МИНИСТЕРСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО СВЯЗИ И ИНФОРМАТИЗАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
УНИТАРНОЕ ПРЕДПРИЯТИЕ
ЛЕНИНГРАДСКИЙ ОТРАСЛЕВОЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
СВЯЗИ - НИО-1

Организация услуг IP-телефонии поставщиками услуг Интернет

Автор: Саморезов Владимир
Лаб. №111
ЛОНИИС
E-mail: samorezov@rts.loniis.ru
http://www.protei.ru

Санкт-Петербург
28.03.2002

Содержание

1. Введение

На сегодняшний день к услугам, которые предоставляют сети коммутации пакетов с самым ярким представителем в виде глобальной сети Интернет, прибавилась еще одна – IP-телефония. Рост ее популярности позволяет судить о большом будущем организации телефонной связи на базе таких сетей. Объем речевого трафика, передаваемого по IP-сетям, составляет 3% мирового трафика передачи речи [1]. Но у данной услуги есть один основной недостаток – малая доступность. Ввиду сложностей с организацией биллинга, аутентификации и авторизации, определения местоположения пользователей и т.д. не так просто организовать обслуживание пользователей IP-сетей провайдерами услуг IP-телефонии (IPTSP – IP-Telephony Service Provider).

В данной статье рассматривается возможность объединения провайдеров, предоставляющих традиционные услуги Интернет (www, электронная почта, ftp и т.д.) с провайдером услуг IP-телефонии.

Второй раздел статьи описывает возможности типового Интернет - провайдера (ISP – Internet Service Provider), организацию его узла, протоколы и способы аутентификации, авторизации и учета.

В третьем разделе содержится описание провайдера услуг IP-телефонии. Обосновывается выбор протокола SIP для предоставления услуг IP-телефонии. Описывается, какие компоненты узла, необходимы для полноценной работы провайдера.

Цель четвертого раздела – показать, каким образом можно интегрировать ISP и IPTSP. Приведена структурная схема интегрированного узла доступа. Показаны преимущества и требования, возникающие при интеграции.

Естественно, любое техническое совершенствование ведет к возникновению разнообразных трудностей. Пятый раздел описывает проблемы, которые могут встретиться у провайдера при построении интегрированного узла доступа, а также возможные пути их решения.

2. Описание типового провайдера услуг Интернет

В настоящее время набором базовых услуг Интернет – провайдера, фундаментом его деятельности, являются:

- Доступ к сети Интернет по коммутируемым линиям;
- Доступ к сети Интернет по выделенным линиям;
- Услуги электронной почты и новостей.

К дополнительным услугам можно отнести:

- Размещение web-серверов клиентов на территории провайдера. Эти услуги подразделяются, как правило, на два класса: размещение виртуальных серверов (web-hosting) и размещение физических серверов (co-location);
- Услуги по организации и управлению политиками безопасности сетей клиентов;
- Услуги по гарантированному предоставлению определенного уровня качества сервиса;
- Организация виртуальных частных сетей.

