и шлюз провайдера IP-телефонии соединяются с помощью выделенных каналов (рис. 10.8).

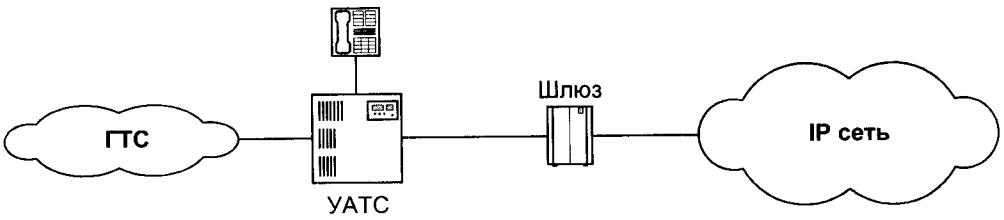


Рис. 10.8. Схема организации доступа частной сети через шлюзовое оборудование провайдера

Во втором случае, если частная телефонная станция может выполнять функции шлюза IP-телефонии, она включается напрямую в сеть провайдера Интернет или в сеть провайдера IP-телефонии (рис. 10.9).

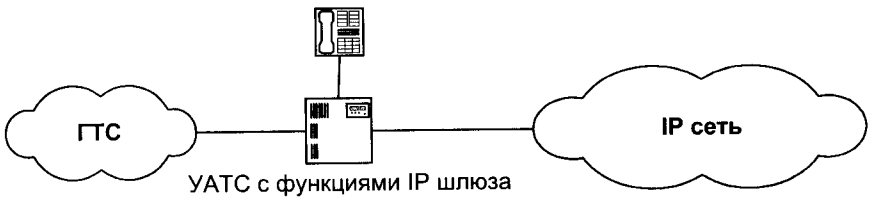


Рис. 10.9. Схема организации доступа частной сети без шлюзового оборудования провайдера.

Организация WEB-поддержки абонента IP-телефонии

Пользователи услуг IP-телефонии, как правило, имеют доступ к системе для получения разнообразной информации (регистрация, изменение профиля услуг, справки о начислениях, оплатах, тарифах, остатке на счете, трафике и др.) через WEB-интерфейс.

Для расчетов с абонентами и другими сетями провайдеру IP-телефонии необходима надежная биллинговая система. Главное отличие биллинговых систем для IP-телефонии – это их работа в реальном масштабе времени. Для простоты и удобства обслуживания абонентов и реселеров, провайдеры IP-телефонии используют, чаще всего, глобальную сеть Интернет. Почти все операторы открывают абонентам и реселерам доступ к их счетам через свой сайт в Интернете. Каждому пользователю выдается свой пароль для доступа, и он в любой момент может проверить состояние своего счета, пополнить его или подписаться на дополнительный сервис.

Реселерские программы

Многие провайдеры для работы с конечными пользователями прибегают к услугам реселеров. Реселерские программы освобождают реселера от необходимости строительства собственной сети передачи данных и дают возможность сосредоточиться только на работе с абонентами, а именно их привлечение и обслуживание. Все заботы о пропуске трафика, качестве предоставляемых услуг, взаиморасчетах и абонентских начислениях берет на себя провайдер услуг. В то же время, сам провайдер снимает с себя необходимость работать непосредственно с абонентами, что сокращает его расходы. С помощью реселеров компании привлекают большее число пользователей и, таким образом, увеличивают свой доход. Некоторые провайдеры вообще не работают с конечным пользователем, возлагая обязанности по привлечению и обслуживанию клиентов на реселеров.

10.4. Принципы тарификации в сетях IP-телефонии

При определение тарифа на вызовы в каком-то направлении оператор IP-телефонии старается получить оптимальную прибыль и привлечь как можно большее число клиентов. Однако есть несколько определяющих моментов в тарифообразовании услуг IP-телефонии.

Для исходящего вызова оператор устанавливает тариф оригинации (Торг.), в котором учитываются затраты оператора на оплату услуг местной телефонной сети и собственные расходы на обслуживание вызова.

Для операторов, пользующихся услугами других сетей, второй составляющей является тариф на услуги транспортных сетей IP-телефонии (Тсет.). Этот тариф устанавливают операторы международных и национальных сетей с учетом всех затрат на обслуживание вызова.

Для входящих вызовов каждый оператор при организации шлюза IP-телефонии определяет географическую область, вызовы в которую будут проходить через этот шлюз (так называемую зону терминации), и определяет тариф терминации (Тер.) на обслуживание этих вызовов. При этом оператор учитывает собственные эксплуатационные расходы и стоимость услуг телефонной сети. Географическая зона обслуживания одного шлюза может быть очень широкой и включать в себя несколько стран. Если область обслуживания одного шлюза состоит из нескольких географических зон с разными тарифами на сети общего пользования, то оператор устанавливает различные тарифы терминации для вызовов в эти зоны, или усредняет эти значения и устанавливает единый тариф терминации для этого шлюза.

Таким образом, тариф на услуги IP-телефонии складывается из тарифа оригинации, сетевого тарифа и тарифа терминации.

Очень большое влияние на величину тарифа услуг IP-телефонии оказывает использование телефонной сети, так как сети IP-телефонии для проключения соединения часто используют не только местные, но и междугородные и международные телефонные сети, где стоимость вызова напрямую зависит от расстояния до абонента. Если сеть провайдера IP-телефонии хорошо развита и имеет большое количество шлюзов в телефонную сеть общего пользования, то стоимость разговора значительно уменьшается за счет сокращения использования каналов сети общего пользования. Так, сеть FREE LINE, имеющая в настоящее время более 12 шлюзов по всему миру, прогнозирует, что развитие этой сети к 2003 году приведет к снижению базового тарифа до 10-15 центов при звонке в любую точку мира. Сейчас тарифы этой компании для вызовов из США достигают 1,30 долл. в минуту.

За рубежом существует несколько крупных провайдеров IP-телефонии, имеющих хорошо развитую сеть шлюзов по всему миру и предоставляющих свои услуги конечным пользователям и провайдерам второго уровня. Сведения о зарубежных провайдерах IP-телефонии приведены в приложении 2.

В табл. 10.1 приведены тарифы на услуги IP-телефонии некоторых крупных операторов IP-телефонии.

Таблица 10.1. Тарифы на услуги IP-телефонии международных операторов

Страна/Сеть	DeltaThree (по всей Европе), $/мин.	DeltaThree (Северная Америка), $/мин.	EUROX (для провайдеров), $/мин.	Inter-Tel, $/мин.	Free Line Network, $/мин.
Франция	0,30	0,13	0,11	0,18	0,3
Англия	0,30	0,14	0,099	0,09	0,3
Израиль	0,18	0,18	0,176	0,24	1,20
США	0,20	0,15	0,108	–	–
Эстония	0,44	0,30	0,292	0,39	0,4
Россия	0,56	0,35	0,299	0,49	0,3
Россия (Москва)	0,23	0,23	0,149	0,49	0,2

Чаще всего, операторы IP-телефонии используют повременную тарификацию вызовов с различной дискретизацией по времени от 1 минуты до 6 секунд. Кроме того, на некоторых сетях предоставляется бесплатное время в начале разговора от 5 до 20 секунд.

Некоторые провайдеры IP-телефонии устанавливают фиксированную абонентскую плату без поминутной тарификации. Например, в сети Access Power установлены два тарифных плана. В одном, ежемесячно с абонента взимается плата в размере 10 долл. в месяц за разговоры только внутри США. В другом, абонентская плата составляет 20 долл. в месяц, но абонент имеет неограниченный доступ в несколько стран Европы и Северной Америки.

Как и на телефонной сети общего пользования, нагрузка на сети IP-телефонии неравномерна по времени, поэтому операторами IP-телефонии используется льготная тарификация по времени суток и по дням недели. Например, одна из российских компаний TarioNet имеет «дневной тариф» (08.00-22.00), «ночной тариф» (22.00-08.00), «льготный ночной тариф» (01.00-05.00) и «тариф выходного дня». При такой тарификации одна минута разговора с США по «ночному тарифу» (22.00-08.00) составляет 7,30 руб., а по «льготному ночному тарифу» (01.00-05.00) и «тарифу выходного дня» всего 5,50 руб. При том, что в рабочее время стоимость одной минуты разговора с США составляет 12,50 руб.

10.5. Организация расчетов в сетях IP-телефонии

Тарифная политика и принципы расчета с абонентами определяются каждым оператором IP-телефонии самостоятельно, исходя из условий его работы, технических и организационных возможностей и взаимоотношений с другими провайдерами IP-телефонии.

Чаще всего, для расчетов с абонентами провайдеры IP-телефонии используют метод предоплаты и предоплаченные карты. В этом случае сводится к минимуму риск неплатежей. Для реализации таких методов расчетов за услуги IP-телефонии необходима соответствующая биллинговая система, способная отслеживать работу абонентов и проводить тарификацию в реальном масштабе времени.

При использовании метода **предоплаты** между компанией и абонентом заключается договор на обслуживание. Абонент вносит определенную оператором сумму на свой счет в компании и получает пароль доступа к услугам. В дальнейшем с этого счета списываются соответствующие суммы, пока баланс счета не станет равен нулю. После этого обслуживание абонента прекращается. Абонент может пополнить свой счет и продолжить работу.

Более перспективным методом расчета с абонентами является использование предоплаченных сервисных карт. В этом случае, у абонента нет необходимости заключать договор с компанией. Достаточно просто приобрести предоплаченную сервисную карту компании определенного номинала. На этой карте уже имеется код доступа, закрытый защитным слоем, и инструкция по пользованию картой. При использовании сервисных карт значительно упрощается схема обслуживания абонентов, так как отпадает необходимость генерации счетов.

Номинал карт устанавливается оператором. Обычно операторы используют сервисные карты трех-четырех различных номиналов. За рубежом, чаще всего, используют карты номиналом 25 долл., 50 долл. и 100 долл., а в России используются карты номиналом 500 и 1000 руб. Целесообразно установить такой номинал карт, чтобы абонент имел возможность сделать 50-100 вызовов, используя эту карту.

При использовании **предоплаченных карт** необходимо иметь разветвленную сеть распространения этих карт среди абонентов. Оплата услуг распространителей карт и стоимость производства карт не должна входить в номинал карт и должна оплачиваться из доходов оператора.

Одним из преимуществ предоплаченных карт является возможность их роуминга, то есть использование одной и той же карты в различных городах и даже странах, где есть представительство этого оператора. При этом биллинговая система должна поддерживать функцию роуминга и тарификацию в реальном масштабе времени.

При обслуживании корпоративных клиентов возможен расчет по факту предоставления услуг.

10.6. Особенности организации взаиморасчетов в сетях IP-телефонии

Взаиморасчеты в телефонных сетях общего пользования

Модель взаиморасчетов в традиционной телефонной сети общего пользования показана на рис. 10.10. Эта модель начинается на вызывающей стороне, которая оплачивает вызов, направляемый в вызываемую сторону. Оператор исходящей сети взаимодействует с другими сетями для обеспечения доступа к сети назначения. Данная модель основывается на компен-

сации затрат каждому сетевому оператору на передачу вызова через его сеть. Для обеспечения компенсации друг другу затрат за пропуск трафика сетевые операторы заключают между собой двухсторонние соглашения. Эти соглашения определяют, как две сети физически соединяются на сетевом уровне, а также как сети взаимодействуют на уровне взаиморасчетов. Например, какую цену сетевой оператор будет платить другому сетевому оператору для завершения его телефонных вызовов.

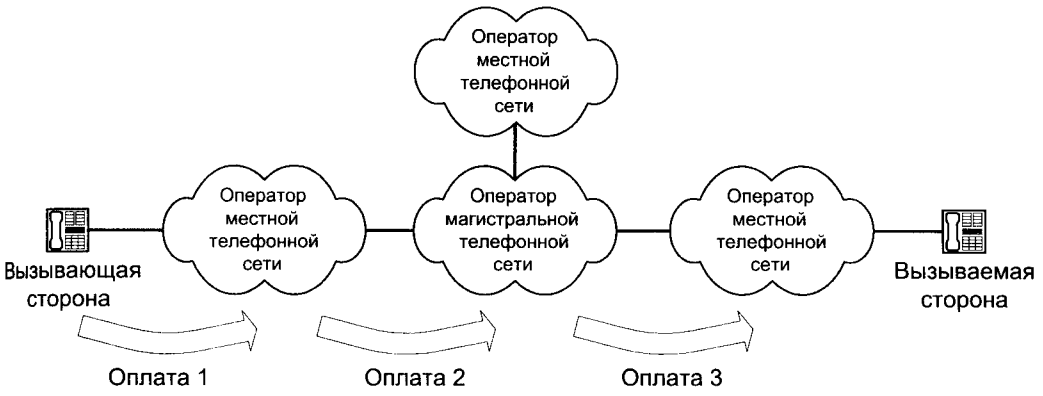


Рис. 10.10. Взаиморасчеты в телефонных сетях общего пользования

Два взаимодействующих сетевых оператора периодически определяют, какой трафик они передали и приняли друг от друга. Трафик, которым обмениваются две сети, позволяет определить потоки «чистого» оплачиваемого трафика. Величина этого оплачиваемого трафика умножается на единицу оплаты взаимодействия. В результате получается «чистая» оплата от исходящей сети к сети назначения.

В модели взаиморасчетов для телефонных сетей сетевое и финансовое взаимодействие происходит между смежными сетями. При этом обеспечивается высокая сетевая безопасность, связанная с обменом трафиком, так как сети имеют прямое соединение между парами коммутационных узлов. Здесь отсутствует риск несанкционированного соединения, так как каждый оператор имеет полный контроль за подключенной группой каналов и детальные сообщения о вызовах (CDRs) генерирует его коммутационный узел.

Взаиморасчеты в сети Интернет

Модель взаиморасчетов в сети Интернет отличается от модели для телефонной сети двумя положениями. Во-первых, в модели взаиморасчетов для телефонной сети продаваемые ресурсы сети оплачиваются в зависимости от степени их использования. В модели взаиморасчетов Интернет пользователи и провайдеры оплачивают доступ к сетевым ресурсам. В случае простой схемы оплаты доступа, плата за взаимодействие основывается на ширине полосы канала, используемого для физического соединения сетей. Например, подключение через канал E1 (доступ на скорости 2 Мбит/с) имеет фиксированную стоимость в месяц независимо от трафика голоса и данных, передаваемого между сетями.

Во-вторых, в модели для телефонной сети весь годовой доход, получаемый от предоставленных услуг, образуется на исходящей стороне. В модели Интернет доход делится между исходящей сетью и сетью назначения. Как показано на рис. 10.11, сторона пользователя

Интернет (аналогичная исходящей стороне) платит своему провайдеру услуг Интернет (ISP) за доступ в сеть Интернет. Сторона WEB-хоста (аналогичная входящей стороне) платит своему Интернет-провайдеру за обеспечение доступа к его сайту всех пользователей сети Интернет. В свою очередь, оба провайдера услуг Интернет платят определенную плату оператору IP-сети для доступа в Интернет.

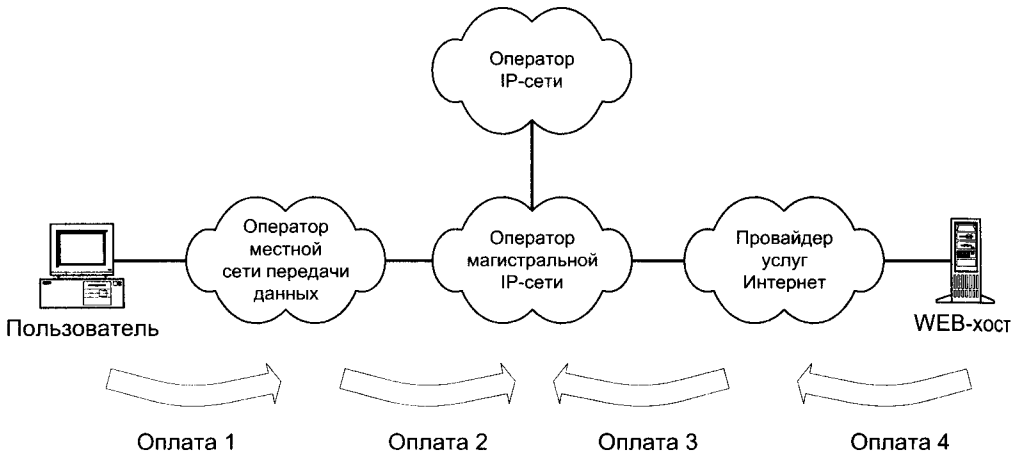


Рис. 10.11. Взаиморасчеты в сети Интернет

Взаиморасчеты при предоставлении услуг IP-телефонии

В модели IP-телефонии стоимость минуты разговора определяется удельной средней величиной всех затрат, включая фиксированные затраты (например, стоимость оборудования шлюзов, программного обеспечения биллинга и др.) и переменные затраты (например, стоимость полосы пропускания, выполнение функций терминации и др.). Тарифные доходы определяются как совокупность расчетных затрат и заданной величины прибыли.

Модель взаимодействия при Интернет-телефонии является комбинацией моделей телефонной сети и сети Интернет. На сетевом уровне взаимодействие между IP-сетями подобно модели взаимодействия Интернет. Операторы местных IP-сетей платят за доступ оператору магистральной IP-сети. Как показано на рис. 10.12, шлюзы IP-телефонии размещаются на границе сети IP-телефонии. Эти шлюзы преобразуют телефонные вызовы в IP-пакеты для передачи их через IP-сеть. Исходящий шлюз преобразует вызов в поток разговорных IP-пакетов и передает через IP-сеть к входящему шлюзу. Входящий шлюз принимает разговорные IP-пакеты и направляет вызов к входящему абоненту. Таким образом, весь сегмент передачи голоса по IP-сети становится прозрачным для вызывающей и вызываемой сторон.

Подобно модели взаимодействия в телефонной сети, все доходы собираются на исходящей стороне. Так же, как и при традиционной телефонии, операторы сетей не будут обслуживать вызовы в интересах других фирм, пока не получат компенсацию за использование ресурсов их сетей. Модель взаимодействия Интернет гарантирует, что оператор магистральной IP-сети получит компенсацию за пропуск IP-трафика от оператора исходящей местной сети. Однако модель Интернет не обеспечивает возможность исходящему оператору IP-телефонии оплатить входящему оператору прием голосовых IP-пакетов и завершение телефонных вызовов.

Рис. 10.12. Взаиморасчеты в сети IP-телефонии

Представление услуг IP-телефонии требует разработки новой модели распределения доходов. Сети, которые не взаимодействуют непосредственно, должны получать компенсацию в соответствии с их ролью по инициации и терминации вызовов. Эта новая модель имеет две основные проблемы. Первая проблема касается организации реального бизнеса. В настоящее время в мире существует множество IP-сетей, которые не соединены, и для их взаимодействия число взаимных соглашений между операторами или провайдерами должно быть равно $n\times(n-1)/2$, где n – число операторов. Заключение и реализация тысяч взаимных соглашений практически невозможна.

Вторая проблема является технической. Услуги, требующие расчетных операции между двумя операторами, которые не связаны непосредственно, должны быть безопасно авторизованы и тарифицированы. Процесс авторизации и тарификации этих услуг в реальном времени является предметом электронной коммерции. Для решения данных проблем должны использоваться соответствующие системы биллинга и клиринга услуг Интернет-телефонии.

В настоящее время практически не существует провайдеров, которые предоставляют услуги связи только внутри своей сети. Большинство провайдеров стремится расширить свои возможности, заключая соглашения с другими провайдерами. Если два провайдера заключают соглашения между собой, то им необходима надежная система взаиморасчетов.

Если провайдеров несколько, то система взаиморасчетов между ними существенно усложняется. Большинство провайдеров, владельцев международных или национальных сетей, предлагают клиринговые программы взаиморасчетов, позволяющие провайдерам, заключившим соглашения с этой сетью, упростить систему взаиморасчетов и уменьшить риск неплатежей. Это такие крупные компании, как AT&T, GRIC, iBasis и многие другие.

Например, если имеется двенадцать провайдеров IP-телефонии, то в соответствии с приведенной выше формулой коммерческая взаимосвязь через двухсторонние соглашения требует заключения 66 индивидуальных соглашений взаимосвязи (рис. 10.13). При использовании для взаиморасчетов между провайдерами клиринг-центра третьего лица общее количество соглашений взаимосвязи будет уменьшено до двенадцати. То есть каждый провайдер IP-телефонии поддерживает только одно соглашение взаимосвязи с клиринг-центром третьего лица вместо поддержания множественных соглашений взаимосвязи с каждым ITSP.

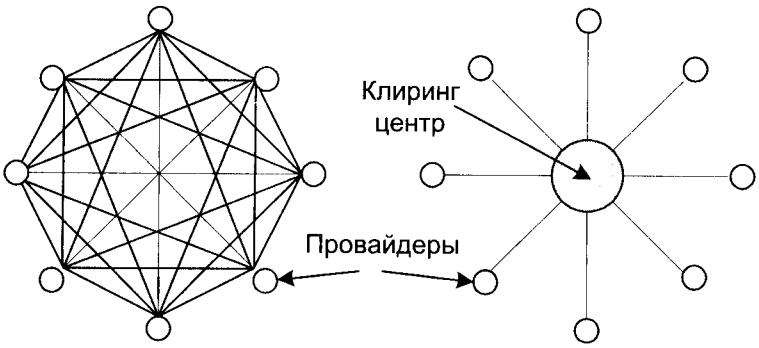


Рис. 10.13. Организация взаиморасчетов без и с использованием клиринг-центра

При заключении взаимных соглашений провайдеры договариваются о стоимости расходов на обслуживание взаимодействия (установленные платы, аудит, биллинг, кредитный риск). В предположении, что средняя стоимость одного соглашения взаимосвязи равна 10000 долл. в год, практика показывает, что экономия общей стоимости при использовании для взаиморасчетов клиринг-центра может быть очень большой с увеличением числа взаимодействующих сетей.

Тарифные доходы клиринг-центра определяются стоимостью расчета одной минуты трафика, создаваемого провайдерами услуг IP-телефонии, пользующихся услугами клиринг-центра. Существующие за рубежом клиринг-центры используют тарифы за расчет каждой минуты трафика в зависимости от стоимости этой минуты. Например, стоимость расчетов в клиринг-центре Arbinet Global Clearing Network приведена в табл. 10.2. Анализ данных таблицы показывает, что в среднем стоимость расчетов каждой минуты разговора IP-телефонии в клиринг-центре составляет порядка 6% от стоимости минуты разговора.