На рисунке 1 приводится структурная схема узла ISP

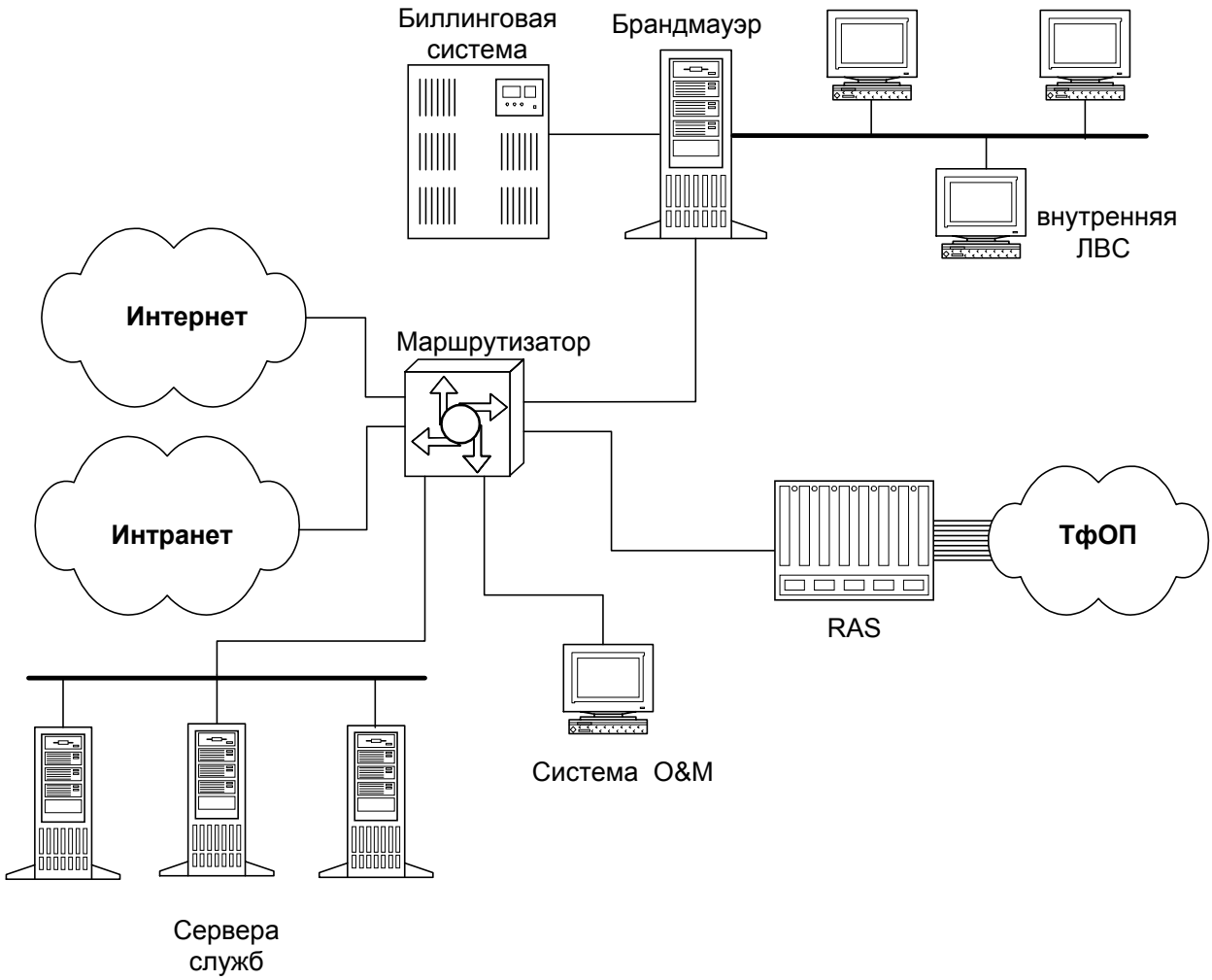

Рисунок 1 – Структурная схема узла Интернет - провайдера

Маршрутизатор – главная компонента узла. Он обеспечивает направление IP – трафика по заданным адресам, регулировку полосы пропускания между подсистемами узла и сетью Интернет.

Подсистема O&M (Operation & Management) позволяет осуществлять контроль за исправностью всех компонентов системы, выявлять возможные неполадки в работе узла, собирать для дальнейшего анализа информацию о состоянии системы и т.д. Другой важной возможностью подсистемы O&M является централизованное конфигурирование компонентов узла.

Для аутентификации, авторизации и учета всех соединений предназначена биллинговая система. В ее состав может входить RADIUS-сервер и биллинговый сервер. Тарифы могут зависеть от времени, объема трафики и используемых служб, запрошенного качества обслуживание (QoS). Для расчетов могут использоваться предоплаченные карты или кредитная система.

На серверах служб провайдер содержит собственные www-сервер, ftp – сервера, почтовые сервера, сервера службы доменных имен и т.д.

В локальной сети узла на уровне сетевого интерфейса, который включает физический и канальный уровень модели ВОС (OSI), в зависимости от подсистемы, это может быть Ethernet или Fast Ethernet. Для пользователей, которые подключаются к серверу удаленного доступа, на канальном уровне используется протокол PPP (Point-to-Point Protocol) [2]. На сетевом уровне применяется Internet Protocol.