Таблица 10.2. Тарифы клиринг-центра Arbinet Global Clearing Network

Стоимость расчета одной минуты трафика в клиринг-центре, долл.	Тариф одной минуты трафика, установленный провайдерами услуг IP-телефонии, долл	Доля стоимости расчета одной минуты трафика от тарифа за минуту разговора IP-телефонии
0,00375	0,0499 и меньше	7,5% и более
0,00425	от 0,0500 до 0,0999	от 4,2% до 8,5%
0,00475	0,1 и более	4,75% и менее

Глава 11

ВНЕДРЕНИЕ УСЛУГ IP-ТЕЛЕФОНИИ ЗА РУБЕЖОМ И В РОССИИ

11.1. Состояние и прогноз рынка услуг IP-телефонии

В настоящее время IP-телефония получила достаточно широкое распространение в странах Европы, Америки и Азии (рис. 11.1). Сведения о некоторых зарубежных провайдерах IP-телефонии приведены в приложении 1. Несмотря на свой небольшой возраст IP-телефония занимает прочное место в телекоммуникационной индустрии многих стран. Прежде всего, этому способствует глубокая интеграция мировой экономики. Многие компании и предприятия как крупные, так и мелкие имеют представительства в разных странах мира. Таким компаниям приходится тратить большие средства на междугородные и международные переговоры. Поэтому IP-телефония, позволяющая тратить на это меньше на 70%, была сразу же востребована потребителем. Многие крупные компании используют свои собственные сети передачи данных для организации международных IP-телефонных разговоров между офисами в разных странах. Другие компании, не имеющие средств и возможности для организации частной сети, пользуются услугами компаний-провайдеров IP-телефонии.

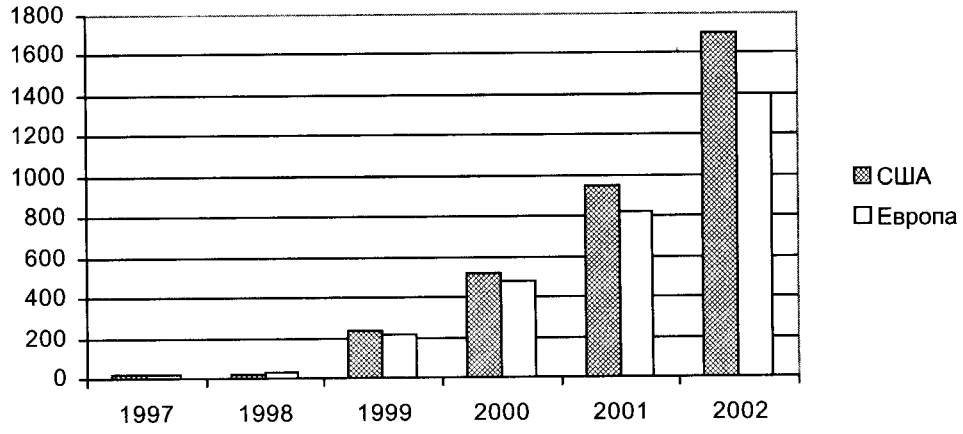


Рис. 11.1. Доходы от IP-телефонии в США и Европе, млн. долл. (по данным Datamonitor)

Учредителями компаний IP-телефонии являются различные международные и национальные организации. Активную роль в развитии сетей IP-телефонии играют крупные телекоммуникационные компании. Так, американская корпорация AT&T не только сама предоставляет услуги IP-телефонии, но и инвестирует очень крупную сеть провайдера IP телефонии ITXC. Компания GTE учредила дочернюю компанию GTE Internetworking, которая предоставляет пакет услуг Интернет, в том числе Интернет-телефонию. Предприятие DeltaThree является дочерней компанией RSL Communications.

Производители оборудования также участвуют в создании сетей Интернет телефонии. Например, компания Franklin Telecom является учредителем сети Fnet, а компания VocalTec инвестирует сети Vocaltec и ITXC.

Рынок IP-телефонии отличается своей пестротой и разнообразием, однако, все компании, занимающиеся предоставлением услуг передачи речи через глобальные сети с пакетной коммутацией, можно разделить на три основных типа.

1. Телекоммуникационные компании.

Эти компании на базе уже имеющейся телекоммуникационной инфраструктуры строят свою сеть передачи данных (если ее не было) и предоставляют услуги IP-телефонии в общем пакете услуг Интернет.

2. Провайдеры услуг Интернет (ISP).

С помощью дооборудования уже существующей сети шлюзами, провайдеры услуг Интернет предоставляют своим пользователям услуги IP-телефонии как часть услуг Интернет. Кроме того, такие компании вообще могут не дооборудовать свою сеть, а предоставлять лишь услуги по транзиту трафика IP-телефонии другим операторам.

3. Провайдеры услуг Интернет-телефонии (ITSP).

Это новые компании на рынке телекоммуникации. Сети таких операторов ориентированы только на передачу речи по сети передачи данных и гарантируют высокое качество своих услуг. Кроме передачи речи, некоторые провайдеры услуг Интернет-телефонии предоставляют услуги по передачи факсов через свою сеть.

11.2. Практика предоставления услуг IP-телефонии за рубежом

IP-телефония сегодня используется, прежде всего, в качестве альтернативы международной и междугородной связи, с экономией на тарифах за счет пропуска трафика по IP или Интернет-каналам, независящим от расстояния. Эта возможность достижения результата с минимальными затратами делает сегмент международной и междугородной связи очень привлекательным для получения высокой прибыли и быстрой окупаемости вложений за счет внедрения услуг IP-телефонии региональными операторами связи.

Следует отметить, что IP-телефония является не только лишь средством извлечения сиюминутной прибыли, а имеет более широкое применение и, следовательно, больший потенциал, чем приложение, имеющее нишу. Эквивалентная ТфОП технология IP-телефонии обеспечивает экономию средств и широкий набор новых услуг. Это позволяет операторам связи соответствовать потребностям существующего рынка и открывать новые возможности.

В качестве иллюстрации далее описан опыт двух западных компаний, одна из которых предоставляет услуги IP-телефонии на мировом уровне через сеть Интернет, а вторая – в пределах одной страны на базе общенациональной сети ATM.

Опыт корпорации ITXC (США)

Корпорация ITXC Corp. (Internet Telephony eXchange Carrier) основана в 1997 году на средства, полученные от компаний AT&T и VocalTec. Согласно данным Telegeography, корпорация ITXC владеет приблизительно 13% международного рынка VoIP. Компания ориентирована на оптовое предоставление услуг Интернет-телефонии международным, национальным и крупным местным провайдерам IP-телефонии.

Сеть корпорации ITXC имеет узлы коммутации в Нью-Йорке и Лос-Анджелесе, причем за время работы сети их производственные мощности были удвоены. В ближайшее время планируется построить еще два узла коммутации в Нью-Джерси и Лондоне. Корпорация обладает одной из самых больших глобальных сетей для передачи голоса через сеть Интернет. Сеть ITXC имеет более 330 точек присутствия, расположенных в 195 городах в 78 странах. С сетью ITXC.net соединены сети компаний: Ameritech, Bell Atlantic, China Telecom, Japan Telecom, Korea Telecom.

В сети ITXC используется оборудование фирм Cisco, VocalTec и Lucent.

Работу сети 24 часа в сутки контролирует центр мониторинга сети (NOC). Для обеспечения качества предоставляемых услуг связи ITXC использует продукт под названием BestValue Routing. Если на каком-либо направлении возникают перегрузки, то трафик немедленно перемаршрутизируется. В качестве резервного маршрута могут использоваться частные сети, например, Above Net и Digital Island, или телефонные сети общего пользования.

В табл. 11.1 приведены основные показатели финансовой деятельности компании ITXC за два года работы на рынке услуг IP-телефонии .

Таблица 11.1. Показатели финансовой деятельности компании ITXC

Финансовые показатели (долл.) и нагрузка в сети (мин.)	За 9-ти месячный период, закончившийся 30 сентября		За 3-х месячный период, закончившийся 30 сентября	
	1998 г.	1999 г.	1998 г.	1999 г.
Доход от IP-телефонии	268850	13313678	222528	6549249
Консалтинговый доход	564708	988232	88236	-
Совокупный доход	833558	14301910	310764	6549249
Амортизация и погашение долгов	157556	1353621	105987	654551
Безналичная компенсация служащим	124993	1753965	57453	1066373
Общие расходы и затраты	5188195	28110339	2664065	12875815
Чистый убыток	4312694	13615597	2253784	6289247
Нагрузка	700000	78000000	643700	42500000

Необходимо отметить, что фактически развертывание деятельности компании на рынке IP-телефонии началось в мае 1998 года, поэтому данные за 9 месяцев 1998 года не являются полными. По данным за трехмесячный период 1998 и 1999 годов можно судить о том, что компания вкладывает огромные средства в развитие своей сети. При этом для развития сети используются полученная от услуг IP-телефонии прибыль и инвестиции таких крупных компаний, как Chase Capital, Flatiron Partners, Intel, Spectrum Equity, Polaris и VocalTec Communications.

На рис. 11.2 показано соотношение доходов и расходов компании за два трехмесячных периода в 1998 и 1999 годах. Из приведенной диаграммы видно, что при увеличении расходов компании в 6 раз доходы от предоставления услуг IP-телефонии увеличились более чем в 20 раз. Каждая обслуженная минута разговора принесла компании прибыль порядка 0,2 долл.

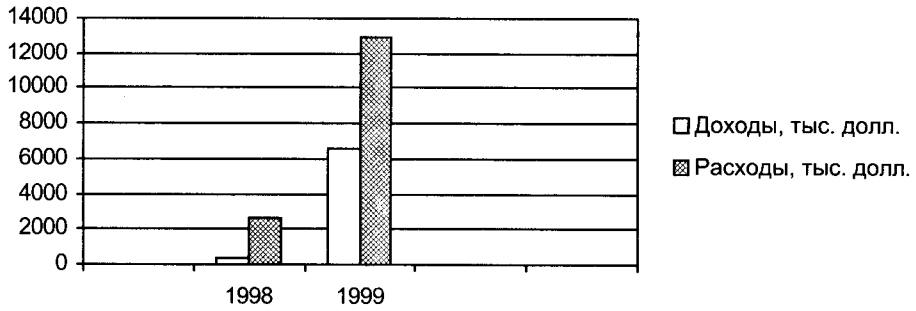


Рис. 11.2. Показатели финансовой деятельности компании ITXC

Опыт компании Telecom Finland

Компания Telecom Finland (Финляндия) внедрила услугу Neophone, в основе которой – передача голосового трафика через сеть передачи данных. Telecom Finland является оператором общенациональной сети ATM, и это решает проблему выделения нужной полосы пропускания. Что же касается взаимоотношений с ТфОП, то, во-первых, Telecom Finland сама является оператором телефонной сети, а во-вторых, услуга Neophone позиционируется не как возможность сэкономить на звонках, а как способ, позволяющий привнести дополнительный интеллект в корпоративную телефонную систему, снабдить ее удобным пользовательским интерфейсом и упростить подключение большой организации к телефонной сети.

Схема технического обеспечения услуги представлена на рис. 11.3.

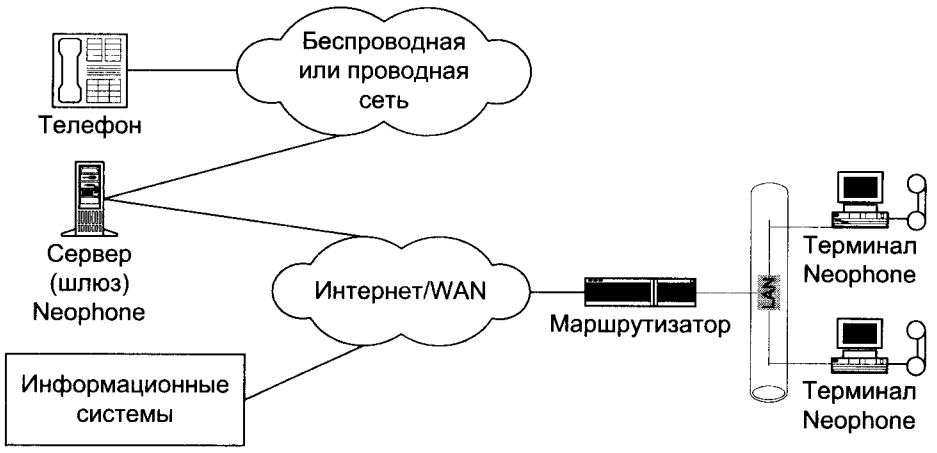


Рис. 11.3. Схема передачи телефонного вызова в рамках услуги Neophone компании Telecom Finland

Пользователем Neophone всегда является организация. Вместо телефонных аппаратов на рабочих местах компании-пользователя устанавливаются мультимедийные персональные компьютеры. Благодаря Neophone сотрудник может работать со своим компьютером, как с телефонным аппаратом.

Голосовой вызов вначале передается по локальной сети организации под IP. Затем он попадает (через маршрутизатор) в глобальную сеть, по которой голосовой трафик передается на установленный на территории Telecom Finland компьютерно-телефонный шлюз, осуществляющий обмен с коммутируемой телефонной сетью. По ней вызов передается на телефонный аппарат абонента. Шлюзом между сетью ATM и телефонной сетью является оборудование от компании Ericsson, а для локальной сети организации-клиента используется компьютерно-телефонное программное обеспечение фирмы Vocaltec.

Каждой из рабочих станций, включенных в локальную сеть, присваивается телефонный номер. Набрав его, абонент с любого телефона (стационарного или мобильного) может получить соединение с сотрудником организации. При этом, абонент даже не заметит, что его вызов на самом деле передается через сеть с коммутацией пакетов.

Обязательным условием для работы с Neophone является подключение клиента к сети ATM. В противном случае невозможно гарантировать качественную передачу голосового трафика. Под голосовой трафик отводится выделенный канал, связывающий корпоративную сеть с компьютерно-телефонным сервером.

Использование Neophone позволяет организации-клиенту отказаться от установки дорогостоящей офисной АТС; отпадает также необходимость в поддержке отдельных компьютерной и телефонной сетей. Кроме того, становится возможным привнесение компьютерного интеллекта в телефонную связь организации. Конечно, современные офисные АТС обладают весьма внушительными возможностями, однако в отношении удобства пользовательского интерфейса они сильно проигрывают компьютерам.

Клиентское программное обеспечение, поддерживающее Neophone, имеет удобный графический интерфейс пользователя. В частности, он позволяет создавать «телефонные справочники». Чтобы набрать номер абонента, занесенного в такой справочник, пользователю достаточно щелкнуть мышью на соответствующей фамилии.

Neophone предоставляет сотрудникам компании большое количество дополнительных интеллектуальных услуг. Например, имеется возможность переадресации вызова на другого сотрудника компании или на другой телефонный номер (на тот случай, если сотрудник компании должен временно отлучиться). Кроме того, сотрудник компании может войти в систему в удаленном режиме и после этого принимать вызовы на свой мультимедийный компьютер, находящийся далеко за пределами офиса. Имеется возможность управления переадресацией вызовов через Internet.

Программное обеспечение для Neophone оснащено программным интерфейсом под TAPI (Telephony Application Programming Interface), что позволяет предоставлять дополнительные сетевые услуги. В частности, осуществляется мгновенная выборка информации о звонящем абоненте (на основе номера вызывающего телефона) из корпоративной базы данных. Это очень удобно для различных центров телефонного обслуживания: к моменту соединения с вызывающим абонентом сотрудник компании уже знает, как зовут клиента, где он живет, какие ранее имел дела с вызываемой организацией и т. д.

Neophone обеспечивает не только прямое голосовое соединение между двумя абонентами, но и поддерживает организацию телефонных и видеоконференций, передачу электронной почты и факсимильных сообщений, а также ряд других услуг.

11.3. Рынок услуг IP-телефонии в России

В России, как и во всем мире, наибольшее развитие IP-телефония получила в промышленных городах, имеющих широкую инфраструктуру и развитый деловой сектор. Это обусловлено и потребностью населения этих городов в международной связи, стоимость которой при использовании IP-телефонии заметно ниже, а также хорошо развитой сетью Интернет. Список основных российских провайдеров услуг IP-телефонии приведен в приложении 2.

Наибольшее число провайдеров IP-телефонии находится в Москве. Причем большая часть из них является провайдерами услуг сети Интернет, то есть для передачи речевого трафика они используют глобальную сеть Интернет.

В основном провайдеры IP-телефонии в России являются лишь ресселерами зарубежных сетей. Например, компании МТУ-Информ, Инкомтел ТГ и ТелеРосс являются ресселерами компании ITXC на российском рынке.

Кроме Москвы и Санкт-Петербурга провайдеры IP-телефонии предоставляют свои услуги в ряде крупных городов. Чаще всего, это провайдеры Интернет, которые предоставляют абонентам местной телефонной сети только международную связь и связь с Москвой и Санкт-Петербургом, потому что практически отсутствует взаимодействие между местными провайдерами различных регионов. Несмотря на очевидную привлекательность IP-телефонии для России с ее огромными территориями, развитие этого вида услуг сдерживается из-за отсутствия единой структуры, координирующей взаимодействие местных операторов и представляющей Россию на международном рынке. В России отсутствует надежный национальный оператор, который обеспечил бы местным операторам взаимодействие друг с другом. Местному оператору необходимо не только достичь другого оператора, но и иметь надежную систему взаиморасчетов, которая минимизировала бы риск неплатежей между операторами.

В настоящее время несколько провайдеров IP-телефонии в Москве предпринимают попытки выступать как национальный провайдер. Это сеть TarioNet, RGC, Incomtel и другие. Однако при работе с ними местные операторы столкнулись с рядом проблем.

Во-первых, на местных операторов полностью возлагается обязанность по обеспечению связи с узлами этих провайдеров, которые в основном находятся в Москве или Санкт-Петербурге. Причем некоторые из них ставят обязательным условием использование выделенных каналов. Не каждый местный оператор способен оплатить аренду выделенного канала до Москвы.

Во-вторых, оборудование этих провайдеров не всегда удовлетворяет требованиям, предъявляемым к оборудованию национальных провайдеров. Поэтому качество услуг таких провайдеров часто очень низкое.

В-третьих, обычно эти операторы имеют выход только на одну сеть международного провайдера, поэтому их тарифы часто неравномерны и невыгодны.

В табл. 11.2 приведены тарифы на международную связь ОАО «Ростелеком» и нескольких провайдеров IP-телефонии в Москве по нескольким самым популярным направлениям связи.

Таким образом, стоимость одной минуты телефонного разговора через сеть Интернет в 2-5 раз ниже стоимости одной минуты разговора через сети ОАО «Ростелеком». Кроме того, например в сети TarioNet действуют льготные тарифы (в ночное время, в выходные), которые в 1,5-2 раза ниже дневного тарифа.

Следует однако учитывать, что тариф IP-телефонии зависит не столько от расстояния между абонентами, как от местонахождения ближайшего шлюза IP-телефонии от вызывае-

мого абонента, то есть степени развития сети оператора ITSP и его партнеров. Так разговоры с некоторыми странами Азии, Ближнего Востока и Южной Америки через сети TarioNet и RGC незначительно экономят средства и сравнимы с расценками традиционной телефонной связи, хотя и ниже их. Если учесть, что качество IP-телефонии не гарантированно и длительность разговора может увеличиться из-за плохого качества, то стоимость одного и того же разговора через Интернет может быть даже выше, чем через традиционную телефонную сеть. Это можно увидеть на примере данных таблицы 11.3, где приведены тарифы ОАО «Ростелеком», TarioNet и RGC в направлениях на Южную Америку, Азию и Ближний Восток и Африку.

Таблица 11.2. Сравнение тарифов нескольких провайдеров IP-телефонии в Москве, долл./мин.

Направление	Tario Net (дневной тариф)	RGC (Rinotel)	Корпорация ОСС (дневной тариф)	ОАО «Ростелеком» (дневной тариф, квартирный сектор)
США	0,43*	0,16	0,19	0,87*
Германия	0,43*	0,18	0,21	0,71*
Франция	0,50*	0,18	0,21	0,71*
Израиль	0,61*	0,21	0,24	1,06*
Эстония	0,56*	0,27	0,25	0,71*

* тариф с учетом НДС

Таблица 11.3. Тарифы IP-телефонии в различных направлениях, долл./мин.

Направления	TarioNet (дневной тариф)	RGC	ОАО «Ростелеком» (дневной тариф, квартирный сектор)
Южная Америка		1,4*	1,4*
Панама	0,54		
Перу	0,42		
Чили	0,23		
Азия и Ближний Восток		1,06*	1,06*
Ирак	0,94		
Иран	0,74		
Йемен	0,79		
Кувейт	0,39		
Африка		1,53*	1,53*
Эфиопия	0,94		
Ангола	0,47		
ЮАР	0,34		

* с учетом НДС

Тарифы на услуги IP-телефонии региональных провайдеров незначительно отличаются от тарифов провайдеров в Москве и Санкт-Петербурге (табл. 11.4).

Таблица 11.4. Тарифы региональных провайдеров IP-телефонии, долл./мин.

Направление	Новосибирск (Ринет)	Ижевск (Ижком)	Москва (Ситек)	Санкт-Петербург (Октагон Технолоджис)
США (Нью-Йорк)	0,38	0,24	0,19	0,38
Германия	0,38	0,28	0,19	0,34
Франция	0,38	0,28	0,19	0,34
Израиль	0,38	0,33	0,21	0,52
Перу	0,62	1,08	0,54	0,88
Москва	0,14	0,14	–	0,11
Санкт-Петербург	0,28	0,14	0,09	–
по России	0,28	до 0,25	до 0,29	до 0,26

Примечание: все тарифы даны с учетом НДС.

В регионах, в отличие от Москвы и Санкт-Петербурга, у пользователя IP-телефонии практически отсутствует возможность выбора провайдера, хотя в последнее время количество провайдеров IP-телефонии в России существенно увеличилось. Кроме того, многие из региональных провайдеров не обеспечивают должное качество услуг, так как для связи с другими сетями они используют сеть Интернет, которая не предназначена для передачи речевой информации в реальном масштабе времени. Поэтому IP-телефония в России не является такой же популярной услугой, как за рубежом. Однако количество операторов, желающих предоставлять услуги IP-телефонии в России, неуклонно растет.

Глава 12

ОБОРУДОВАНИЕ IP-ТЕЛЕФОНИИ

12.1. 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 реализаций 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 трафика 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 или

дооборудовать 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 Lucent 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 книги, 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, авторы рекомендуют для получения самой свежей информации обращаться непосредственно к производителям или получить информацию на соответствующих сайтах в Интернете.

12.2. 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 ECI 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, соеди-

ненных 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. 12.1. 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.

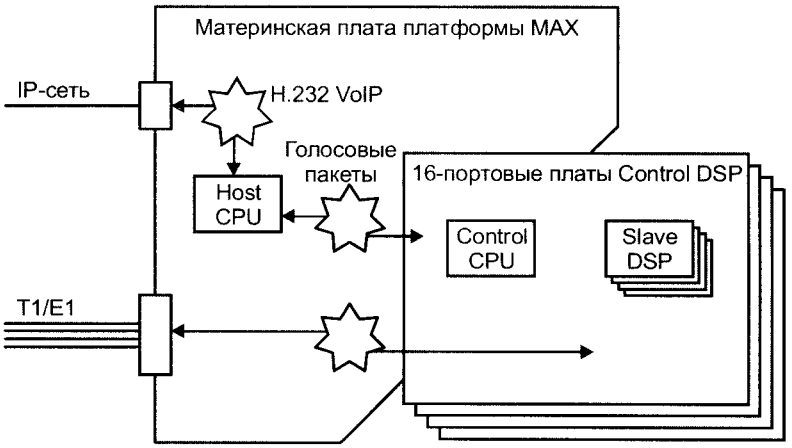


Рис. 12.1. Схема коммутатора доступа MAX 6000

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. Зоной 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 и 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.

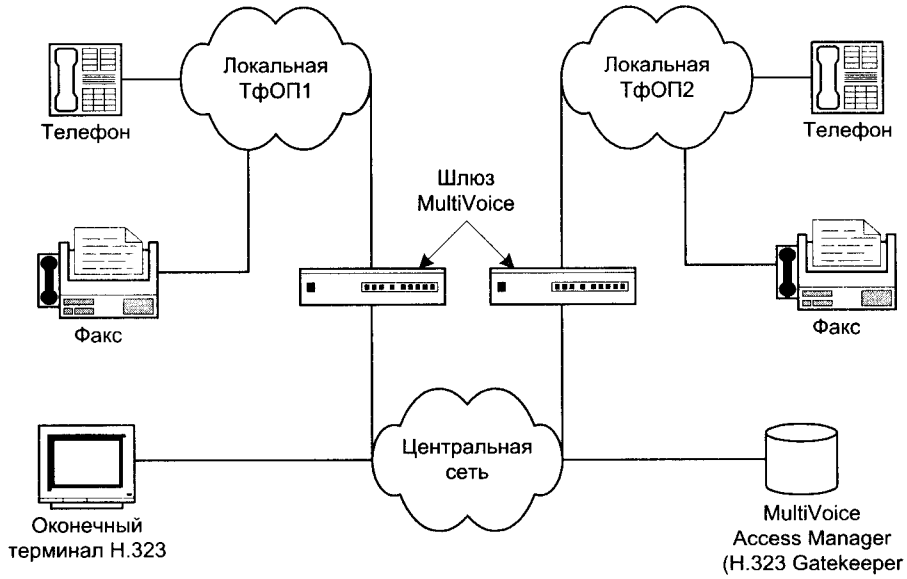


Рис. 12.2. Схема сети IP-телефонии на базе оборудования Lucent Technologies

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 трафика голоса, видео и данных (рис. 12.3). Все оборудование управляется единой системой Integrated Navis Management.

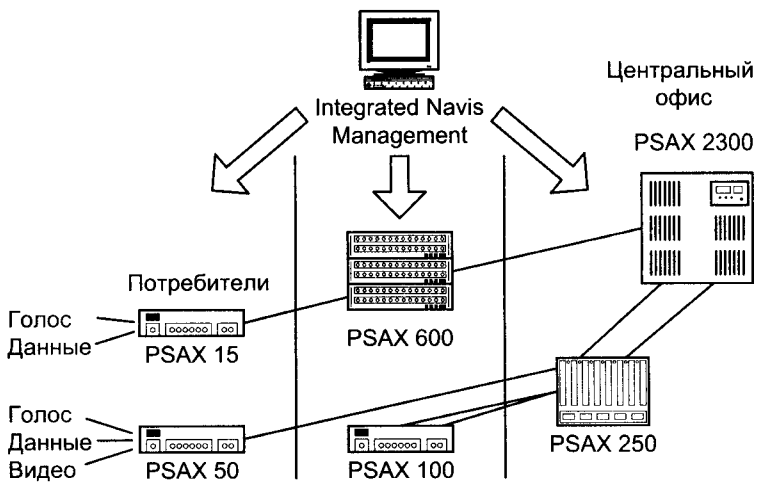


Рис. 12.3. Семейство мультимедийных шлюзов Lucent Technologies для сетей ATM

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 Distributed Softswitch, которая, помимо этого, включает в себя Clarent Call Manager, Clarent GateKeeper и 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 дебитных 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 конфигурируется в 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 трафиком 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 и перевод звонка, интеграция с голосовой почтой, совмещенных с высокоскоростным досту-

пом 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 трафиком. Пользуясь механизмами авторизации, маршрутизации и биллинга Clarent Command Center, программный пакет Connect позволяет не просто создавать маршруты в другие сети, но регулировать количество трафика 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 трафиком между двумя сетями, второе – предоставляет всем членам клирингхауса получать регулируемый доступ к терминации трафика 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 трафика.

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 100Base-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 ThroughPacket – 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 – процессор

Pentium или Celeron от Intel + Windows NT Server, карты AudioCodes для оцифровки голоса и телефонные интерфейсы Natural Microsystems. В семейство входят следующие шлюзы:

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

Характеристики семейства шлюзов Clarent приведены в табл. 12.1-12.3. 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 к ТфОП с помощью общеканальной сигнализации. Дополнительных устройств или изменения конфигурации сети при этом не требуется.

Таблица 12.1. Характеристики семейства шлюзов Clarent Carrier Gateway

Шлюз	Gateway 100	Gateway 400	Gateway 1200
Подключение к ТфОП	FXO, E&M analog, T1/E1	4 × T1/E1	4, 8, 10 или 12 T1/E1
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	1×250	2×250	2×400

Таблица 12.2. 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 12.3. Поддержка межстанционных телефонных интерфейсов в шлюзах Clarent

Семейство или шлюз	E1 R2	E1 R1.5	User-Side PRI	Network-Side PRI	E1 E&M	SS7/C7
Gateway 100	Да	Да	Да	Да	Да	Нет
Gateway 400	Да	Да	Да	Да	Да	Да
Gateway 1200	Да	Да	Да	Да	Да	Да

Как и Clarent CPG, шлюзы поддерживают Clarent ThroughPacket. При повреждении внешнего IP канала, шлюзы могут направить весь входящий трафик 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 12.4 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. 12.5.

Таблица 12.4. Характеристики шлюзов Cisco

Семейство или шлюз	MGCP (межшлюзовый протокол управления)	H.323v2
VG200	Есть	Есть (фаза2)
CISCO 1750	Нет	Есть
CISCO 3810 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-x1	Планируется	Нет

В табл. 12.6 отражена поддержка голосовыми шлюзами Cisco цифровых интерфейсов телефонной сети.

Как видно из таблиц, спектр 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 повышает надежность и производительность оборудования Cisco, а также увеличивает его срок службы.

Таблица 12.5. Поддержка аналоговых телефонных интерфейсов в шлюзах Cisco

Семейство или шлюз	FXS	FXO	E&M	Аналоговый DID/CLID
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 IOS 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-x1	Есть	Нет	Нет	Есть в IOS 12.1(4)T Нет в 12.1(2) xx

Таблица 12.6. Поддержка цифровых телефонных интерфейсов в шлюзах Cisco

Семейство или шлюз	E1 R2	E1 CAS	User-Side PRI	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-x1	Нет	Нет	Есть	Есть	Нет	Нет	Есть

При использовании оборудования Cisco, реализующего функции серверов доступа или 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 36xx или 26xx) со специализированной операционной системой IOS. Для каждого семейства существует несколько разновидностей операционной системы, выбор которых зависит от конкретной задачи.

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 Inernetworking, GRIC, Carrier1, 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 – 261x 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 Card (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 семейства 26xx голосового шлюза с цифровыми интерфейсами телефонной сети E1, в зависимости от версии IOS, наличия модуля AIM, объема оперативной памяти и выбранного типа сложности кодеков, 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 FXS/FXO/E&M или до двух цифровых трактов T1-CAS, в ближайшее время анонсирована поддержка T1/E1 PRI и E1 CAS. На шасси имеется встроенный интерфейсный порт Ethernet 10/100 Base-T.

Маршрутизаторы Cisco 36xx для IP-телефонии

Семейство модульных маршрутизаторов Cisco 36xx 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 в 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 рассмотренных 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, «бандл» – 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 K 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. 12.4.

12.3. 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.

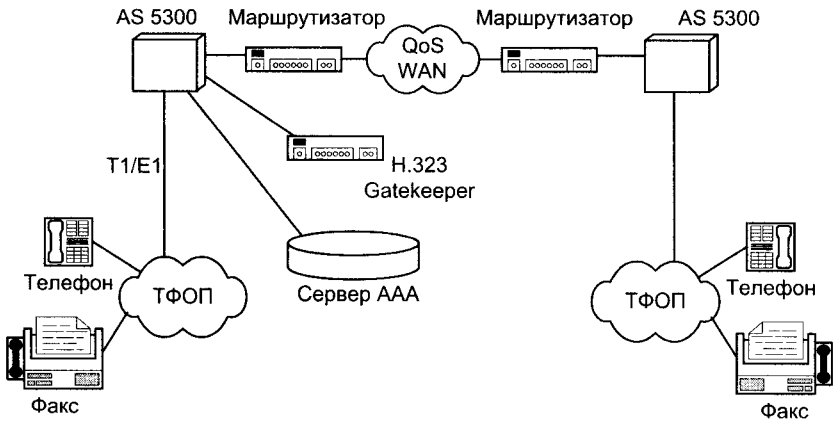


Рис. 12.4. Построение сети IP-телефонии на базе Cisco AS5300

На рис. 12.5 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.

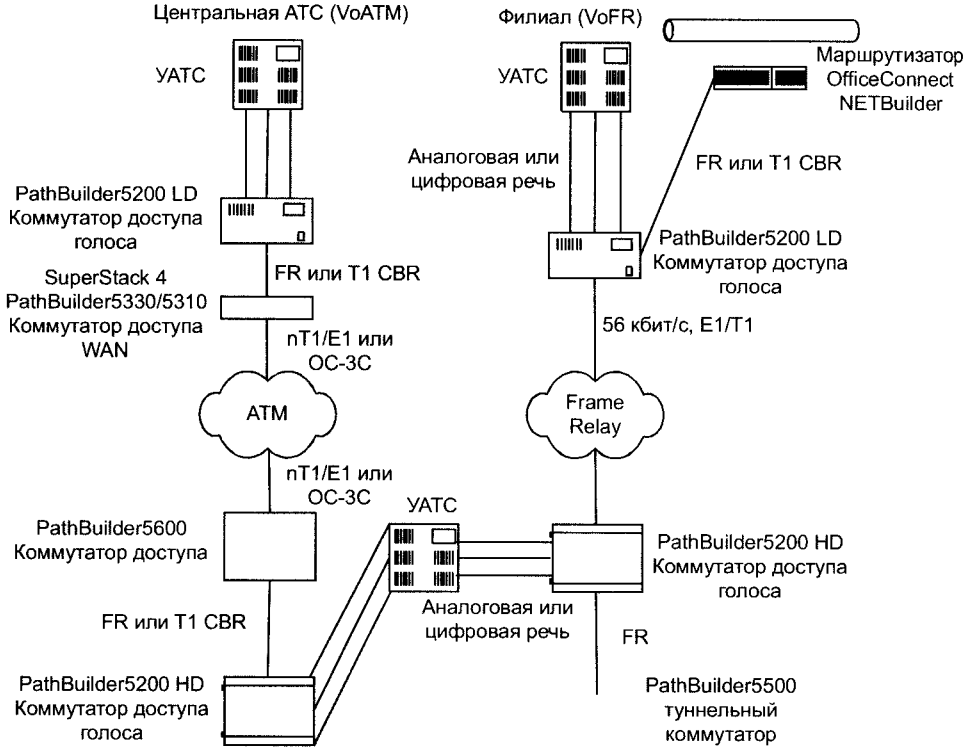


Рис. 12.5. Решение VoIP компании 3COM

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: E1, 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. 12.6.

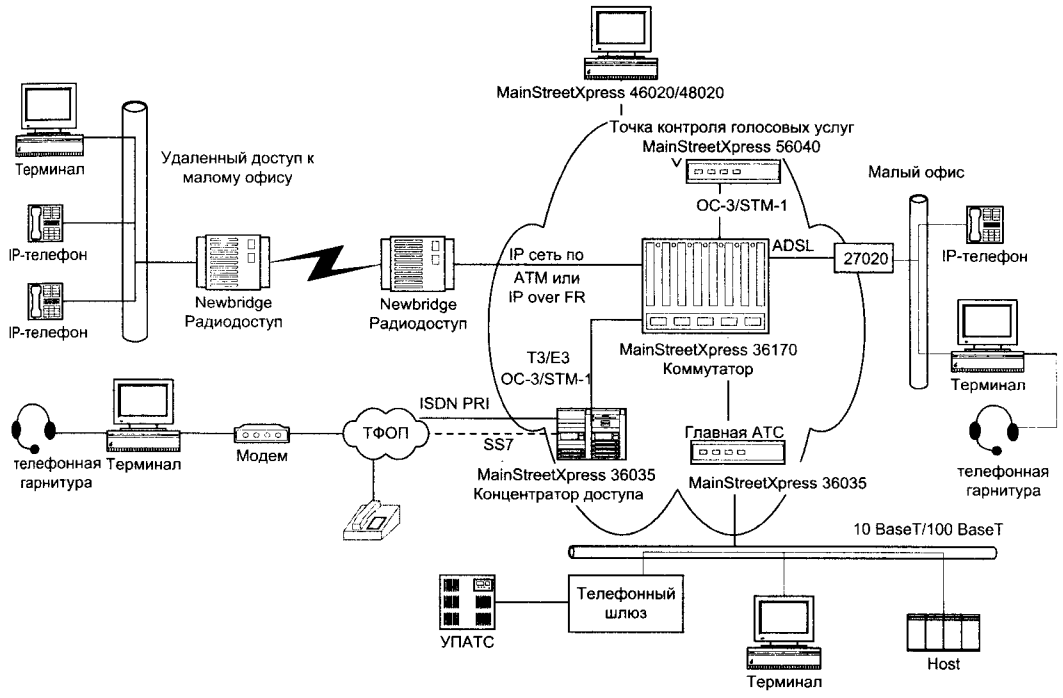


Рис. 12.6. Решение VoIP на базе оборудования компании Newbridge

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 интерфейса с общедоступными сетями, то система может работать с линиями T-1/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 видеотрафика.

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 OpenView, HP OpenView UNIX и 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) и 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 пакетом 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 теле-

коммуникационными 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 и способы 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. 12.7), 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.

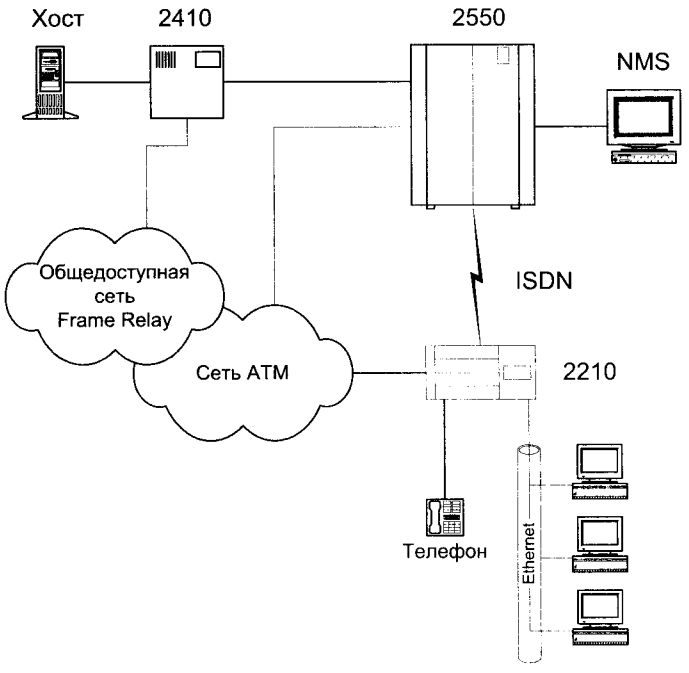


Рис. 12.7. Решение VoIP на базе оборудования компании Netrix Corp.

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 и выполняться 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 дебитных 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.723.1a, G.728, G.729, G.729a, G.729b, G.729ab.

Модель обладает развитыми механизмами обеспечения QoS, что немаловажно для решения задач по передаче голоса через пакетные сети. Наиболее важные из них: фрагментация пакетов, уплотнение заголовков, управление полосой пропускания по протоколу RSVP, по-

давление 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. 12.8 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.

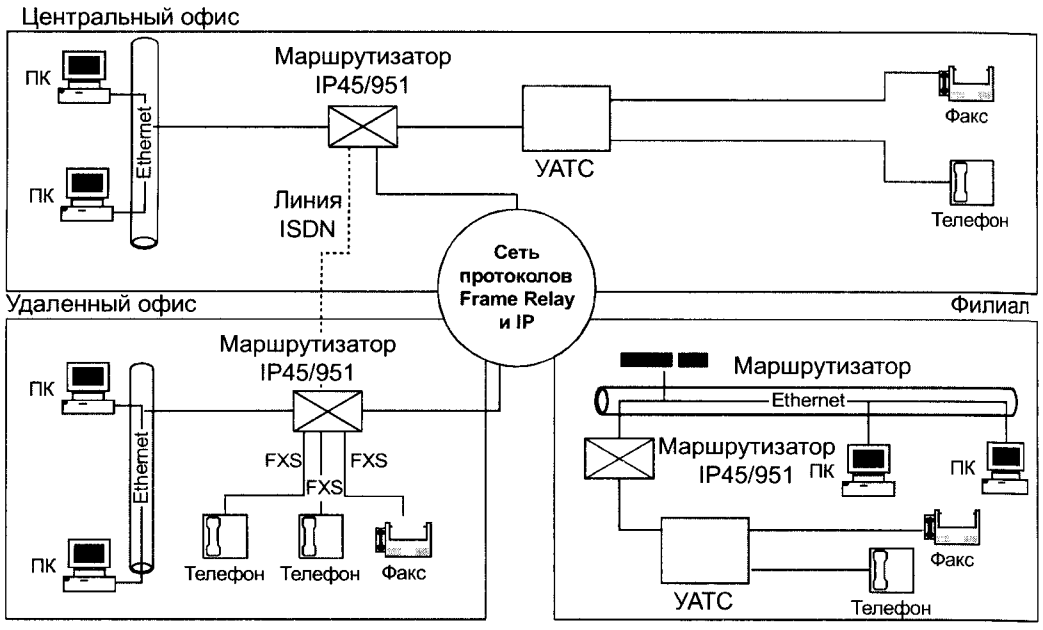


Рис. 12.8. Фрагмент типовой корпоративной сети на базе шлюза-маршрутизатора IP45/951 корпорации NEC

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 безопасную ра-

боту 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. 12.9). 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.

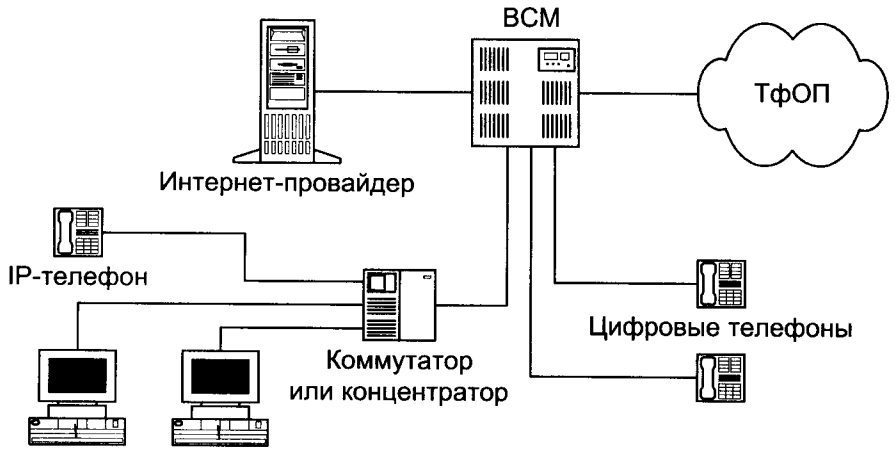


Рис. 12.9. Реализация сети IP-телефонии на базе системы BCM фирмы Nortel Networks

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 WGXчерез 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.164 – 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, иден-

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.

12.4. УАТС с функциями IP-телефонии

Реализация функции IP-телефонии в УАТС

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. 12.10).

Следует отметит, что используемые в УАТС шлюзы постоянно отслеживают качество связи и, если оно становится ниже заданного уровня, переводят соединение в традиционные сети (рис. 12.11).

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 отмстить, 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.