Управление и мониторинг обеспечиваются с помощью протокола прикладного уровня SNMP (Simple Network Management Protocol)[3].

Интерфейс между серверами удаленного доступа и биллинговой системой реализуется с помощью протокола RADIUS (Remote Authentication Dial In User Service) [4]. RADIUS является протоколом, обеспечивающим аутентификацию, авторизацию пользователей, подключающихся к устройствам доступа и учет проведенных сеансов связи.

Серверы служб взаимодействуют с рабочими станциями пользователей по протоколам прикладного уровня HTTP, FTP, SMTP, POP3.

Основными компонентами узла, ответственными за базовые услуги являются сервера доступа (RAS – Remote Access Server). В них агрегируются потоки трафика от пользователей коммутируемого доступа и передаются далее, также с их помощью подключаются клиенты, использующие выделенные линии. RAS включает в себя: интерфейс с сетью, через которую подключается удаленный пользователь (в данном случае - ТфОП), средства инкапсуляции и выделения дейтаграмм протоколов третьего уровня в (из) пакеты канального уровня (PPP, SLIP и т.п.), средства аутентификации, интерфейс с сетью узла. В современных серверах доступа подключение пользователей осуществляется с помощью устройств, к которым подключаются цифровые тракты от АТС. Эти устройства содержат в себе модули обработки телефонной сигнализации и цифровые

модемы, при помощи которых происходит обмен информацией между пользователем и сервером доступа.

На рисунке 2 представлена функциональная схема сервера доступа.

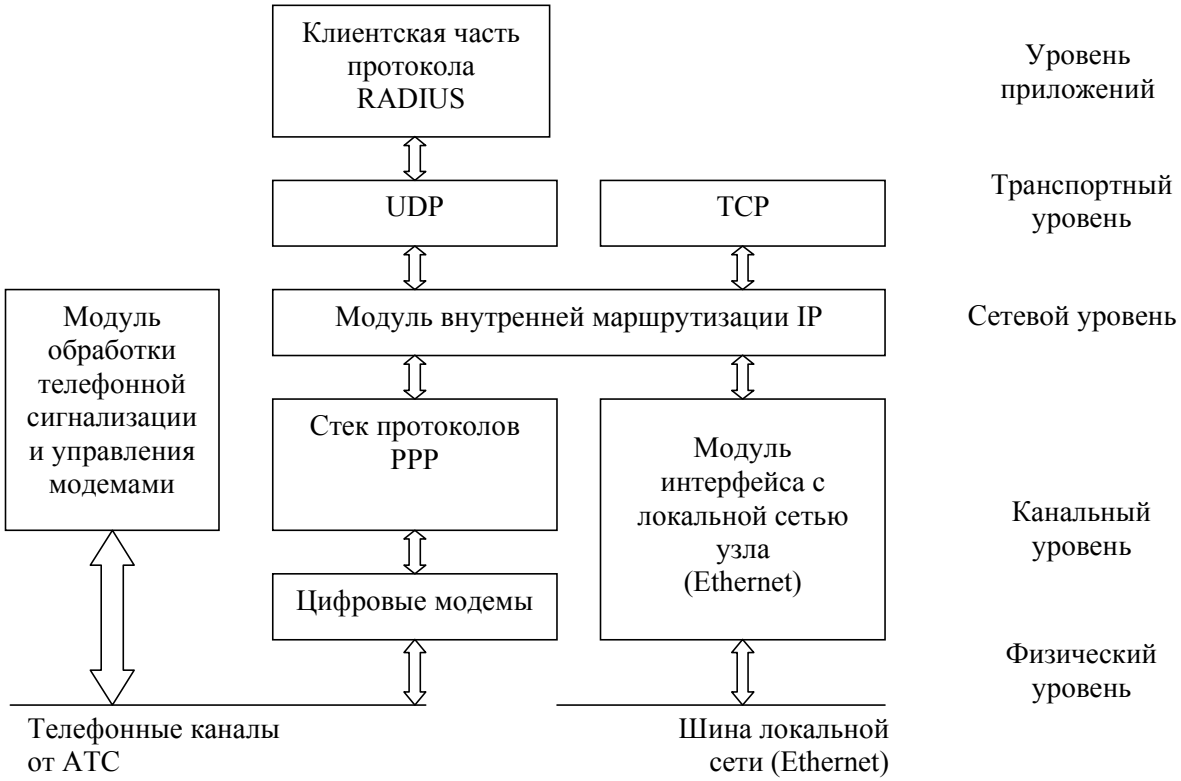

Рисунок 2 - Функциональная схема сервера доступа в соответствии с уровнями модели ВОС (OSI).