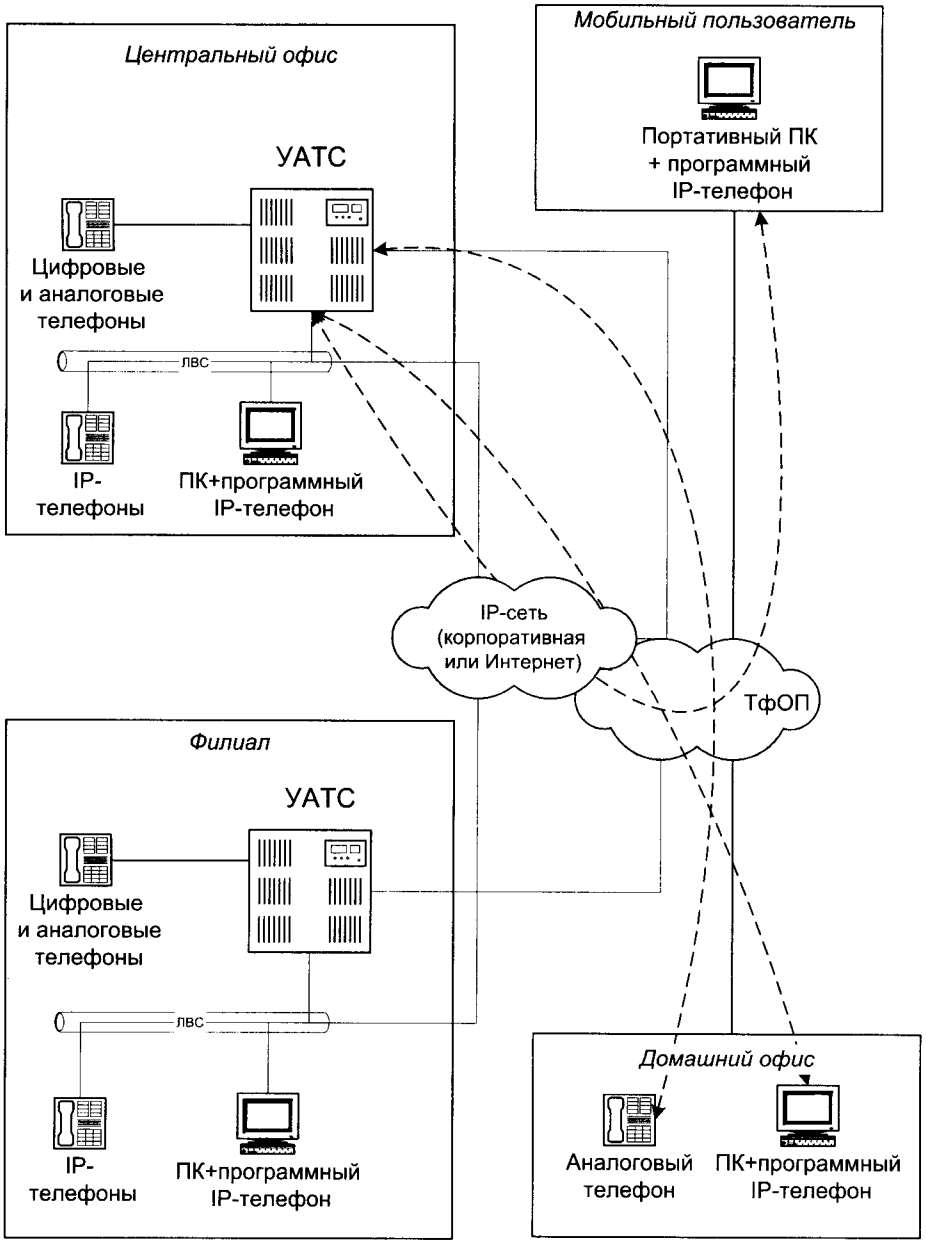


Рис. 12.10. Реализация корпоративной сети IP-телефонии

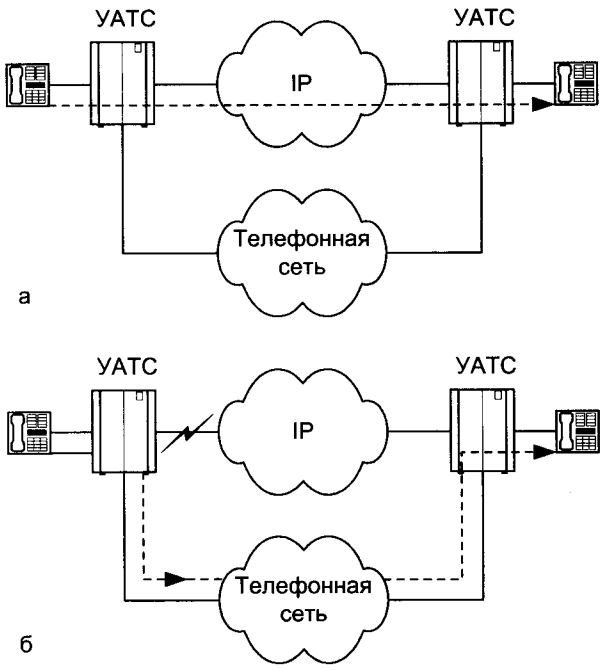


Рис. 12.11. Переход IP-УАТС на телефонную сеть при резком ухудшении качества IP-сети

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. 12.7 и табл. 12.8 [11].

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

Таблица 12.7. 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	Hicom 150 E	+	+	+

Таблица 12.8. 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.729A, GSM-EFR	G.711, G.723, G.729, G.729A	G.711, G.723.1,
Поддержка H.323	+	+	+	+	+	+
Поддержка SIP	–	–	–	–	–	–
Перевод трафика в ТфОП при ухудшении качества IP-связи	+	+	+	+	+	+
Передача по IP-сигнализации (QSIG и/или фирменных)	+	+	+	+	+	+

УАТС 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, если по тому же соединению он получит «издалека» пакеты IP с голосом, они будут соответствующим образом обработаны. (Стоит отметить, что сами станции могут иметь встроенный интерфейс ATM или frame relay).

Стратегия Alcatel заключается в масштабном переходе на новую унифицированную платформу в своих решениях. Любопытно, что, в отличие от других производителей, компания внедряет нововведения в свои продукты, начиная с верхнего уровня. Это объясняется ориентацией Alcatel в первую очередь на рынок крупных корпоративных заказчиков и операторов связи. Следует отметить, что по заявлениям Alcatel уже имеющиеся УАТС серии 4400 можно без проблем превратить в OmniPCX 4400.

Линия продуктов WebSwitch компании ERICSSON

В настоящее время компания Ericsson (Швеция) идет по пути создания новой линии продуктов – WebSwitch 2000. WebSwitch не заменят, по крайней мере, в обозримом будущем, существующие модели станций фирмы Ericsson, а будут развиваться параллельно с ними. В 2000 году фирма Ericsson выпустила модули расширения с поддержкой IP-телефонии и для других своих УАТС, однако это направление компания намерена развивать в первую очередь именно в линии WebSwitch.

Первые модели WebSwitch поддерживают от 32 до 64 абонентов по IP-соединениям и по традиционным линиям. Соответственно, они могут иметь внешние соединения с IP-сетями и с обычными ГТС. Судя по емкости станции, Ericsson достаточно осмотрительно развивает новую линию продуктов, не торопясь выпускать дорогие модели, так как высокая цена может отпугнуть заказчика IP-станции. Как свидетельствуют характеристики WebSwitch, компания вполне четко видит ее сегодняшнюю рыночную нишу – компактное, самодостаточное решение для удаленного офиса или подразделения, где есть потребность в компьютерной телефонии. Впрочем, при внешней компактности WebSwitch поддерживает все основные сервисы цифровой УАТС и в силу этого может использоваться и как платформа для создания распределенной телефонной системы. Акцент на простоту в инсталляции и эксплуатации свидетельствует о том, что компания стремится создать IP-телефонии имидж потребительского решения.

WebSwitch также дополняется двумя приложениями. Первое – PhoneLink – представляет собой «виртуальный» телефон – абонентское место для мультимедийного ПК. Второе – SwitchLink – является консолью администратора и позволяет управлять станцией по IP-сети. Оба приложения также характеризуются компактностью и простотой и подтверждают намерение Ericsson развивать новое направление «снизу».

Одной из самых любопытных характеристик WebSwitch является возможность подключения к станции беспроводных IP-телефонов. Правда, количество таких аппаратов крайне невелико, так как каждое подключение требует установки отдельного радиомодуля. Поэтому свой полномасштабный IP-DECT развернуть не удастся, хотя обеспечить мобильным IP-аппаратом администратора можно уже сейчас. Не исключено, что со временем, когда настольные IP-телефоны получат реальный спрос, беспроводные аппараты появятся и у других производителей. С технической точки зрения в них нет ничего сложного – попросту говоря, обычный радио-Ethernet.

Вообще говоря, идея беспроводного IP-телефона достаточно привлекательна. Например, в случае если радиомодуль, выполняющий функции точки доступа, установлен непосредственно на станции, то телефонный трафик на участке станция-аппарат передается по отдельному сегменту, с более чем достаточной пропускной способностью. Тем самым значительная часть проблем с качеством решается сама собой. С другой стороны, правда, потребность в простом по функциональности IP-телефоне (все-таки, это «трубка», а не системный аппарат) пока еще не стоит на повестке дня. Во всяком случае сам факт, что и беспроводная телефония тоже поддается «пакетизации», весьма примечателен.

УАТС DEFINITY компании Avaya Communication

Для компании Avaya Communication (бывшее подразделение корпоративных сетей Lucent Technologies) IP-телефония является одним из этапов развития уже имеющейся коммуникационной платформы DEFINITY. IP-телефония хорошо вписывается в сегодняшнюю стратегию развития DEFINITY на базе распределенной архитектуры. Образно говоря, Avaya Communication встраивает ATM во внутреннюю шину DEFINITY, что позволяет разносить блоки станции на неограниченное расстояние. Поскольку фактически станция сама по себе представляет своего рода локальную сеть, создание внешнего сетевого интерфейса – дополнение не радикальное.

Следует отметить, что IP-интерфейс DEFINITY поддерживает несколько типов компрессии голоса, как стандартные (G.723, например), так и частные разработки Avaya Communication, которые компания считает более эффективными. Разумеется, если IP-телефонию DEFINITY требуется стыковать с внешними шлюзами (или решениями других производителей в локальной сети), то придется использовать стандартные средства. Однако в частной сети компания рекомендует именно свои разработки.

Абоненты, работающие через IP, получают прозрачный доступ ко всем сервисам станции, но их обслуживание IP-модулем имеет свои особенности. Группы пользователей IP-телефонии могут иметь разные приоритеты в отношении качества обслуживания. Разумеется, при осуществлении звонка с одного IP-телефона (аппаратного или программного) на другой (двойного) преобразования голоса внутри станции не происходит – связь осуществляется на уровне IP-интерфейса.

Для доступа к телефонным сервисам с ПК Avaya Communication предлагает программное абонентское место – развитый программный персональный коммуникатор из семейства продуктов PassageWay. Упрощенный доступ к телефонным IP-сервисам также возможен через интерфейс Web (при помощи загружаемого апплета). Кроме того, функции IP-телефонии полностью прозрачным образом интегрируются с уже реализованными на платформе DEFINITY функциями и приложениями CTI, например с ПО Avaya Communication для операторских центров CenterVu. Вдобавок DEFININTY поддерживает альтернативные варианты связи с абонентом. Если по умолчанию его телефонный номер привязан к «виртуальному» аппарату, т. е. к ПО, работающему на ПК, то в случае, если ПК выключен или завис, звонок перенаправляется на ближайший к нему телефон (конкретный номер задается заранее).

В том, что касается доступа к функциям управления станцией, Avaya Communication предпочитает придерживаться консервативного подхода – через консоль по отдельному порту IP-интерфейс (не собственно модуль, а именно протокольный интерфейс) не имеет непосредственного доступа к ядру DEFINITY, и никаких функций управления станцией в IP-модуль не заложено. Таким образом, даже если система IP-телефонии будет иметь выход в Internet, «взлома» станции опасаться не стоит. Впрочем, и сам программный интерфейс IP-телефонии является защищенным от несанкционированного доступа благодаря авторизации пользователей и шифрованию паролей.

Разумеется, достаточно большой интерес вызывает вопрос о возможности модернизации уже находящихся в эксплуатации станций. Avaya Communication не берется утверждать, что во всех без исключения случаях «старые» DEFINITY можно без проблем превратить в IP-станции. Однако в России продажи DEFINITY через партнеров в больших объемах начались лишь в 1994-95 году и поэтому у нас почти нет устаревших моделей. Поэтому путем добавления новых модулей, обновления ПО и, в крайнем случае, замены процессора имеющуюся УАТС можно при желании превратить в IP-станцию.

Среди отдаленных перспектив развития IP-решений для DEFINITY Avaya Communication планирует (пока без определения четких сроков) выпуск беспроводных систем IP-телефонии, что неудивительно, так как компания является одним из лидеров рынка беспроводных сетей. В целом стратегия Avaya Communication разрабатывалась с учетом интересов крупных корпоративных заказчиков и поддержки большой инсталлированной базы, поэтому компания идет путем постепенного добавления новых сервисов и интерфейсов к имеющейся платформе, по возможности избегая радикальных нововведений (новых продуктовых линий).

УАТС компании NORTEL

Компания Nortel последовательно движется в направлении реализации тотальных IP-решений в рамках своей концепции Unified Networks. Движение это не только последовательно, но и постепенно, и интеграцию IP-телефонии в свои УАТС компания ведет «снизу вверх», начав со станций серии Mercator. Первой станцией со встроенным IP-шлюзом у Nortel стала Mercator 6500, новая модель называется уже Mercator 6500IP. Чтобы решение было полноценным с точки зрения управления сервисами, компания предлагает использовать Telephony Manager на базе платформы управления Nortel Optivity. Кроме того, постепенно все больше функций IP приобретает и семейство Meridian, для него также имеются модули расширения с IP-интерфейсами для подключения к глобальным (Internet Gateway) и к локальным сетям.

Развиваемая Nortel концепция Inca (Internet Communications Architecture) в целом основана на постепенном внедрении IP-телефонии в корпоративное окружение путем добавления все новых и новых компонентов. Таким компонентом, например, является Meridian SL-100 Internet Gateway – шлюз с поддержкой до 480 транков ISDN на один контроллер. Сама концепция Inca объединяет целый ряд распределенных, по-разному позиционируемых решений (некоторые компоненты, разумеется, совпадают). Например, Inca model M1, как можно видеть из названия, предназначается для тех заказчиков, кто хотел бы создать IP-инфраструктуру вокруг станций Meridian 1. В свою очередь, Inca model 7500 позиционируется как радикально эволюционировавшее решение, хорошо дополняющее Mercator 6500IP.

Как видно, в рамках своей стратегии развития IP-телефонии компания Nortel продвигает внешние (в том числе серверные) решения и средства интеграции IP в УАТС, как взаимодополняющие части одного решения. Такая стратегия позволяет достаточно гибко осуществлять миграцию на IP и внедрять компоненты системы IP-телефонии в корпоративное окружение по мере необходимости. Скорее всего, из этих соображений в обозримом будущем компания вряд ли откажется от внешних по отношению к станциям компонентов как типовой части решения, даже при дальнейшем увеличении степени интеграции IP-сервисов в УАТС. Концепция внешних многофункциональных модулей (MFM) для IP-облака является для Nortel основной (рис. 12.12). Это не какой-нибудь недостаток по сравнению с решениями, в которых вся функциональность переносится в УАТС, а просто альтернативный вариант развития.

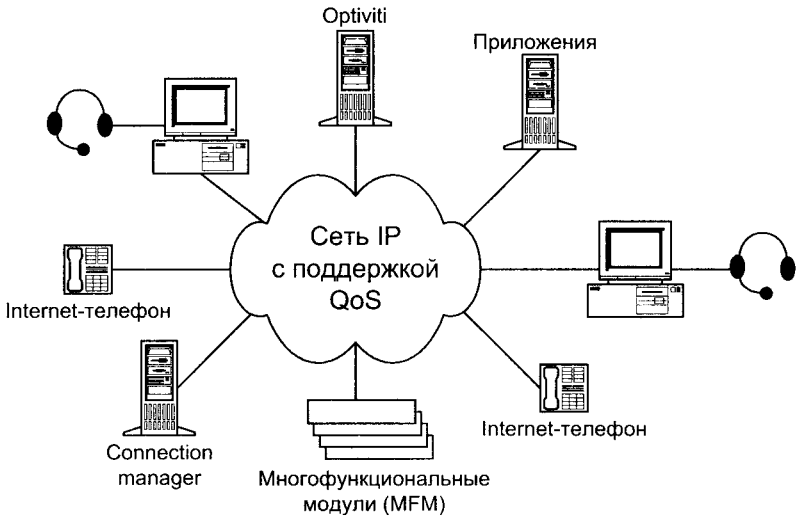


Рис. 12.12. Схема корпоративной сети IP-телефонии на базе оборудования Nortel

УАТС компании SIEMENS

В качестве платформы для интеграции IP-телефонии Siemens выбрала свое семейство УАТС Hicom 150E (станции среднего класса), для которого она выпускает модуль расширения Hicom Xpress @LAN. Вообще говоря, Xpess @LAN как аппаратное решение представляет собой нечто большее, чем IP-шлюз. Этот модуль действительно является мостом или даже маршрутизатором начального уровня. Xpress @LAN обеспечивает станции интерфейс с локальной сетью для реализации IP-телефонии, а также позволяет использовать внешние соединения ISDN для объединения локальных сетей удаленных офисов. Совместно с Xpress @LAN станция может исполнять роль ISDN-маршрутизатора, а также динамически группировать внешние каналы ISDN в зависимости от трафика. При увеличении потребности в пропускной способности до 8 или 16 каналов класса B (в зависимости от реализации) могут быть задействованы автоматически; при снижении уровня трафика ненужные каналы не задействуются.

Поскольку IP-интерфейс у Siemens полноценный и не ограничен только функциями передачи голоса, а также потому, что он выполняет пограничные функции, очевидно, что он нуждается в защите от несанкционированного доступа. Защита реализована посредством встроенного брандмауэра. Брандмауэр разрабатывался в расчете на самые строгие немецкие требования по защите и вполне сравним по уровню надежности с существующими популярными средствами. Еще одним расширением УАТС Siemens является поддержка видеоконференций.

Для проведения видеоконференций Siemens предлагает специальное клиентское ПО. Специальное программное обеспечение разработано и для организации абонентского места (виртуального телефона) на мультимедийном ПК. Решения по IP-телефонии также естественным образом интегрируются с имеющимися у Siemens средствами CTI.

Подход Siemens к конвергенции данных и голоса является достаточно радикальным, так как он подразумевает не только интеграцию пакетной передачи голоса в УАТС, но и непосредственное наделение станции функциями оборудования по передаче данных. В определенном смысле, это можно назвать «ответом» на тенденцию наделения мультисервисных

устройств для удаленных офисов функциями УАТС начального уровня. В данном случае ситуация почти зеркальная. Как можно предполагать, такой встречный курс приведет к созданию устройства, где в полной мере реализуются функции как телефонной станции, так и граничного устройства для рынка SOHO или удаленного офиса. Насколько можно судить, стратегия компании по интеграции пакетной телефонии основана на изначальной ориентации на определенный класс заказчиков, о чем говорит выбранная для модернизации платформа. Интегрировать IP-сервисы в станции Hicom 300 на аппаратном уровне Siemens не планирует. Стратегия развития этой серии схожа с подходом, исповедуемым Nortel, – станция превращается в коммуникационную платформу, а различные дополнительные сервисы реализуются с помощью внешних серверов – в данном случае за счет решения HiNet.

12.5. IP-телефоны

Использование IP-телефонов

Аппаратный IP-телефон – самостоятельное устройство, которое не требует подключения к телефонной линии и позволяет пользоваться услугами IP-сети для осуществления междугородных и международных переговоров, например через Интернет-каналы.

IP-телефону присваивается собственный телефонный номер, на который может позвонить любой абонент IP-сети. В отличие от привычного варианта доступа к услугам, когда абонент должен вначале позвонить по городскому телефону доступа к провайдеру IP-сети, набрать свой PIN-код и только после этого набрать требуемый телефонный номер, IP-телефон используется как классический телефон. Абонент просто снимает трубку и набирает требуемый номер. IP-телефон предназначен как для частного пользования, так и для установки в офисах. В последнем случае, при использовании нескольких аппаратов, появляется возможность организовать офисную или корпоративную связь без использования классической телефонии. При этом совершенно безразлично территориальное размещение аппаратов – организация связи будет одинаково простой как в случае, если они расположены на соседних столах, так и при установке их в противоположных точках земного шара. Для подключения IP-телефона необходимо только наличие подключения к IP-сети (в случае сети Интернет – желательно постоянно действующего).

Структурная схема IP-телефона показана на рис. 12.13.

IP-телефон включает в себя следующие компоненты:

- интерфейс пользователя (User Interface);
- речевой интерфейс (Voice Interface);
- сетевой интерфейс (Network Interface);
- блок процессора (Processor Core);
- связывающая логика (associated logic).

Интерфейс пользователя обеспечивает реализацию традиционных функций телефона. Как минимум, это клавиатуры для набора номера (кнопки 0-9, *, #) и звуковой индикатор для сигнализации о входящих вызовах пользователю. На более сложных телефонных аппаратах используются дополнительные клавиши, обеспечивающие повторный набор номера, хранение номеров, переадресацию, конференцсвязь и т.д. Обычно используется дисплей для отображения подсказки пользователю, набираемого номера, информации о входящих вызовах и т.д. В некоторых моделях телефон оборудован последовательным интерфейсом для подключения устройств типа PDA (персональный цифровой помощник), которое позволяет обеспечивать синхронизацию телефонной информации, облегчает автоматический набор номера и т.д.

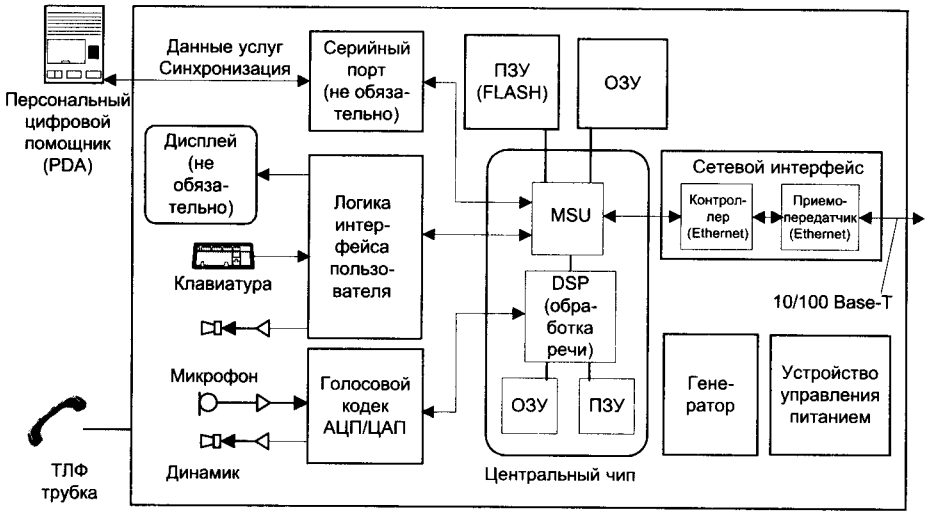


Рис. 12.13. Структурная схема IP-телефона

Речевой интерфейс обеспечивает преобразование аналогового голосового сигнала в цифровые отсчеты. Речевые сигналы от микрофона дискретизируются с частотой 8 кГц, что создает после кодера с импульсно-кодовой модуляцией цифровой поток данных на процессор со скоростью 64 кбит/с. Обратный процесс позволяет преобразовать поток данных 64 кбит/с через декодер ИКМ в аналоговый речевой сигнал, который передается в телефонный капсуль или громкоговоритель.

Сетевой интерфейс обеспечивает передачу и прием речевых пакетов от/в телефона в локальную вычислительную сеть чаще всего с интерфейсом 10BaseT или 100BaseT Ethernet, работающую по протоколу TCP/IP. IP-телефон может иметь второй разъем RJ-45 Ethernet для подключения персонального компьютера, чтобы совместно использовать одно подключение к настенной розетке.

Блок процессора выполняет обработку голосовой информации, обработку сигнализации, обработку протокола и функции программного управления всей схемой телефона. Как показано на рис. 12.13, он состоит из цифрового сигнального процессора (DSP) для выполнения функций обработки голоса и устройства микроконтроллера (MCU) для выполнения остальных функций управления. Для обеспечения гарантированного хранения программного обеспечения в телефоне используется флэш-память.

Настройка IP-телефона крайне проста и может выполняться самим абонентов в соответствии с инструкцией. Абоненту выдаются авторизационные данные (имя, PIN-код) и выделяется уникальный телефонный номер для звонков с другого IP-телефона.

Преимущества использования аппаратных IP-телефонов:

- простота и экономия технических ресурсов при организации корпоративной или частной сети связи, поскольку не используется классическая телефония;
- ускорение процесса дозвона – исключаются звонок на телефон доступа к сети IP-телефонии и набор PIN-кода;
- мобильность – IP-телефон может быть быстро перемещен в любую другую точку с минимальной перенастройкой или вообще без нее;
- возможность прямых звонков на другой IP-телефон;
- для операторов – экономия технических ресурсов, так как не используются линии связи.

Пример связи с помощью IP-телефона через сеть Интернет показан на рис. 12.14. Здесь в качестве управляющего протокола используется протокол SIP (Session Initiation Protocol). Функции авторизации и учета, а также обеспечение взаимодействия с компонентами IP-сети, работающими на основе протокола H.323, выполняют SIP-Proxy и SIP-H.323 Signalling Gateway.

Звонки учитываются точно так же, как и звонки через шлюз оператора сети IP-телефона. Для клиентов, использующих IP-телефон, оператор может создать специальный тарифный план. Биллинговая система выполняет специальную проверку для клиентов с таким тарифным планом и не допускает звонков обычным путем, через входные телефоны общедоступного шлюза.

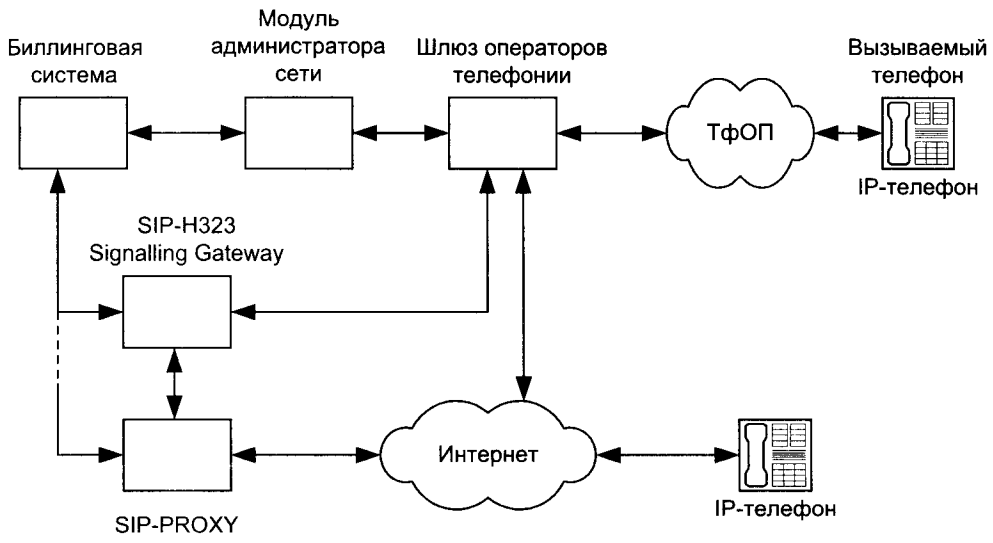


Рис. 12.14. Схема связи через Интернет с использованием IP-телефона

В качестве недостатков использования IP-телефонов следует указать необходимость локального питания, а это дополнительные неудобства и снижение надежности. Без дистанционного питания IP-телефоны вряд ли получат широкомасштабное распространение, а стандарта на организацию такого питания по ЛВС пока нет.

Следует отметить, что помимо аппаратной существуют и программные реализации IP-телефонов. В этом случае персональный компьютер, оборудованный телефонной гарнитурой или микрофоном и колонками, превращается в многофункциональный коммуникационный центр. Пользователь персонального компьютера, помимо доступа к обычному телефонному сервису, получает массу других возможностей, повышающих продуктивность его работы. Так, благодаря наличию стандартного телефонного прикладного программного интерфейса TAPI к другим программам, можно автоматически получать информацию о звонящем абоненте (извлекается из базы данных по его идентификатору), а также использовать удобные интерфейсы для контроля за телефонными вызовами и работы с речевой почтой. Сведения о некоторых программных IP-телефонах приведены в приложении 6.

Далее рассмотрены наиболее известные аппаратные IP-телефоны, выпускаемые ведущими мировыми производителями телекоммуникационного оборудования.

IP-телефоны фирмы Cisco

Фирма Cisco одна из первых начала выпускать IP-телефоны. В настоящее время на рынке представлено несколько моделей таких телефонов. Настольный IP-телефон существует в двух вариантах: IP Ethernet-телефон серии Cisco IP-Phone, который подключается непосредственно в сетевой разъем Ethernet RJ-45 (отличается от традиционного телефонного разъема RJ-11) и телефонная трубка/телефон-наушники, которые подключаются непосредственно к персональному компьютеру. Второй вариант понравится тем пользователям, которые интенсивно используют телефон вместе с ПК.

IP Ethernet-телефон – это новое устройство, которое похоже на обычный телефон, подключаемый к УАТС, но, в отличие от него, подсоединяется к Ethernet-порту коммутатора. IP-телефон обеспечивает качество звука, сравнимое с обычным телефоном, а также имеет программируемый ускоренный набор номера и другие расширенные функции. У IP-телефона много общего с ПК. Он может работать, как обычное IP-устройство, и иметь собственный IP-адрес. Поскольку IP-телефон полностью совместим со стандартом H.323, с его помощью можно связаться с любым другим H.323-совместимым устройством или ПО, например с Microsoft NetMeeting. Ниже приведены некоторые основные характеристики IP-телефона:

- 10BaseT Ethernet (RJ-45);
- программируемые кнопки для функций, ускоренного набора номера и индикатор состояния линий;
- IP-адрес и передача сигнализации (по TCP/IP) через CallManager;
- поддержка стандарта H.323;
- встроенная аудиокомпрессия: G.711, G.7234
- назначение IP-адреса и конфигурация через сервисы DHCP, BootP или с клавиатуры;
- администрирование или настройка функциональных кнопок через Web-браузер;
- встроенное шифрование голосового трафика для защиты от прослушивания;
- третья пара проводов для резервирования питания в случае отказов электроснабжения;
- взаимодействие ПК и приложения NetMeeting с помощью единственной кнопки (T.120); для поддержки таких функций, как совместное использование приложений, видео, chat и whiteboarding;
- встроенный порт сетевого концентратора для каскадного подключения устройств Ethernet-телефонов и ПК (реализовано лишь в модели 12);
- разнообразные модели: спикерфон, дисплей, многокнопочные аппараты – Cisco поставляет 12- и 30-кнопочные модели IP-телефонов (рис. 12.15).

а) б) в)

Рис. 12.15. Модели IP-телефонов фирмы Cisco: а) 7910 и 7910+SW; б) 7940; в) 7960

В состав серии Cisco IP-Phone входят четыре модели, характеристики которых приведены в *табл. 12.9.*

Таблица 12.9. Характеристики IP-телефонов серии Cisco IP-Phone

Тип IP-телефона	7910	7910+SW	7940	7960
Количество программируемых клавиш	4	4	6	10
Тип дисплея	48-символьный ЖК-дисплей	48-символьный ЖК-дисплей	Большой ЖК-дисплей	Большой ЖК-дисплей
Подключение к сети Ethernet	Прямое подключение	Прямое подключение	Встроенный Hub, 2 порта Ethernet 10/100 Base-Tx Ethernet (RJ-45)	Прямое подключение
Количество и тип портов	1 порт 10BaseT (RJ-45)	2 порта 10/100 BaseT	1 порт EIA/TIA RS-232	2 порта 10/100 Base-Tx Ethernet (RJ-45), 1 порт EIA/TIA RS-232
Компрессия	G.711, G.729a	G.711, G.729a	G.711, G.729a	G.711, G.729a

На ЖК-дисплей всех моделей Cisco IP Telephone выводятся дата и время, номер и имя вызывающего абонента, цифры набираемого номера. Кроме того, в моделях 7940 и 7960 определяется и высвечивается тип вызова: внутренний или внешний.

Также существует чисто программная версия телефона для ПК. Программный продукт Cisco IP SoftPhone позволяет эмулировать IP-телефон на компьютерах, работающих под управлением операционных систем Windows 95/98/NT 4.0. ПО виртуального телефона может быть установлено на ПК или мобильный компьютер, оснащенный звуковой картой и микрофоном. Подобно IP-телефону Cisco, имеющему встроенный программный интерфейс Microsoft NetMeeting API, вызывающая сторона может устанавливать сессии NetMeeting нажатием единственной функциональной кнопки и использовать приложения для видео и функции whiteboarding. Cisco IP SoftPhone полностью совместим с телефонами Cisco IP и поддерживает компрессии G.711, G.723.1, G.729.A.

IP-телефоны компании Avaya

Компания Avaya для корпоративных сетей разрабатывает продукты семейства ECLIPS (Avaya Enterprise Class IP Solutions). Все устройства этой линейки продуктов являются неотъемлемой частью телекоммуникационного сервера Definity и не могут функционировать отдельно.

Новые IP-телефоны Avaya 4612 и 4624 (рис. 12.16), отличающиеся количеством функциональных кнопок (12 и 24 соответственно), появятся в России ориентировочно в феврале-марте 2001 года. Чуть позже на рынок выйдет 6-кнопочная модель Avaya 4606. IP-адрес может быть статическим или динамическим (как клиент DHCP). IP-телефоны могут питаться дистанционно от УАТС Definity по Ethernet-сети 10/100Base-T или от локального источника

питания. Устройства поддерживают голосовые кодеки G.711, G.723.1 и G.729. Минимальная полоса пропускания при использовании кодека G.729 составляет около 33,6 кбит/с, т.е. теоретически IP-телефоном можно пользоваться из дома, подключаясь к корпоративной сети с помощью обычного модема. Устройства оснащены встроенным концентратором, позволяющим с одной стороны подключить телефон к локальной сети, а с другой – рабочую станцию пользователя. Есть одно гнездо для наушников, USB-интерфейс и инфракрасный порт. В телефоны также встроен дуплексный громкоговоритель с функцией эхокомпенсации для повышения качества голоса.

Рис. 12.16. IP-телефоны компании Avaya

Интересно реализована функция обновления ПО устройств. Каждый раз при подключении к сети IP-телефон в первую очередь ищет FTP-сервер и сравнивает свою версию ПО с установленной на сервере. В случае обнаружения более поздней версии, процесс обновления осуществляется автоматически. По данным производителя, IP-телефоны совместимы с ПО NetMeeting. Для работы IP-телефонов необходима 9-я версия ПО для станции Definity, вышедшая 4 декабря 2000 г. (она появится в одно время с IP-телефонами).

Следующим поколением в семействе ECLIPS станет аппарат 4630 IP Screenphone, ориентировочные сроки выхода которого намечены на середину 2001 года. Данное устройство представляет собой IP-телефон с большим цветным сенсорным экраном, обеспечивающим, помимо основных функций, доступ в сеть Интернет. Для обеспечения связи 4630 IP Screenphone будет поддерживать трехпроводную, а также R1.5 сигнализации.

По данным компании, телефонные IP-аппараты будут стоить от 250 до 600 долл. в зависимости от модели.

IP-телефон фирмы Siemens

Подразделение Information and Communication Networks (IC Networks) концерна Siemens выпустило Ethernet-телефон HiNet LP 5100 IP (рис. 12.17). Этот аппарат представляет

собой многофункциональный телефон бизнес-класса со встроенным адаптером Ethernet, который обеспечивает прямое подключение к корпоративной ЛВС.

HiNet LP 5100 IP упаковывает речь в IP-пакеты и позволяет звонить на любой IP-телефон, через IP-шлюз на любой обычный телефон и на любой мультимедийный ПК, поддерживающий стандарт H.323.

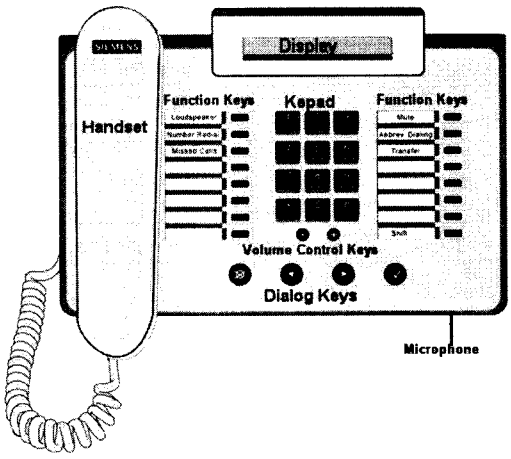


Рис. 12.17. IP-телефон HiNet LP 5100 фирмы Siemens

Пользовательский Cisco интерфейс OptiGuide дает возможность пользователю HiNet LP 5100 IP конфигурировать его посредством прокрутки меню и выбора на 24-символьном ЖК-дисплее необходимых функций. Ethernet-телефон концерна Siemens имеет, в частности, функции автоматического дозвона, набора номера при неснятой трубке, громкоговорящей связи, установки быстрого набора 16 программируемых номеров, отображения текущей даты и времени и сохранения информации (имена и IP-адреса звонивших) о 20 последних не принятых вызовах.

HiNet LP 5100 IP поддерживает стандарты H.323, H.225 и H.245, протоколы связи и управления TCP/IP, FTP, DHCP и SNTP, алгоритмы оцифровки речи G.711 (64 кбит/с) и G.723.1 (6,3 кбит/с), а также функцию активного эхоподавления. Его оптовая цена – 425 долл.

IP-телефоны компании Alcatel

В состав серии IP-телефонов Reflexes™ компании Alcatel входят две модели телефонов: Premium IP и Advanced IP. Обе модели телефонов могут подключаться к нескольким линиям, имеют громкоговорящую связь, набор без снятия трубки и набор по имени с помощью встроенной буквенно-цифровой клавиатуры. Однако первая модель Premium IP имеет меньше программируемых клавиш, дисплей меньшего размера и ориентирована на индивидуальное использование. Вторая модель Advanced IP предназначена для группового использования и обеспечивает выдачу на дисплей одновременно нескольких строк, контроль связи и фильтрацию звонков. Характеристики IP-телефонов серии Reflexes™ Models компании Alcatel приведены в табл. 12.10, а внешний вид – на рис. 12.18.

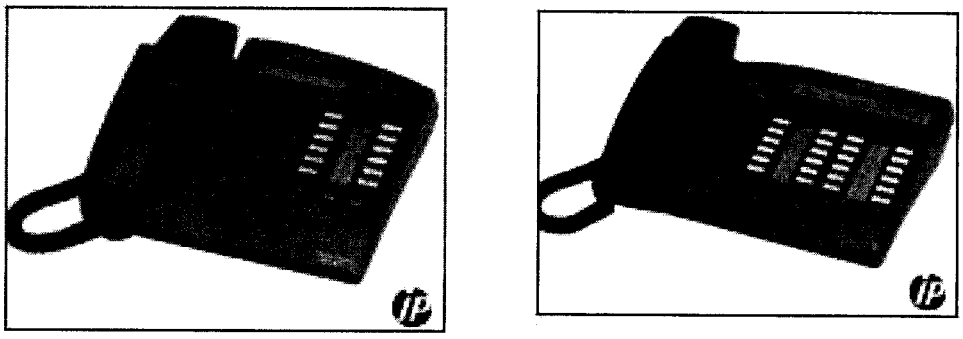
IP-телефон корпорации Pingtel

Основой IP-телефонов Xpressa корпорации Pingtel (США) является протокол SIP и открытые Java-интерфейсы программирования (рис. 12.19). Благодаря встроенной поддержке

IP-телефоны Xpressa смогут выполнять различные приложения или их части, например подключаемые программы, Java-аплеты и Java-сценарии. Обеспечена также их тесная интеграция с такими приложениями для настольных систем типа Outlook корпорации Microsoft. В телефонах имеется и целый ряд функций маршрутизации, включая идентификацию вызывающего абонента, переключение и ретрансляцию вызовов.

Таблица 12.10. Характеристики IP-телефонов серии Reflexes™ Models компании Alcatel

Характеристики телефонов	Premium IP	Advanced IP
Количество программируемых клавиш	12	24
Обслуживаемая нагрузка	Ориентирован на индивидуальное использование (мультили-	Ориентирован на групповое использование (мультилиния)
Размеры дисплея (строк × символов)	1×20	2×40 (с навигатором)
Наличие громкоговорителя	Да	Да
Набор без снятия трубки	Да	Да
Набор по имени	Да, (встроенная буквенно-цифровая клавиатура)	Да, (встроенная буквенно-цифровая клавиатура)
Наличие интерфейса к Advanced Communication	Да (интегрирован)	Да (интегрирован)



а) б)

Рис. 12.18. IP-телефоны Reflexes™ компании Alcatel: а) Premium IP; б) Advanced IP

Отличительными чертами телефонов на основе протокола SIP являются:

- встроенная поддержка Java; Java-интерфейсы прикладного программирования для телефонии;
- интеграция приложений для ПК с интерфейсами прикладного программирования JTAPI и Microsoft TAPI;
- графический интерфейс доступа к функциям ПК, встроенным в телефонный аппарат;
- традиционные и принципиально новые телефонные функции;
- поддержка функций обеспечения безопасности и качества обслуживания, включая DiffServ и MPLS.

Рис. 12.19. Внешний вид IP-телефона Xpressa корпорации Pingtel

Выполнение этих функций обеспечивает следующие преимущества для пользователей:

- открытая среда разработки приложений;
- доступ к библиотекам настольных систем; вызов абонента по его идентификатору URL, а также с помощью приложений установления связи;
- ускоренный вызов абонента, интуитивно понятный доступ к приложениям;
- поддержка функций выключения телефона без отключения абонента (Hold), пересылки и ретрансляции вызовов, ведения журнала телефонных переговоров, организации конференций и ряда других;
- защита ведущихся переговоров от прослушивания и высокое качество звука.