3. Услуги IP-телефонии и IPTSP

При решении о предоставление услуг IP-телефонии одним из важных вопросов является выбор протокола установления соединений, который будет использоваться в IP-сети. Сейчас существует три вида таких протоколов и, следовательно, подходов к построению сетей IP-телефонии: H.323, основанный на рекомендации ITU-T [5]; SIP (Session Initiation Protocol), разработанный организацией IETF и оформленный в виде RFC 2543 [6]; протоколы, использующие принцип декомпозиции шлюзов, примером которого является протокол MGCP (RFC 2705) [7]. Более подробную информацию о каждом из этих протоколов, а также об областях их использования можно получить в [8].

По мнению автора, для предоставления услуг IP-телефонии Интернет-провайдером лучше всего подходит протокол SIP по следующим причинам.

Протокол SIP является простым и понятным протоколом, это облегчает его изучение (а провайдеру, скорее всего, не сильно хочется заниматься серьезной переподготовкой своих сотрудников), а также дальнейшее обслуживание оборудования, построенного на

базе этого протокола. Текстовый формат сообщений значительно упрощает их кодирование, декодирование и анализ, это позволяет реализовать протокол на базе любого языка программирования. Число возможных информационных полей SIP составляет всего несколько десятков при сотне в протоколе H.323.

Протокол SIP позволяет предоставить широкий спектр дополнительных услуг связи, таких как перевод соединения в режим удержания (Call hold), переключение связи (Call Transfer), переадресация (Call Forwarding), уведомление о новом вызове во время связи (Call Waiting), конференция. Протокол SIP имеет хороший набор средств поддержки персональной мобильности пользователей, в число которых входит переадресация вызова к новому местоположению пользователя, одновременный поиск по нескольким направлениям (с обнаружением зацикливания маршрутов) и т.д. В протоколе SIP это организуется путем регистрации на сервере определения местоположения.

Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом Internet Engineering Task Force (IETF). Эта архитектура включает в себя также протокол резервирования ресурсов (Resource Reservation Protocol, RSVP; RFC 2205), транспортный протокол реального времени (Real-Time Transport Protocol, RTP; RFC 1889), протокол передачи потоков в реальном времени (Real-Time Streaming Protocol, RTSP; RFC 2326), протокол описания параметров связи (Session Description Protocol, SDP; RFC 2327). То, что протокол SIP разрабатывался IETF, говорит о том, что он легко интегрируем в стек существующих протоколов Интернет, с которыми ISP в силу свой работы связан постоянно. Это является существенным аргументом в пользу SIP.

SIP-сеть (рисунок 3) состоит из SIP-клиентов и SIP-серверов. Клиенты посылают запросы или серверам или напрямую другим клиентам. Для того чтобы узнать местоположение пользователя SIP-сервер может обратиться к серверу определения местоположения с помощью протоколов LDAP (RFC 1777), rwhois (RFC 2167), или других. Клиент при включении, выключении или смене местоположения регистрируется на сервере определения местоположения с помощью специального сообщения протокола SIP.

На рисунке 3 показан пример SIP-сети. Терминал A с использованием специального программного обеспечения посылает запрос на установление соединения на локальный SIP-сервер (1). Последний принимает запрос и на основании свой базы данных перенаправляет запрос на другой SIP-сервер, который, возможно, может его обслужить (2). Второй SIP-сервер консультируется с сервером определения местоположения о том, где можно найти вызываемого пользователя (3). После выяснения текущего адреса терминала SIP-сервер связывается с ним (4). IP-пакеты с речевым трафиком идут напрямую между терминалами.