ПРИЛОЖЕНИЕ 1

Зарубежные провайдеры IP-телефонии
(источник: http://www.iptelephony.org/frame/providers.html)

Провайдер	Сеть	Услуги	Аппаратное обеспечение	Совместимость с H.323
Access Power	Africa, Belgium, Canada, Central America, Denmark, France, Germany, Ireland, Italy, Luxembourg, South America, Mexico, Netherlands, Puerto Rico, South America, Spain, Sweden, Switzerland, UK, USA	PH to PH, PC to PH, Fax	NetSpeak	Да
ACT Teleconferencing	Australia, Belgium, Canada, Europe, France, Germany, Hong Kong, Netherlands, UK, USA	PH to PH, Video	ACT Teleconferencing, Clarent	–
American Internet Communications	Argentina, Brazil, Chile, Peru, Venezuela	PH to PH	Cisco	Нет
AT&T Canada	Canada	PH to PH	Cisco	–
Avantel	Mexico	PH to PH, PC to PH	NetSpeak	–
Best Telephone Rates	Global	PC to PH	Net2Phone	–
Bezeq International	Israel	PH to PH	3Com	Да
Billion Telecom	Hong Kong	PH to PH	IPVoice	–
BIZTRANS	Australia, Brazil, Canada, China, France, Germany, Italy, Japan, Korea, Netherlands, Pakistan, Singapore, Taipei, Taiwan, UK, US, Venezuela	PH to PH, PC to PH, Fax	VocalTec	Да
Broadmedia	Asia, Israel, USA	PH to PH	Broadmedia	Нет
BT Ignite	Hungary & Czech Republic	PH to PH	Cisco, Clarent	–
Call Works	Global	PC to PH, Web	Call Works	–
Callrewards	Canada, USA	PC to PH, PC to PC	ITXC, NetSpeak	–
Callserve	London, Paris, Frankfurt, New York and San Francisco	PC to PH	NetSpeak	Да
Cesky Telecom	Belgium, Czech Republic, Denmark, Finland, Luxembourg, Norway, Sweden, Greece Portugal and Spain	PH to PH, PC to PH	Ursus Telecom	–
China Jitong	China	–	Clarent, Norsat	–
China Mobile	China	–	Clarent	–
China Telecom	China	–	Clarent, deltathree.com, RADVision & VocalTec	–

Провайдер	Сеть	Услуги	Аппаратное обеспечение	Совместимость с H.323
China Unicom	China	–	3Com, Cisco, deltathree.com, NetSpeak	–
Clariti Telecommunications International	Australia, Europe, USA	–	Cisco, ECI Telecom	–
Colt Telecom	Europe, USA	–	Cisco	–
Com Tech International	Denmark, England, France, Germany, Netherlands, USA	–	IPAXS	–
Comlink Switching	Asia, Latin America, USA	–	Nx Networks	–
CoolCall.com	Global	PH to PH	Cisco, Clarent	Да
Counsel Communications LLC	USA	PH to PH	Cisco	Да
Crys-Tel Telecommunications	Canada, Italy, Uruguay and US	PH to PH	Nokia, Nx Networks	–
Cybercall	Switzerland	–	Dialogic, GRIC	Да
Daci.Net	USA	PH to PH, PC to PH	Access Power VocalTec	Да
Davnet Limited	Asia, Australia, North America	–	Cisco, Davnet Limited, InnoMedia	Да
Delta Three	Global	PH to PH, PC to PH, PC to PC	Ericsson & VocalTec	Да
DeTeLine	Germany	–	Alcatel	–
Deutsche Telekom	Trial from New York to Australia, Brazil, Britain, Canada, China, France, Germany, Hong Kong, India, Israel, Italy, Japan, Mexico, the Netherlands, the Philippines, Russia, South Korea, Spain, Switzerland and Taiwan	–	VocalTec	–
Dialpad.com	USA	–	Cisco, Clarent	Да
Dial-Thru International	Argentina, Europe, USA	–	Mockingbird Networks	–
DigiNet	Brazil	–	Open Port	–
Digitcom	Australia, Germany, Indonesia, Japan, Korea, Russia, Taiwan, USA	PH to PH, Fax, Web	Digitcom, Natural MicroSystems, MicroSystems	–
Dohwa Operation Service	Seoul, Korea	PH to PH	Inter-Tel	Нет
Dostana	UK	–	Interline	Да
E2.Tele2.Tel	Switzerland	PH to PH	Ericsson	Да
eGlobe	Hong Kong, USA	–	Nuera	

Провайдер	Сеть	Услуги	Аппаратное обеспечение	Совместимость с H.323
Eircom	Ireland	–	Net2Phone	Да
Elvis Telecom	Russia	PH to PH	Clarent	Да
Equant	Global	–	Cisco	Да
EuroTel Praha	Czech Republic	PH to PH	–	Да
Evergroup	China, Taiwan, USA	PH to PH	Inter-Tel	Нет
Exit2Europe	The Netherlands, with plans for Australia, Canada, Indonesia, Japan and South Africa	PH to PH, PC to PH	VocalTec	Да
Exodus Communications	Global	–	Netergy Networks	–
EzyCom Communications	Hong Kong, USA	PH to PH, PC to PH	NetSpeak	Да
Firetalk	USA	PC to PH, PC to PC	dynamicsoft	Да
Firstnet Telephony Limited	UK	PH to PH	IPVoice	Да
FNet	Global	PH to PH	Franklin Telecom	Да
Gateway IP	Africa, Europe and the Middle East	–	Cisco, Mockingbird Networks, NeTrue	–
Gecco.net	Germany, the Middle East and Asia	–	Clarent	Да
Geonet LTD	Georgia	–	Cisco	–
Global Crossing	Atlanta, Chicago, Dallas, Denver, Kansas City, Rochester (NY) and Seattle	PH to PH	Sonus Networks	Да
Global Transmedia Communications	Brazil, Columbia, Peru, Venezuela, USA (Hackensack, Miami, New York, San Antonio, St. Louis)	PH to PH	Clarent	Да
Globaltron Communications	USA, Russia	–	Lucent	Да
Global Voice & Data Communications	London, Lebanon, Syria, Pakistan, India, UAE, Saudi Arabia, Egypt, Morocco, Palistine, Jordan, USA	–	Global Voice & Data	–
GlobalNet Telecommunications	Global	PH to PH, PC to PH, Fax	Dialogic	Да
Globe Telecom	Philippines	–	Cisco	–
GlocalNet	Great Britain, Netherlands, Spain, Sweden	PH to PH	Cisco	–
Golden Line	USA, Europe, Asia, South America and Africa.	PH to PH, Fax	ArelNet	Да
Golden Telecom	Russia, CIS	–	Cisco	–
High Speed Access	USA	Cable	Lucent	–
Halo Telecommunicaions	USA	–	Clarent, VocalTec	Да
HarvardNet	Northeastern USA	–	Cisco	–
I-Link	Europe/USA	PH to PH	I-Link, MiBridge	Да

Провайдер	Сеть	Услуги	Аппаратное обеспечение	Совместимость с H.323
i2line	South Korea (Seoul, Pusan, Ulsan, Kwang-ju Chung, Daejon, Daegu, Inchon)	PH to PH	Lucent	Да
iCall	U.S.	–	Cisco	Да
ID Telecoms	Asia, Africa, Middle East	–	Cisco	Да
iDial Networks	Australia, Belgium, Canada, France, Germany, Hong Kong, the Netherlands, Switzerland, UK, USA	–	SynapSys, Cisco	Да
IncomTel TG	Moscow, Canada, Israel, USA	PH to PH, PC to PH, Fax, Web	VocalTec	Да
INDD	Hongkong, Indonesia, Malaysia, Singapore, Taiwan and Thailand	–	Cisco, Vienna, VocalTec and Lucent	–
Infonet	Global	–	Cisco	–
Innofone.Com	Canada, USA	PH to PH, PC to PH	NetSpeak	Да
InnoMedia	Global	PH to PH, PC to PH	InnoMedia	Да
Intelligent Public Network	Australia	–	Interspeed	–
Interdata Engineering	USA, Europe, Russia, the Caribbean and Latin America	–	Lucent	–
Internet Data Systems	Poland	PH to PH	deltathree.com	Да
Internet PhoneCall	Global	PH to PH, PC to PH	VocalTec	Да
InternetConnect	USA	PH to PH	NetWorks Telephony	–
Internet Global Services	Texas, Denver, Seattle & Portland	PH to PH	Ericsson	Да
Inter-Tel	USA	PH to PH	Inter-Tel	Да
Interoute	Global	PH to PH	Cisco	–
Intercommunication American Systems	Brazil, Argentina, Chile, Paraguay, USA	–	Cisco, Vocaltec, Motorola	–
IP.COM	Italy	PH to PH	Better On-Line Solutions	Да
IP&P	Los Angeles, San Jose & Taiwan	PH to PH	IP&P	–
IPfon	Taiwan	–	IPfon	–
iPhoneline.com	Mexico, USA	–	iPhoneline.com	–
IPirion AG	Europe	PH to PH	Cisco	–
IPOperations	Australia, Canada, Europe, Korea, Middle East, New Zealand, South America, Taiwan, USA	PH to PH, PC to PH, Web	Cisco, Hypercom, Nuera & VocalTec	Да
iPriumus	Canada	PH to PH	Cisco	–

Провайдер	Сеть	Услуги	Аппаратное обеспечение	Совместимость с H.323
IPw@Да	France	–	Clarent	Да
Ireland On-Line	Ireland	PC to PH, Fax	NetWorks Telephony	–
ISF Corporation	Japan	PH to PH, PC to PH	VocalTec	–
ISPtel.com	Asia, Europe, USA	PH to PH	Ascend	–
Japan Telecom	Japan	PH to PH	Fujitsu Business Systems	–
Jitong	China	PH to PH	Cisco, Clarent	–
Junroo NetCommunications	Asia, Europe, Latin America, USA	PH to PH	Cisco	Да
Justice Internet Telephone	Singapore, Indonesia, Malaysia, Mexico, Panama, Dominican Republic, Venezuela, Argentina, Peru, Chile, Nigeria, and Lithuania	PH to PH	Cisco	Да
Keppel Communications	Singapore	–	ArelNet	–
Keystone Port Terminal	Japan	–	NeTrue	–
KPN Telecom	Netherlands	PH to PH, Web	eFusion & Clarent	Да
Latinode	Colombia, Guatemala, El Salvador, Ecuador, Nicaragua and Venezuela	PH to PH, PC to PH, Fax	deltathree.com	–
Liberty One	Australia, New Zealand	PH to PH	Franklin Telecom	Да
Macrocom	Rep. of Georgia, Tbilisi	PH to PH, PC to PH, Web	VocalTec	Да
Marconi Comunicacoes Internacionais	Portugal	PH to PH PC to PH	Net2Phone, VocalTec	Да
Maxcall.com	Global	PC to PH	Net2Phone	–
MediaNet	Poland	–	Cisco, GRIC	–
mediaWays GmbH	Europe	–	3Com, Digi International	–
MegaWorld	Caribbean, Central and South America	PH to PH	Mockingbird Networks	–
MegaHertz Communications	USA	PH to PH	ECI Telecom	–
MegsINet	USA	–	Cisco, Nortel Networks	–
MEMTel	UK	–	MEMTel	–
MessageClick	USA	–	Genuity	–

Провайдер	Сеть	Услуги	Аппаратное обеспечение	Совместимость с H.323
MicroWorld	Hong Kong	–	iBasis & VocalTec	Да
Mondiacom	France	–	Planet Telecom	–
Mundi Telecom	Spain	–	Cisco	–
MyFreeLD	USA	PC to PH	MyFreeLD	–
MyOperator	USA	PH to PH, PC to PH	VocalTec	Да
Net2Phone	Global	PH to PH, PC to PH, Fax, Web	IDT, Net2Phone	–
Net Communications	Africa, China, Europe, South America and New York	PH to PH, Videoconference	Motorola	–
NetPhone	Hungary	PH to PH, PC to PH, Fax	Computer Protocol Malaysia	Да
Nettel Global Communication	Australia, Thailand, Hong Kong, Malaysia, Singapore, Vietnam	–	Nettel Global	–
Nexbell	USA	–	Cisco	Да
Nexcom	Bulgaria, Estonia, Lithuania & Macedonia	PH to PH, PC to PH, PH to PC, Web	Cisco, VocalTec	Да
Nextra	Norway	–	Clarent	Да
Nigerian Telecommunications	Africa	–	deltathree	–
North American Gateway	Canada	–	Mockingbird Networks	–
NorthVoice Communications	Australia, Canada, Hong Kong, South Korea, USA	PH to PH, PC to PH	Lucent	Да
Ola Internet	Spain	PH to PH	Lucent	Да
P2P Tel.Com	Malaysia & Singapore	PH to PH	Net2Phone	–
Pagoo	USA	–	Cisco, NetCentrex	Да
PC2Call	UK	PC to PH, Web	PC2Call	–
Peoplecall.com	Spain	PC to PH	NetSpeak	Да
Philippine Long Distance Telephone	Philippines	–	deltathree.com, ITXC	–
Phone Comp@ny	Belgium	PH to PH, PC to PH, Fax	Aplio	–
Phonecalls.com	Asia Pacific, USA	PC to PH, Web	CC&T Technologies, Nuera, Quintum Technologies	–
PhoneFree.com	USA	PH to PH, PC to PH	ITXC	–

Провайдер	Сеть	Услуги	Аппаратное обеспечение	Совместимость с H.323
POPTEL	Germany, USA, France, and Switzerland	PH to PH	Clarent	–
Rapid Link Communications	Asia, Europe, USA	PH to PH	Clarent	Да
Rayes Technology Group	China	PH to PH	Netrue	–
Red Cube Group	Europe	PH to PH	I-Link	Да
Rhinos	France, Germany, Italy, UK	PH to PH	deltathree	Да
RinoTel	Russia	PH to PH, PC to PH	VocalTec	Да
RMI.NET	Denver,Boulder and Colorado Springs to USA	PH to PH	Nokia	–
Shandong Sanlian Electronic Information	Plans for Jinan, China	PH to PH	Ericsson	–
SITEC	Russion Federation	PH to PH	deltathree.Com	–
Somnet	Sweeden, Great Britain & the Netherlands	PH to PH	GlocalNet	Нет
Sovintel	Russia – Moscow, St. Petersburg	PH to PH, Fax	Cisco	Да
STAR-NET	Japan	PH to PH, Fax	GRIC	–
Star Telecommunications	Australia, Germany, England, South America, Spain, USA	PH to PH	Clarent	Да
SurfEU	Austria, Germany, Finland, Sweden, Switzerland	PH to PH, PC to PH	deltathree.com	–
Tario.net	Russia	PH to PH, PC to PH	VocalTec	Да
Tekson	China	PH to PH, PC to PH	InnoMedia	Да
Telecom Italia	Europe, Latin America, and the Mediterranean	–	Cisco	–
TeleGlobe	Global	PH to PH	Cisco	–
TeleMatrix	Canada, China, France, Hong Kong, Italy, Japan, Korea, Taiwan, USA	PH to PH	Cisco, NetSpeak	Да
Telenor Nextel	Norway	PH to PH, PC to PH	Delta Three	Да
TeleNova	Argentina, Brazil, Chile, Paraguay, Uruguay	PH to PH	Cisco, ITXC, NetSpeak	–
Telia	Scandinavia & Sweden	PH to PH, PC to PH	Cirilium, Cisco, Clarent Ericsson, Nortel	–
TheStream.com	Buenos Aires, Frankfurt, Geneva, Johannesburg, Lima, Miami, Moscow, Paris, Tokyo	PH to PH, PC to PH, Web	Cisco	–
Thyssen Telecom AG	Germany	PH to PH, Web	Siemens	Да
US Digital	USA	PH to PH	Lucent	–

Провайдер	Сеть	Услуги	Аппаратное обеспечение	Совместимость с H.323
USA Global Link	Australia, Brazil, the Benelux countries, Chile, England, France, Hong Kong,Indonesia, Japan, Korea, London, New York, Seattle, South Africa, Tokyo	PH to PH	3Com	Да
Virtual Network	USA	PC to PH	Lucent	–
VirtualPTT	Global	PH to PH, PC to PH	VocalTec	Да
Vitech America	USA, South America	PH to PH	Cisco	Да
Voicenet	USA	PH to PH	Cisco	–
Vocall	USA	PH to PH, PC to PH, Web	Lucent	Да
Vocalscape	USA	PH to PH, PC to PH, Web	Vocalscape	–
WeAreTheWorld	Carribean, Europe, Mexico, South America	PC to PH, PH to PH	VocalTec	Да
Welltel.net	Asia, USA	–	Natural MicroSystems, Welltel.net	Да
WHEREVER.net	China, Hong Kong, Japan, Singapore, USA	PH to PH, Fax	Dialogic	Да
WorldQuest Networks	Lating America, USA	PH to PH, PC to PH, Fax	InterVoice	–
World Interactive Network(WIN)	Brazil, China, Costa Rica, Haiti, Israel, Japan, Malaysia, Russia, South Africa, Thailand, Turkey, USA	PH to PH, PC to PH	VocalTec	Да
X/IP	Africa, Central & Eastern Europe, USA	PH to PH	ECI Telecom	–
Xplorium	Africa, Caribbean, Europe, Middle East, South America, USA	–	Cisco, Clarent	–
ZeroPlus.Com	Global	PH to PH, PC to PH	ZeroPlus.Com	Да

В таблице использованы следующие обозначения услуг:

PH to PH – звонок «телефон-телефон»
PC to PH – звонок «компьютер-телефон»
Web – звонок с Web-сервера на телефон
Fax – передача факсов

ПРИЛОЖЕНИЕ 2

Российские провайдеры IP-телефонии
(источник: www.comptek.ru)

Провайдер	Оборудование	Расположение собственных серверов	Прием трафика	Предоставляемые услуги					Комментарии
				1	2	3	4	5	
Tario Trading	DM3	Сеть объединяет порядка 55 городов в России и СНГ и имеет выход на 237 стран мира	Любой город мира	К	К	К	К	Т	Фирма координирует работу сети Tario.Net
ЗАО «Корпорация ОСС»	VGW, 150 цифровых линий	Москва, С.-Петербург, Нью-Йорк и др. Более 50 узлов на территории СНГ	Весь мир	К	К	К	К	К	Имеет связь с сетями: ITXC, Teleglobe и др. Бесплатный биллинг. В сети имеется роуминг
RGC	VGW, Cisco AS5300, 120 цифровых линий	Москва, С.-Петербург, Южно-Сахалинск, Владивосток, Хабаровск, Новосибирск, Самара, Пермь, Липецк, Чита, Краснодар, США (Нью-Йорк), Германия (Мюнхен, Берлин, Франкфурт)	Любой телефон в мире	К	К	К	К	К	Фирма занимается техническим развитием и координинацией работы сети
Satellite	VTG	Торонто		Т	К	N/A	К	К	Бесплатно подключает к своему серверу
«Дион»	Cisco	Челябинск, Екатеринбург	Весь мир	К	К	К	К	Т	Есть биллинговая система собственной разработки
ОАО «Оренсот»	VTG (8 линий), Cisco 2610 (4 ан. линии)	Оренбург. Планируются другие крупные города Оренбургской области	Россия + 300 стран мира	К	К	П	П	П	
Деловая Сеть – Иркутск	VTG, 8 аналоговых линий	Иркутск, Усолье-Сибирское Планируется Ангарск	Москва, С-Петербург, Рига, Красноярск, Чита, Хабаровск и др. Во все страны мира	К	N/A	N/A	К	Т	

Провайдер	Оборудование	Расположение собственных серверов	Прием трафика	Предоставляемые услуги					Комментарии
				1	2	3	4	5	
ЗАО «ИнкомТел ТГ»	VGW, 30 цифр. линий. VTG, 8 анал. линий	Москва	Весь мир	К	К	Т	К	К	Партнер ITXC
НП «Магнитоцентр»	VTG, 4 аналоговые линии	Магнитогорск	Россия, страны мира	К	К	N/A	Т	П	
SITEK	Ericsson IPTC, 260 цифровых линий Cisco	Москва, Санкт-Петербург, Самара, Н. Новгород, Саранск, Кишинев, Киев, Воронеж, Архангельск, Северодвинск, Вологда	Любая точка мира	К	К	К	К	П	Автоматический роуминг. Тарификация звонка – 6 с.
ЭЛВИС-ТЕЛЕКОМ	Clarent Gateway, 60 цифровых линий	Москва	Россия, весь мир	К	К	К	N/A	N/A	250 стран. Тарификация звонка – 1 с. Собств. канал 8 Мбит/с, включ. в сеть Телия (Швеция)
SCS-ABADON Ltd.	IPStar-2000, IPStar-700, IPStar-800	Москва, Seattle (USA), Bulgaria (Varna, Plovdiv, Sofia, Ruse, Lovech)		N/A	К	N/A	К	N/A	
ЗАО «НИАВЕК»	н/д	Москва	Tario.Net	Т	К	N/A	Т	N/A	Прямой канал на сервер Tario.Net 128 кбит/с
КубаньСвязь Сервис	VGW	Краснодар	Любой телефон в мире	RGC	К	К	К	К	
Сахалинская Сетевая Связь	VGW	Сахалин	Любой телефон в мире	RGC	К	К	К	N/A	
United World Communications	VTG, 12 цифр. линий. Motorola 6560, 96 цифр. и 16 анал. линий	Вашингтон (США), Москва, Санкт-Петербург. Планируется Рига, Прага	Весь мир	К	К	N/A	К	Т	Имеет прямой канал связи из США в Москву и в С.-Петербург
Единство-Телеком	DM3, 8 аналоговых линий	Иркутск	Большинство крупных городов в России	N/A	К	К	N/A	N/A	

Провайдер	Оборудование	Расположение собственных серверов	Прием трафика	Предоставляемые услуги					Комментарии
				1	2	3	4	5	
Октагон Технолоджис	VTG, 8 аналоговых линий	Санкт-Петербург	Tario.Net	К	К	N/A	К	К	Канал на Москву 128 кбит/с
ОАО «Ринет»	VTG на 8 линий Сервер Cisco AS5300 на 30 линий	Новосибирск	Москва, весь остальной мир	К	К	К	Т	N/A	
Логос-Линк	DM3, 8 аналоговых линий	Ижевск	Tario.Net	К	К	П	N/A	N/A	
АК Мобилтелеком	VGW, 8 аналоговых линий	Улан-Удэ	Весь мир	Т	К	К	К	Т	
ООО «Коммуникации ЭКС-НЭТ» LLC X-Net Communications	VGW, 8 аналоговых линий	Липецк	Любой телефон в мире	RGC	Т	Т	Т	Т	
Mellanta Ltd.	VGW, 60 цифровых линий	Москва	Весь мир	К	К	К	Т	Т	
Ринотел Северо-Запад	VGW	Санкт-Петербург	Любой телефон в мире	RGC	К	К	К	К	
Stream Line Communications	VGW, 48 аналоговых линий	Москва, Благовещенск	Весь мир	К	К	N/A	N/A	N/A	Является координатором сети FELINE по России и странам СНГ, обладает своим биллингом
VISS	VGW, 60 цифр. и 8 анал. линий DM3, 60 цифр. и 8 анал. линий	Москва, Рига	Весь мир	К	К	К	N/A	N/A	
ООО «Спектр-Интел»	DM3, 8 аналоговых линий	Челябинск	Весь мир	К	К	К	К	N/A	
ЗАО «Крафтсвязь-Новосибирск»	DM3, 16 аналоговых линий	Новосибирск	Зарубежье, города сети	К	К	К	Т	Т	

Провайдер	Оборудование	Расположение собственных серверов	Прием трафика	Предоставляемые услуги					Комментарии
				1	2	3	4	5	
			Tario, Сибирь						
ВИП-Центр	Cisco AS5300, 30 цифровых линий	Казань	Россия, весь мир	К	К	К	Т	П	
Intercall	DM3, 4 цифровые и 4 аналоговые линии	Москва, планируется С.-Петербург	Весь мир	К	К	К	К	К	
РОСНЕТ С.-Петербург	Cisco, 30 цифр. линий, 4 аналоговые линии	С.-Петербург	Весь мир	К	К	К	П	П	
Аркон ТМЛ	Cisco, 30 цифр. линий	Москва, Нью-Йорк, Белгород, Запорожье, Пермь, Пенза	Весь мир	К	К	К	К	N/A	
ЗАО «Диджитал Нетворк»	Cisco AS5300, 60 цифровых линий	Москва, С.-Петербург	Весь мир	К	К	К	Т	П	
ООО «ИЖКОМ»	Cisco 3661, 60 цифровых линий	Ижевск	Весь мир	П	К	К	П	П	
ИНФОСВЯЗЬ	VTG, 30 цифровых линий	Новосибирск	Западная Сибирь	П	К	К	–	–	
ЗАО «Интернет-Архангельск»	Lucent Definity, 60 цифр. и 24 анал. линии; Cisco 3640, MC3810, 24 цифр. и 10 анал. линий	Архангельск, Северодвинск, Вологда	Весь мир	К	К	К	Т	П	
Сатком-Тел Петербург	Cisco 5300, 30 цифровых линий	Санкт-Петербург	Санкт-Петербург	Т	К	К	Т	П	
ЗАО «ПК Мостком»	Cisco 5300, 3600 (30 цифр. и 16 анал. линий)	Москва	Любая точка мира	К	К	К	–	–	
Ариадна-линк	Cisco3640, 6 анал. линий	Выборг	–	П	К	Т	П	П	
Коммуникационная компания МАРК-	Cisco 5300 + 3640 30 цифр. линий, 4	Ижевск	Ижевск	Т	К	Т	Т	П	

Провайдер	Оборудование	Расположение собственных серверов	Прием трафика	Предоставляемые услуги					Комментарии
				1	2	3	4	5	
ИТТ	анал. линии								
Matrix Telecom	Cisco, 60 цифр. линий	Москва	Весь мир	–	–	–	–	Т	
ООО Рикоп	Cisco, 4 анал. линии	Новосибирск	–	Т	Т	Т	Т	Т	

В таблице использованы следующие обозначения услуг:

Нумерация подколонок в колонке «Предоставляемые услуги»

1 – Подключение чужих телефонных серверов к сети
2 – Звонок «телефон-телефон (компьютер)»
3 – Звонок с факсимильного аппарата на факсимильный аппарат
4 – Звонок «компьютер-телефон»
5 – Звонок с Web-сервера на телефон

Обозначения в колонке «Предоставляемые услуги»:

К – Работа в коммерческом режиме
Т – Работа в тестовом режиме
П – Работа в стадии планирования
N/A – Неприменимо, либо фирма этим не занимается
RGC – Компания является оператором сети Rinotel и подключает чужие серверы через головную компанию

Обозначения в колонке «Оборудование»:

н/д – Нет данных
Cisco – Cisco
VGW – VocalTec Ensemble Architecture
VTG – VocalTec Telephony Gateway 3.x
DM3 – Dialogic DM3/IPLink
Lucent – Lucent Technologies

ПРИЛОЖЕНИЕ 3

ХАРАКТЕРИСТИКИ СИСТЕМ БИЛЛИНГА И МЕНЕДЖМЕНТА ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-ТЕЛЕФОНИИ

Название системы	Фирма, страна	Назначение системы	Форма оплаты	Идентификация в PMB (роуминг)	Авторизация в PMB (доступ к услугам)	Поддержка шлюзов IP-телефонии	Масштабируемость
IMS 3.1 (Internet Management System)	Belle System A/S, Дания	Биллинг и менеджмент сети	Дебетовые (предоплаченные) и кредитные карты	+ (в т.ч. через Radius Server)	+ (в т.ч. через Radius Server)	Cisco	Более 20 млн. счетов и 1 млн. одновременных пользователей
BizBill	Biztrans, США	Биллинг IP-услуг	Кредитные карты	–	–	Vocaltec	20 шлюзов и 10 тыс. пользователей
BillxPress	Cosmobridge, Корея	Центральная биллинг система на несколько узлов	Предоплаченные карты	+	+	Cosmobridge Telephony Gateway	Н/д
NET-CHARGER	ЕНРТ, Швеция-США	Распределенная система биллинга и менеджмента для всех IP-услуг	Любая, в т.ч. предоплаченные карты	+	+	Любые	Н/д
Tempest DVG AMAS&Billing	Franklin Telecom, США	Система авторизации пользователей и биллинга	Любая в т.ч. дебетные и кредитные карты	+	+	Tempest	Н/д
eBill	Infozech, Индия	Система менеджмента и биллинга IP-услуг для операторов связи	Любая, в т.ч. дебетные и кредитные карты	+	+	Н/д	От 10 тыс. до 2 млн. записей о разговорах (CDR) в месяц
RODOPI	Intranet Software, США	Система менеджмента и биллинга IP-услуг	Любая, в т.ч. дебетные и кредитные карты	Через RADIUS server	+	Любые	Н/д
Arbor Internet	Kenan Systems, США	Комплексная платформа биллинга любых услуг связи	Любая, в т.ч. дебетные и кредитные карты	+	+	Любые	Н/д
iPhoneEX	MIND CTI, Израиль	Система менеджмента и биллинга IP-телефонии	Любая, в т.ч. дебетные и кредитные карты	+	+	Любые (VocalTec, Ascend, Lucent, Arelnet)	От 100 до 1 млн. пользователей

Название системы	Фирма, страна	Назначение системы	Форма оплаты	Идентификация в PMB (роуминг)	Авторизация в PMB (доступ к услугам)	Поддержка шлюзов IP-телефонии	Масштабируемость
OpenInformer	uni-X Software AG, Германия	Система менеджмента и биллинга IP-услуг	Любая, в т.ч. дебетные карты	+	+	Cisco	От мелких провайдеров до крупных операторов связи
Infranet IPT	Portal, США	Система менеджмента и биллинга IP-телефонии	Любая, в т.ч. дебетные и кредитные карты	+	+	С любыми	Более 1 млн. пользователей
IAF Horizon	Solect Technology Group	Система менеджмента и биллинга IP-услуг	Любая, в т.ч. дебетные карты	+	+	Cisco Ericsson	Н/д
Talking NT Enterprise SQL	Telephony Experts, США	Программная платформа IP-коммутации и биллинга	Любая, в т.ч. дебетные карты	–	–	Аппаратное обеспечение Dialogic	Н/д

Название системы	Менеджмент сетевых элементов	Поддержка QoS	Поддержка мультимедийных услуг	Поддержка вторичных провайдеров	Управление услугами со стороны пользователя	Интеграция с финансовыми системами	Аппаратно-программная платформа	Использование на сетях
IMS 3.1 (Internet Management System)	+ (ПО Atlantech Technologies, Orchestream)	+ (через Cisco MPLS VPN)	Голос, данные, видео, e-mail, e-commerce	+ (доступ через платформу SilverStream)	Через CORBA и WEB интерфейс	Oracle Financials, SAP, EHPT, Kenan, Saville	Oracle 8, UNIX, HP, SUN, CORBA	Европа, Ближний Восток Африка, Азия
BizBill	–	–	–	–	Доступ только к счетам, регистрация через WEB	–	Win NT/95	США
BillxPress	–	–	Голос, данные, факс	+ (платформа клиент-сервер)	–	Н/д	MS NT Server 4.0/Oracle 7.3, MS Win95 or NT Workstation	Азия
NET-CHARGER	–	Н/д	Любые IP-услуги в т.ч. электронная коммерция	+	WEB-интерфейс	+	Серверы: HP-UX, HP9000, Solaris, Sun, Oracle, UNIX, Клиенты: WinNT Win98, Web	Более 20 систем в мире (контракт с провайдером AB Lietuvos)

Название системы	Менеджмент сетевых элементов	Поддержка QoS	Поддержка мультимедийных услуг	Поддержка вторичных провайдеров	Управление услугами со стороны пользователя	Интеграция с финансовыми системами	Аппаратно-программная платформа	Использование на сетях
Tempest DVG AMAS&Billing	–	–	Голос, факс	Только ресселеров	+	Н/д	WinNT SQL database	
eBill	–	–	Голос, факс, голосовая почта, услуга 800, электр. платежи и др.	+	–	Система электронных платежей по кредитным картам IC Verify	Server, MS SQL Client Win95/Win NT4.0	Н/д
RODOPI	Н/д	Н/д	Голос, факс, электронная почта, электронные платежи и др.	+	WEB-интерфейс	Система электронных платежей по кредитным картам IC Verify	Server UNIX/NT	Более 2300 POPs в США, Канаде, Мексике, Австралии
Arbor Internet	Н/д	Н/д	Любые услуги в т.ч. широкополосные, мобильные, беспроводные, Интернет	Н/д	WEB-интерфейс	Н/д	Server UNIX Oracle/Sybase SQL DB Client WinNT	Н/д по IP-телефонии
iPhoneEX	–	–	Голос, факс	+	Доступ к счетам через WEB-интерфейс	–	Win NT4	Bell Atlantic, China Unicom, Telia Light, Deutsche Telecom (pilot)
OpenInformer	+	Н/д	Голос, факс, e-mail, видео, электронная коммерция и др.	+	+	А также с ERP-пакетами (SAP R/3)	UNIX, SQL DB Oracle, Ingres, Informix, Sybase	Германия, Великобритания
Infranet IPT	–	–	Голос, факс	+	WEB-интерфейс	Интегрируется с MS Commercial Internet System, Netscape SuiteSpot	UNIX, Win NT, Sun/Solaris Oracle/ MS SQL server	США, Европа, Юго-Восточная Азия
IAF Horizon	–	–	Голос, факс, видео, e-mail	+	Н/д	Н/д	Oracle	AT&T Canada, BT, Tele Danmark, Telecom Eircom, Saritel (Telecom Italia), Swiss Online/ Cablecom
Talking NT Enterprise SQL	–	+	Голос, факс, голосовая почта, электронная коммерция и др.	–	–	–	WinNT MS SQL Server	Н/д

ПРИЛОЖЕНИЕ 4

ШЛЮЗЫ IP-ТЕЛЕФОНИИ

(источник: http://www.iptelephony.org/GIP/vendors/gateways/)

Производитель	Продукт	Количество портов	Операционная система	Поддержка Fax	Поддержка H.323	Поддерживаемые протоколы
3Com	Total Control 1000	До 300	–	да	v2	SIP
	Total Control 2000	До 672	–	да	да	Megaco
ACT Networks	ServiceXchange-10	До 120	–	да	да	–
Advanetced Telesoft Limited	AT323 VoIP Gateway	До 120	Win NT	да	да	–
	ATS CP9000	До 360	Win NT	да	да	–
Anatel Communications	MB-24	До 24	–	да	да	MGCP
	MB-48	До 48	–	да	да	MGCP
	MB-96	До 96	–	да	да	MGCP
	MB-192	До 192	–	да	да	MGCP
ArelNet	i-Tone Pro	До 60	Win NT	да	v2	MGCP-SIP
	i-Tone Primo	До 120	Win NT	да	v2	–
	i-Tone Prime	До 720	Win NT	да	v2	MGCP-SIP
Better On-Line Solutions	TeleLynk	До 90	Win 95, 98, NT	да	да	–
Broadmedia	RMT-12	12	–	–	да	MGCP-SIP*
Cheap Call	Cheap Call	4-128	Win 95, Win NT	–	нет	–
Cirilium	Media Gateway 2000/2500	2	–	да	да	MGCP-SIP*
	Media Gateway 4000	До 120	–	да	да	MGCP-SIP*
	Media Gateway 6000	До 240	–	да	да	MGCP-SIP*
	Media Gateway 6200	До 240	–	да	да	MGCP-SIP*
Cisco Systems	2600 Series	2-48	–	да	да	–
	3660 Series	2-288	–	да	да	–
	AS5300	48-96	–	да	да	–
	7200 Series	48-720	–	да	да	–
	7500 Series	48-720	–	да	да	–
	AccessPath-VS3	48-1260	–	да	да	

Производитель	Продукт	Количество портов	Операционная система	Поддержка Fax	Поддержка H.323	Поддерживаемые протоколы
Clarent	Gateway 100	4-30	Win NT	да	да	MGCP
	Carrier Gateway	8-120	Win NT	да	да	MGCP
	Gateway 400	24-120	Win NT	да	да	MGCP
	Gateway 1200	До 360	Win NT	да	да	MGCP
Com-Match	Duet 6001	До 120	–	да	да	MGCP-Megaco
	Duet 6002	До 120	–	да	да	MGCP-Megaco
ComGates Communications	CGAN-2000	До 150	Win NT	да	да	SIP
	CMGW-5000	До 576	Win NT	да	да	–
Cosmobridge	CTG2000	4-24	–	да	да	–
	CTG3200	До 240	Win NT/Solaris	да	да	–
	CTG3400	–	Win NT	да	v2	–
Computer Protocol Malaysia	CpIP VoiceGateway	2-16	Win 95, Win NT	да	да	–
CyberFax	Gateway	До 120	Win NT	да	да	–
Dialogic	DM3 IP Link	До 120	Solaris, Win NT	да	да	MGCP-SIP
Digi Europe	NetBlazer 8500	До 120	Unix	нет	да	–
ECI Telecom	ITX 180	До 180	–	да	да	MGCP
	ITX 1000	До 480	–	да	да	MGCP
Engage Communication	IP Tube	До 24	–	–	–	–
Ericsson	WebSwitch 100	2-4	–	да	v2	–
	WebSwitch 100 IP Extension	4	–	да	v2	–
	WebSwitch 2000	До 32	–	да	v2	–
	IPT	До 780	Win NT	да	да	–
FastComm	MetroLan	3	–	–	–	–
	GlobalStack-EX	До 120	–	–	–	–
Franklin Telecom	Breeze	2	Linux	да	да	–
	Tempest	До 96	Linux	да	да	–
	Typhoon	До 192	Linux	да	да	–
Innomedia	InfoGate 1000	4	Win NT	да	да	–
	InfoGate 3010	4-16	Win NT	да	да	–

Производитель	Продукт	Количество портов	Операционная система	Поддержка Fax	Поддержка H.323	Поддерживаемые протоколы
IntelliNet	SS7oIP Gateway	До 128	Win NT, UNIX & Solaris	нет	нет	–
Intelesys International	Intele-Gate Bantam	2	–	да	да	–
	Intele-Gate Deluxe	До 360	–	да	да	–
	Intele-Gate Gold	До 840	–	да	да	–
Intelliswitch	iSwitch	8-150	Win NT	да	да	–
InterTel	InterPrise 400	До 4	Win 95, 98, NT	да	да	–
	InterPrise 2400	До 24	Win 95, 98, NT	да	да	–
	InterPrise 3200D	До 32	Win 95, 98, NT	да	да	–
	InterPrise 128D	До 128	Win 95, 98, NT	да	да	–
	Vocal'Net 3200S	От 8 до 32	Win 95, 98, NT	да	да	–
	Vocal'Net 9600S	До 96	Win 95, 98, NT	да	да	–
	Vocal'Net 3200D	До 128	Win 95, 98, NT	да	да	–
	Vocal'Net 128D	До 128	Win 95, 98, NT	да	да	–
Interline	Analogue Gateway	До 20	Unix	нет	да	–
	Digital Gateway	До 30	Unix	нет	да	–
i-p-tel	Portline	До 120	–	да	да	–
	Varigate	От 30 до 120	–	да	да	–
IPAxess	VocalWare IP Server	До 256	–	–	да	–
IP Voice	SuperConnect	До 120	–	да	да	–
	UltraConnect	480	–	да	да	–
IPAXS	OmniAXS GSP 2000	–	–	да	да	–
	OmniAXS GSP 6000	–	–	да	да	–
	OmniAXS GSP 14000	До 420	–	да	да	–
iTOPIA	Gateway	До 240	–	да	да	SIP
ITXC	SNARC	До 120	–	да	да	–

Производитель	Продукт	Количество портов	Операционная система	Поддержка Fax	Поддержка H.323	Поддерживаемые протоколы
Latic	LATNET 120	До 12	–	да	–	–
	LATNET 240	До 24	–	да	–	–
Lucent	MultiVoice for the MAX	120	TAOS	да	да	–
	MultiVoice for the TNT	До 672	TAOS	да	да	–
	MultiVoice for the APX 8000	От 192 до 2688	TAOS	да	да	–
Mariposa Technology	ATX50	До 60	–	да	да	–
	ATX100	До 60	–	да	да	–
	ATX150	До 120	–	да	да	–
MasterMind Technologies	MasterVox	До 96	Win NT	да	да	–
Mediatrix Telecom	APA III-1FXS	1	–	да	да	MGCP-SIP
	APA III-4FXS	До 4	–	да	да	MGCP-SIP
Memotec	CX800	2	–	да	да	–
	CX950	До 30	–	да	да	–
	CX960	До 60	–	да	да	–
	CX2000	До 360	–	да	да	–
MICOM	V/IP Phone/Fax IP Gateway	4 - 30	DOS, NetWare, Win 95, Win NT	да	нет	–
	Passport 4400	До 30	–	да	G.729	–
Mitel	Ipera 2000	384	Win NT	да	да	–
	Ipera Applications Gateway	До 256	Win NT	да	да	–
Mockingbird	Nuvo200	От 24 до 240	Solaris	да	да	–
	NuvoStream 3000	От 96 до 1680	Solaris	да	да	–
Motorola	Vanguard 320	До 4	–	–	–	–
	Vanguard 6435/6455	От 2 до 60	–	да	v2	–
MultiTech Systems	MVP200	2	–	да	да	–
	MVP400	4	–	да	да	–
	MVP800	8	–	да	да	–
	MVP2400	24	–	да	да	–
	MVP3000	30	–	да	да	–

Производитель	Продукт	Количество портов	Операционная система	Поддержка Fax	Поддержка H.323	Поддерживаемые протоколы
net.com	Shout500	–	–	да	нет	–
	Shout1100	До 240	–	да	да	–
N-Soft	N-Switch	–	–	да	да	–
NETPBX	NetPBX IT Gateway	4-24	Win	–	нет	–
Netergy Networks	Symphony Gateway	4	–	–	да	–
Netrix	Network Exchange 2210	–	–	да	да	–
	Network Exchange 2214	До 30	–	да	да	–
	3000 Series	–	–	да	да	–
NeTrue	NeTrueLink	От 4 до 32	Win NT/Unix	да	да	–
	NeTrueCom	До 120	Win NT/Unix	да	да	–
NewMi	IT Gateway	–	–	–	–	–
NexTone	iEdge 500	2	–	да	v2	MGCP-SIP-iNOW!
	iEdge 510	2	–	да	v2	MGCP-SIP-iNOW!
	iEdge 1000	120	–	да	v2	MGCP-SIP-iNOW!
Nortel Networks	Business Communications Manager	–	–	да	–	–
	Centrex Unlimited	–	–	да	–	–
	Communications Server 2000	–	–	да	–	SIP
	Communications Server 3000	–	–	да	–	SIP
	Cornerstone Host Digital Terminal	До 3360	–	да	–	–
	Cornerstone PacketPort	–	–	да	да	DOCSIS 1.1
	CVX 600	До 612	–	да	–	–
	CVX 1800	До 2688	–	да	–	–
	CVX SS7 Gateway	–	–	–	–	–
	IPOffice	До 50	–	да	–	–
	Succession Solutions	–	–	да	–	SIP
	Succession Cable Media	–	–	да	–	–
	Succession Local Line	–	–	да	–	–
	Succession Local Tandem	–	–	да	–	–
	Universal Audio Server	От 96 до 4000	–	да	–	–

Производитель	Продукт	Количество портов	Операционная система	Поддержка Fax	Поддержка H.323	Поддерживаемые протоколы
	V/IP Phone/Fax IP Gateway	–	–	да	–	–
Nuera	f50ip	4	–	да	да	MGCP-SIP
	f200ip	До 30	–	да	да	MGCP-SIP
	f200SIP	–	–	да	да	MGCP-SIP
	ORCA GX-8	До 480	–	да	да	MGCP-SIP
	ORCA GX-21	До 2040	–	да	да	MGCP-SIP
Nx Networks	2210	До 10	–	v2	да	–
	2214	До 10	–	v2	да	–
	3000	До 30	–	v2	да	–
	6000	До 120	–	yv2	да	–
Oki Network Technologies	BV1250	4	–	да	–	–
OzTel	Gateway	2	Win 95, NT	да	да	–
PacketPort.com	VoicePak	От 2 до 8	–	да	да	MGCP
	DataCrate Gateway	До 96	–	да	да	SIP
Performance Technologies	MicroLegend 300	От 2 до 24	–	–	нет	–
	MicroLegend 4000	До 240	–	–	нет	–
Petacom	Stargate	До 120	Windows NT	да	да	–
Taqua Systems	Open Compact Exchange	До 384	–	–	да	–
QuesCom	QuesCom 400	–	–	–	–	–
	QuesCom 500	24	Win NT	да	да	MGCP-SIP
	QuesCom 600	До 120	Win NT	да	да	MGCP-SIP
	QuesCom 700	240	Win NT	да	да	MGCP-SIP
Quintum Technologies	Tenor MultiPath	До 32	–	да	да	–
RadVision	VIU-323	2	RTOS	–	да	–
	L2W-323P PRI Gateway	4/8	RTOS	да	да	–
	L2W-323 BRI Gateway	4/8	RTOS	да	да	–
	MCU-323	До 24	RTOS	–	да	–
Ring	iMPACT	4	Win NT	нет	да	–
Science Dynamics	The Integrator	До 192	–	да	да	–

Производитель	Продукт	Количество портов	Операционная система	Поддержка Fax	Поддержка H.323	Поддерживаемые протоколы
	The Integrator C-2000	1344	–	да	да	–
Shoreline Communications	ShoreGear Teleworker Voice Switch	4	–	да	–	–
	ShoreGear Voice Switch	4-24	–	да	–	–
Siemens	HiPath RG 2500	До 30	–	да	да	–
	HiPath 5000	До 30	–	да	да	–
	Hicom Xpress	До 120	–	да	да	–
Soliton Systems	SolPhone 1004	4	–	да	да	–
Solphone	GW 3000 Series	От 2 до 4	–	да	v2	–
Sonus Networks	GSX9000 Open Services Switch	До 8064	–	да	да	MGCP
SOSINC	Sovereign	2-60	–	да	да	–
StarVox	IP Centrex	–	–	нет	–	MGCP
	VoIP VPN	–	Win NT	нет	v2	–
TEK DigiTel	V-Server iGate	2	Win NT-Unix	да	v2	–
	V-Server OfficeBuilder	2/4	Win NT-Unix	да	v2	–
Tekelec	IP7 Secure Gateway	–	–	–	–	–
Tellabs	SALIX 7720	–	–	да	нет	MGCP
	SALIX 7750	До 4	–	да	да	MGCP-Megaco
Teldat	Voxnet	4	Win NT-Unix	да	да	MGCP
Telinker	Enterprise VoIP Switch	До 12	Win NT	да	да	–
	One Platform Switch	До 240	Win NT	да	да	–
	Carrier Super Switch	960	Unix	да	да	–
Texas Instruments	VoIP Gateway	40	Wind River VXWorks	да	да	–
Tundo	Network Telephony System	4-60	–	–	да	MGCP
VegaStream	Vega50	8-48	–	нет	да	SIP
	Vega100	До 120	–	нет	да	–
	Vega200	До 30	–	нет	да	–
VideoServer	Encounter NetGate	До 16	Win NT	–	да	–
	Encounter NetServer ADX 1000	До 48	Win NT	–	да	–