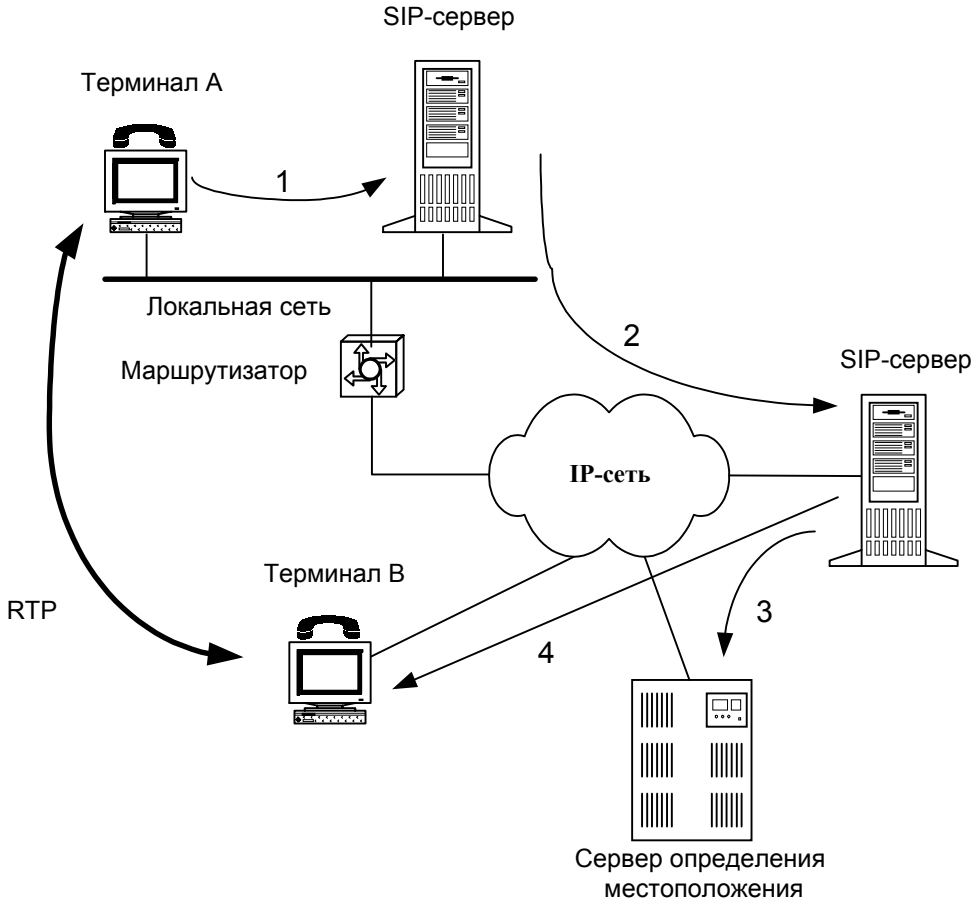

Рисунок 3 – Пример SIP-сети0

В качестве адресов рабочих станций используются специальные универсальные указатели ресурсов - URL (Universal Resource Locators), так называемые SIP URL.

SIP-адреса бывают четырех типов:

- *имя@домен*,
- *имя@хост*,
- *имя@IP-адрес*,
- *№телефона@шлюз*.

Таким образом, адрес состоит из двух частей. Первая часть – это имя пользователя, зарегистрированного в домене или на рабочей станции. Если вторая часть адреса идентифицирует какой-либо шлюз, то в первой указывается телефонный номер абонента.

Во второй части адреса указывается имя домена, рабочей станции или шлюза. Для определения IP-адреса устройства необходимо обратиться к службе доменных имен - Domain Name Service (DNS). Если же во второй части SIP-адреса размещается IP-адрес, то с рабочей станцией можно связаться напрямую.