Производитель	Продукт	Количество портов	Операционная система	Поддержка Fax	Поддержка H.323	Поддерживаемые протоколы
	Encounter 3000 NetServer	До 64	Win NT	–	да	–
VipNet	Telco-In-A-Box	–	Win NT	да	да	–
Vive Synergies	AutoVoIP	2	Win 95, 98 & NT	да	да	–
	ŸEnsemble!	До 8	–	да	–	MGCP-SIP
VocalTec	Series 120	До 120	Win NT	да	v2	–
	UniPOP	До 180	Win NT	да	v2	–
	Series 2000	До 480	VxWorks	да	v2	SIP*
	Signaling Gateway for SS7	–	Win NT	да	v2	–
Vodavi	DiscoveryIP	2, 4, 8	–	да	да	–
Voice & Data Systems	iPad	До 30	–	да	–	–
VocalData	VG-2 VoIP Gateway	До 1000	Unix	да	да	MGCP-SIP
VoIP Group	VComX	До 120	Win NT	нет	да	–
Voxo Telecom	OTS-300 IP Gateway	32	Unix	да	нет	–
WellX Telecom	Office	От 4 до 8	Win NT	да	v2	–
Woodwind Communications	Piccolo	До 8	–	–	да	–
	ClariNet	До 12	–	–	да	–
World Telecom Labs	INx	До 240	Unix	да	да	–

*в стадии внедрения

ПРИЛОЖЕНИЕ 5

АППАРАТНЫЕ IP-ТЕЛЕФОНы

(источник: http://www.iptelephony.org/frame/vendors_gateways.html)

Производитель	Модель IP-телефона
ADtech	IP Phone
Alcatel	Web Touch
Broadmedia	G-Phone CVB
	G-Phone CVX
	G-Phone DLX
	G-Phone IPX
Cisco	7910 IP Telephone
	7960 IP Telephone
	12 SP+ IP Telephone
	30 VIP IP Telephone
Congruency	i.Picasso
Cosmobridge	IP Phone
DSG Technology	InterPhone
e-tel	FreeRide SLT
	FreeRide TLT
ESI	IVX 128
hippo	Internet Telephone
InterActive	SoundXchange
Mitel	Superset 4015 IP
	Superset 4025 IP
Newchip	NewVoice DSP-040
Nortel Networks	i2004 Internet Telephone
Pingtel	xpressa VoIP Phones
Siemens	optiPoint 300 basic
	optiPoint 300 advance
UniData Communication Systems	IP Centrex Phone
	IPW-1000
	IPW-2500
	IPC-3000
WebCall World	IP Phone

ПРИЛОЖЕНИЕ 6

ПРОГРАММНЫЕ IP-ТЕЛЕФОНЫ

(источник: http://www.iptelephony.org/frame/vendors_gateways.html)

Производитель	Продукт	Опции	Платформы	Протоколы	Видео	Цена, долл.
01 Communique	I'm InTouch	Fax Support. File Transfer, Caller IDt	Win 95/98/2000/Me/NT	H.323 – GPRS	да	–
	Communicate! i2000	Unified Messaging, Fax Support, File Transfer, Caller ID, Directories	Win 95/98/2000/NT	H.323	да	149.95
	Communicate! Pro	Voicemail, Fax Support, File Transfer, Caller ID, Text Chat	Win 95/98/2000/NT	–	да	109.95
	Communicate!	Voicemail, Fax Support, File Transfer, Caller ID, Text Chat	Win 3x/95/NT	–	да	69.99
BoxTop	iVisit	Group Conference, Directory Assistance, Text Chat	Win 95/98/2000/NT/MAC	–	да	Б/п
buddyPhone	buddyPhone	Directory Assistance for Other Users & ICQ Users	Win 95/98/2000/NT	–	нет	Б/п
Callserve	React	PC to phone	95/98/2000/NT	H.323	нет	Б/п
CineCom	CineVideo	Text Chat	Win 95/NT	–	да	49.95
	Virtual Educator	–	Win 95/NT	–	да	2500
Cosmobridge	VoIP Java Web Client	–	–	–	–	–
CUseeMe	CU-SeeMe Pro	Whiteboard, Application Share, File Transfer, Group Conference, Directory Assistance, Text Chat	Win 95/98/NT/MAC	H.323	да	39
Cybration	ICUII	Directory Assistance, Caller ID, Text Chat	Win 95, 98, NT	–	да	39.95
Delta Three	Internet Phone Lite	Used With PC to Phone Service	Win 95/98/2000/NT	–	нет	Б/п
Dialpad	Agent	PC to PC & PC to Phone, Online Notification, Address Book	Win/MAC	H.323	нет	Б/п
Dwyco	Conference System	Group Conference, File Transfer, Directory	Win 95/98/NT	–	да	Б/п

Производитель	Продукт	Опции	Платформы	Протоколы	Видео	Цена, долл.
		Assistance, Text Chat				
Engineering Consulting	ClearPhone	Whiteboard, Group Conferencing, File Transfer, Application Share, Text Chat	Win 98+/MAC	–	да	69.95
Ezonics	EZPhone Cam	Built in Speakers and Microphone, user directories, full duplex communications	Win 98, ME, 2000	–	да	–
FireTalk Communications	FireTalk Basic	VoIP communications, text chat, user directories, full duplex conference calls of up to 1,000 participants	Win 95/98/2000/NT	SIP	нет	Б/п
	FireTalk VQ	VoIP communications, text chat, user directories, full duplex conference calls of up to 1,000 participants	Win 95/98/2000/NT	SIP	нет	19.95/mo
FreeTel Comm.	FreeTel	Directory Assistance, Caller ID, Text Chat	Win 3.x, 95	–	нет	39.95
FreeWebTel	FreeWebTel	Address Book, Caller ID, Voicemail and Text Chat	Win 95/98/2000/NT	–	нет	Б/п
iChatterbox	Vphone	Video Mail	Win 95, 98 & NT	–	да	Б/п
INRIA	Б/п Phone	Group Conference, Directory Assistance, File Transfer	Win 95/98/Sun/Linux	–	нет	Б/п
Intel	Internet Video Phone	Make Video Calls over Regular Lines, Application Share	Win 95/98	H.323	да	124 w/Cam
IPAxess	VocalWare IP Client	Use traditional phone, browse Internet, share documents	Win 95/98	–	нет	–
IRIS	IRIS Phone	Directory Assistance, Caller ID, Call Waiting, Text Chat	Win 3.x/95/NT	–	да	19.95
John Walker	Speak Freely	Group Conference	Win 3.x/95/NT	–	нет	Б/п
Livehelper.com	Livehelper	Full Duplex, Voice and Text Chat	Win 95/98/NT	–	нет	Б/п
Lucent	MultiVoice PC Client	Full duplex, G.711, G.729(a), G.723, GSM coders, Adv. Acoustic Echo Suppression, JAVA Developer's Tool Kit (Object Code), PC to Phone, PC to PC, Phone to PC (Internet Call waiting), web based and 32-Bit version.	Win 95/98/NT/2000	H.323	нет	–

Производитель	Продукт	Опции	Платформы	Протоколы	Видео	Цена, долл.
Microsoft	NetMeeting	Call Answer, Whiteboard, Application Share, File Transfer, Group Conference, Text Chat, Directory Assistance	Win 95/98/ME/NT	–	да	Б/п
MediaRing	MediaRing Talk	Caller ID, Directory Assistance, Text Chat	Win 95/98/2000/NT	–	нет	Б/п
Nautilus	Nautilus	Half Duplex, Encrypted Speech	Win 95/98/NT/Solaris/ Linux/DOS	–	нет	Б/п
Net Talk	Community Chat	Used for PC to Phone Service. Features multipoint voice conferencing, 3D video animation, private text messaging, file transfer, whiteboarding, application sharing and communications recording/storing	–	–	–	–
Net2Phone	Net2Phone	Used for PC to Phone Service	Win 3.x/95/98/2000/ ME/NT/MAC	–	нет	Б/п
Netscape	CoolTalk	Whiteboard, Caller ID, Text Chat	Win 3.x/95/NT/MAC/ Solaris/Unix	–	нет	Б/п
NetSpeak	Mini WebPhone	Whiteboard, Group Conference, Directory Assistance, Caller ID, Text Chat	Win 3.x/95/98/NT	H.323	да	–
	WebPhone	Whiteboard, Group Conference, Directory Assistance, Caller ID, Voicemail, Text Chat	Win 95/98/NT	H.323	да	49.95
Network Associates	PGP Fone	–	Win 95/NT/MAC	–	нет	Б/п
Paltalk	Paltalk	Text Chat, File Transfer	Win 95/98/2000/NT	–	да	Б/п
Paramax	MaxPhone Lite	–	Win 95/98/NT4	–	нет	29.95
PC-Telephone.com	PC-Telephone	PC to PC/PC to Phone Calling, Fax, File Transfer, Voicemail	Win 95/98/2000/NT	–	нет	56
PhoneFree	PhoneFree	Whiteboard, File Transfer, Directory Assistance, Text Chat	Win 95/98/2000/NT	–	да	Б/п
PictureTalk	PictureTalk	–	Win 95/NT/MAC/Sun	–	нет	Б/п
ReallyEasy.Com	ReallyEasy Interactor	Directory Assistance, Text Chat, Security, Conferencing, Voicemail	Win 95/98/NT/MAC	H.323	нет	Б/п

Производитель	Продукт	Опции	Платформы	Протоколы	Видео	Цена, долл.
SecurIPhone	SecuriIPhone	Directory Assistance, Text Chat, Encryption	Win 95/98/2000/ME/NT	–	нет	Б/п
Smith Micro Software	Internet CommSuite	Directory Assistance, Text Chat, Fax Support	Win 95/98/NT	–	да	49.95
SilverSoft	Softphone	Full Duplex, Voicemail,	Win 95	–	да	19.95
Tribal Voice	PowWow	Whiteboard, Group Conference, Directory Assistance, Text Chat	Win 3.x/95/98/2000/NT	–	нет	Б/п
University College London	Robust Audio Tool (RAT)	Whiteboard, Group Conferencing	Win 95, NT, FreeBSD, HP-UX, IRIX, Linux, NetBSD, Solaris, Sun	–	нет	Б/п
	Videoconferencing Tool	Whiteboard, Group Conferencing	Win 95, NT, FreeBSD, IRIX, Linux, Solaris, Sun	–	да	Б/п
VocalTec	Internet Phone Lite	Whiteboard, Application Share, File Transfer, Group Conference, Caller ID, Text Chat, PC to Phone, Call Waiting and Directory Assistance	Win 95/98/NT	–	да	49.95
VoxPhone	Video VoxPhone Gold	Group Conference, PC to Phone, Voicemail, Directory Assistance, File Transfer, Caller ID, Text Chat	Win 95/98/NT	H.323	да	31.99
Virtual Universe Corporation	Virtual Talker	Video Conferencing, Unified Communications & File Transfer	Win 95/98/2000/NT	–	нет	–
Wintronix	XtX	Group Conference, Whiteboard, Application Share, File Transfer, Directory Assistance	Win 95/98/NT	–	да	69.95

СПИСОК СОКРАЩЕНИЙ

AAA	Authentication, Authorization, Accounting	аутентификации, авторизации и учет
ADC	Analog to Digital Converter	аналого-цифровой преобразователь
ADPCM	Adaptive Differential Pulse Code Modulation	адаптивная дифференциальная ИКМ
ANSI	The American National Standards Institute	Американский национальный институт стандартов, АНИС
APoA	IP Application Point of Attachment	точка подключения IP приложений
ARP	Address Resolution Protocol	протокол разрешения адреса
ATM	Asynchronous Transfer Mode	асинхронный режим передачи
BGP	Border Gateway Protocol	протокол граничных шлюзов
B-ISDN	Broadband Integrated Service Digital Service	широкополосная цифровая сеть с интеграцией служб
BRI	Basic Rate Interface	интерфейс базового доступа
BSP	Branded Service Provider	провайдер фирменных услуг
CAS	Channel Associated Signalling	канально-ориентированная сигнализация 2ВСК
CBC	Cipner Block Chaining	цепочка зашифрованных блоков
CBSP	Certificate Based Service Protection	механизм защиты, основанный на цифровых сертификатах
CC	Country Code	код страны
CDR	Call Detail Record	детальная информация о вызовах
CFB-x x	Criptotext Feedback mode	битовая зашифрованная обратная связь
CHAP	Challenge Handshake Protocol	протокол взаимодействия вызовов
COPS	Common Open Policy Service	сервис общей открытой политики
CoS	Class-of-Service	класс обслуживания
DCD	Duty Cycle	случайный джиттер
DDJ	Data Dependent Jitter	джиттер, зависимый от данных
DES	Data Encryption Standard	стандарт шифрования данных
DHCP	Dynamic Host Configuration Protocol	протокол динамической настройки хоста
DiffServ	Differentiated Services	дифференцированное обслуживание
DNS	Domen Name System	сервер имен доменов
DoS	Denial of Service	отказ от обслуживания
DSP	Digital Signalling Processor	цифровой сигнальный процессор, ЦСП
DSP	Directory Service Provider	провайдер информационных услуг
DTMF	Dual Tone Multiple Frequency	двухчастотная абонентская сигнализация
EAP	Extensible Authentication Protocol	гибкий протокол аутентификации
ECB	Electronic Code Book	электронная кодовая книга
EF	Expedited Forwarding	срочная отправка

ETSI	The European Telecommunications Standards Institute	Европейский институт стандартизации по телекоммуникациям
FQDN	fully qualified domain name	полное доменное имя
FTP	File Transfer Protocol	протокол передачи файлов
GGSN	Gateway GPRS Supporting Node	узел, выполняющий функции шлюза GPRS
GPRS	General Radio Packet System	система пакетной радиосвязи общего пользования
GSM	Global System for Mobile communications	глобальная система мобильной связи
GSTN	Global Switched Telephon Network	всемирная коммутируемая телефонная сеть
HE	Home Entity	домашний компонент
HLR	Home Location Register	регистр домашнего местоположения
HTTP	HyperText Transfer Protocol	протокол передачи гипертекста
ICMP	Internet Control Message Protocol	протокол передачи управляющих сообщений
ICP	Interconnectivity Provider	провайдер услуг взаимодействия
ID	Identifier	идентификатор
IDEA	International Data Encryption Algorithm	международный алгоритм шифрования данных
IEEE	The Institute of Electrical and Electronics Engineers	Институт инженеров по электротехнике и электронике
IETF	The Internet Engineering Task Force	Инженерная группа по проблемам Интернет
IMS	Internet Management System	система менеджмента Интернет
IMTC	International Multimedia Teleconferencing Consortium	Международный консорциум мультимедийных телеконференций
IntServ	Integrated Services	рабочая группа по интегрированному обслуживанию
IOS	Internetwork Operating System	межсетевая операционная система
IP	Internet Protocol	межсетевой протокол
IPAP	IP Access Provider	провайдер доступа IP
IPEU	IP end user	конечный пользователь IP
IPNP	IP Network Provider	провайдер IP сети
IPSec	IP Security	IP-безопасность
ISDN	Integrated Service Digital Service	цифровая сеть с интеграцией служб, ЦСИС
ISP	Internet Service Provider	провайдер услуг Интернет
ISUP	Integrated Services User Part	подсистема пользователя сети с интеграцией служб
ITSP	Internet Telephony Service Provider	провайдер услуг Интернет-телефонии
ITU-T	The International Telecommunications Union	Сектор стандартизации телекоммуникаций Международного союза электросвязи
LAN	Local Area Network	локальная вычислительная сеть, ЛВС
LCP	Link Control Protocol	протокол управления связью
LDAP	Lightweight Directory Access Protocol	упрощенный протокол доступа к каталогу

LD-CELP	Low-Delay Code-Excited Linear Prediction	кодирование с возбуждающим воздействием, линейным предсказанием и малой задержкой
LPC	Linear Predicative Coding	кодирование с линейным предсказанием
MCU	Multi Point Conferencing Unit	устройство управления многоточечной конференцией
MF	Multi Frequency	многочастотный
MG	Media Gateway	транспортный шлюз
MGC	Media Gateway Controller	контроллер транспортного шлюза
MIPS	Million Instructions Per Second	миллион инструкций в минуту
MMUSIC	Multiparty Multimedia Session Control	рабочая группа по управлению многоточечными сеансами мультимедиа-связи
MOS	Mean Opinion Score	единица субъективной оценки
MPLS	Multiprotocol Label Switching	многопротокольная коммутация меток
MP-MLQ	Multipulse Maximum Likelihood Quantization	метод квантования по максимуму правдоподобия
MPPE	Microsoft Point-to-Point Encryption	шифрование двухточечной связи Microsoft
NSN	National Significant Number	национальный значащий номер
NAI	Network Access Identifier	идентификатор доступа к сети
NAoP	Network Point of Attachment	точка подключения сети
NCP	Network Control Protocols	протоколы управления сетью
N-ISDN	Narrowband Integrated Service Digital Service	узкополосная цифровая сеть с интеграцией служб
OFB	Output feed-back	выходная обратная связь
OSI	Open System Interconnection	взаимодействие открытых систем, ВОС
OSP	Open Settlement Protocol	протокол открытых соглашений
OSPF	Open Shortest-Path First	протокол кратчайшего пути
PAP	Password Authentication Protocol	протокол аутентификации пароля
PBSP		механизм защиты, основанный на паролях
PBX	Private Branch Exchange	учрежденческая АТС
PDP	Packet Data Protocol	протокол пакетных данных
PDP	Policy Decision Point	точка принятия решений
PEP	Policy Enforcement Point	точка реализации стратегий
PFWG	Policy Framework Working Group	рабочая группа IETF по общей архитектуре
PIB	Policy Information Base	база данных о стратегиях
PIN	Personal Identification Number	персональный идентификационный номер
PINT	PSTN and Internet Internetworking	взаимодействие ТфОП и сети Интернет
PKI	Public Key Infrastructure	инфраструктура с открытыми ключами
POTS	Plain Old Telephone System	аналоговая телефонная система
PPP	Point-to-Point Protocol	протокол "точка-точка"

PPTP	Point-to-Point Tunneling Protocol	туннельный протокол между двумя точками
PRI	Primary Rate Interface	интерфейс первичного доступа
PSTN	Public Switched Telephon Network	телефонная сеть общего пользования, ТфОП
QDU	Quantization Distortion Units	единицы искажения квантования
QoS	Quality of Service	качество обслуживания
RADIUS	Remote Access Dial-In User Service	система обеспечения доступа удаленных пользователей
RARP	Reverse Address Resolution Protocol	реверсивный ARP
RAS	Registration/Admission/Status	протокол регистрации, подтверждения и состояния
RAS	remote access server	сервер дистанционного доступа
RFC	Request for Comment	предложение по спецификациям IETF
RSVP	Resource Reservation Protocol	протокол резервирования ресурсов в сети Интернет
RTCP	Realtime Transport Control Protocol	протокол управления передачей в реальном времени
RTP	Realtime Transport Protocol	протокол передачи в реальном времени
SAP	Session Announcement Protocol	протокол уведомления сеанса связи
SCAP	Switched Circuit network Access Provider	провайдер доступа к сети с коммутацией каналов
SCN	Switched Circuit Network	сеть с коммутацией каналов
SCNP	Switched Circuit Network Provider	провайдер услуг сети с коммутацией каналов
SDP	Session Description Protocol	протокол описания сеанса связи
SG	Signalling Gateway	шлюз сигнализации
SGSN	Serving GPRS Support Node	узел, поддерживающий услуги GPRS
SHA	Secure Hash Algorithm	алгоритм безопасного хэша
SIP	Session Initiation Protocol	протокол создания сеанса связи
SLA	Service Level Agreement	соглашение об уровне предоставляемых услуг
SMTP	Simple Mail Transfer Protocol	протокол передачи сообщений
SNMP	Simple Network Management Protocol	протокол управления сетью
SSL	Secure Sockets Layer	уровень защиты сокетов
TAPI	Telephony Application Programming Interface	телефонный прикладной программный интерфейс
TCP	Transmission Circuit Protocol	протокол передачи в канале
TIPHON	Telecommunications and Internet Protocol Harmonization over Networks	название проекта ETSI, имеющего целью обеспечить взаимодействие IP-сетей и SCN
TLS	Transport Layer Security	безопасность транспортного уровня
ToS	Type of Service	тип обслуживания
UAC	User Agent Client	клиент агента пользователя
UAS	User Agent Server	сервер агента пользователя

UDP	User Datagram Protocol	протокол пользовательских дейтаграмм
UMTS	Universal Mobile Telecommunications System	система универсальной мобильной связи
VAD	Voice Activity Detector	детектор голосовой активности
VASP	Value Added Service Provider	провайдер дополнительных услуг
VoIP	Voice over IP	передача голоса по сети с протоколом IP
VON	Voice over Net Coalition	организация, которая содействует развитию Internet-телефонии и представляет интересы производителей в области Internet-телефонии
VPN	Virtual Private Network	виртуальная частная сеть
WAN	Wide Area Network	глобальная сеть

АДИКМ	адаптивная дифференциальная импульсно-кодовая модуляция
АДЭ	Ассоциации документальной электросвязи
АТС	автоматическая телефонная станция
АЦП	аналого-цифровое преобразование
ВСК	выделенный сигнальный канал
ИКМ	импульсно-кодовая модуляция
ЛВС	локальная вычислительная сеть
ОЗУ	оперативное запоминающее устройство
ОКС	общеканальная сигнализация
ПК	персональный компьютер
ПО	программное обеспечение
СКК	сеть с коммутацией каналов
СОРМ	система оперативно-розыскных мероприятий
ТфОП	телефонная сеть общего пользования
УАТС	учрежденческая АТС
ЦАП	цифро-аналоговое преобразование
ЭМВОС	эталонная модель взаимодействия открытых систем