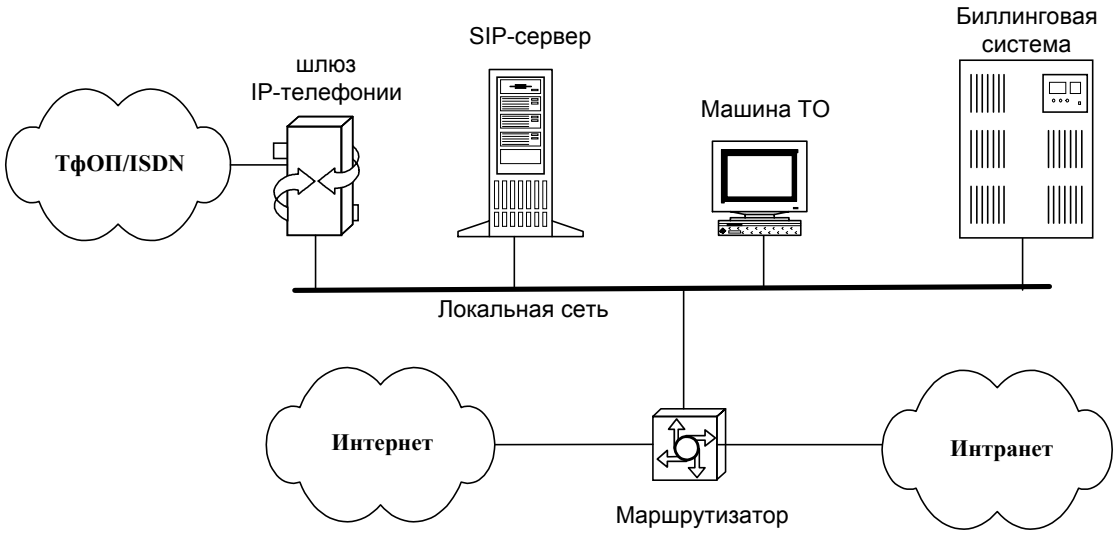

Рисунок 4 – Архитектура узла IPTSP

Теперь перейдем к описанию провайдера услуг IP-телефонии или IPTSP. На рисунке 4 показана архитектура узла такого провайдера.

Для предоставления услуг IP-телефонии абонентам ТфОП необходим шлюз, который осуществляет преобразование сигнализации, используемой в сети с коммутацией каналов, в сигнализацию SIP. Кроме того, шлюз преобразует речь и упаковывает её в IP-пакеты. К ТфОП шлюз может подключаться по ИКМ-трактам или по аналоговым соединительным линиям (например, трехпроводным).

Для учета стоимости разговоров, осуществления проверки подлинности абонентов и подобных задач предназначена биллинговая система. Отличия этой системы от аналогичной для Интернет-провайдера небольшие. В частности, это другая система учета стоимости, например, в зависимости от тарифной зоны. Система расчета опять таки может быть с предоплаченными картами или кредитная. Пользователь покупает карту данного провайдера, звонит на шлюз IP-телефонии по номеру, указанному на карте, в тональном наборе набирает PIN-код, в случае его правильности ему предлагается набрать номер вызываемого абонента. Для связи шлюза с биллинговой системой используется протокол RADIUS или подобный ему.

SIP-сервер принимает запросы от клиентского ПО и на основании своей базы данных маршрутизирует их. Возможно, что SIP-сервер выполняет авторизацию и аутентификацию (это позволяет сделать протокол SIP).

Маршрутизатор направляет IP-пакеты в публичный Интернет или в Интранет, где может поддерживаться качество обслуживания (QoS). В данном случае выделенная IP-сеть Интранет предназначена специально для трафика IP-телефонии и рассчитана на критичные к задержке речевые пакеты (в этом случае её обычно называют сетью IP-

телефонии). Может случиться, что вызываемая сторона недоступна по Интранет, и надо пользоваться Интернет, в этом случае провайдер не может гарантировать, что соединение будет удовлетворять допустимым нормам по задержке и джиттеру. На современном этапе развития использовать публичный Интернет для целей IP-телефонии нецелесообразно.

В заключение этого пункта хочется отметить, что большинство современных провайдеров IP-телефонии для построения своих систем используют протокол H.323. Но стремительный рост популярности SIP позволяет предположить, что этот протокол в будущем найдет более широкое применение при построении сетей IP-телефонии.

4. Интеграция ISP и IPTSP

Теперь попробуем представить, что провайдер услуг Интернет решил организовать у себя узел IP-телефонии. Он может теперь кроме обычного соединения с Интернет для своих пользователей организовать телефонную связь прямо с персонального компьютера к абонентам ТфОП или к другим пользователям в какой-либо IP-сети. Возможно также , что абоненты ТфОП с использованием предоплаченной карты пользуются услугами IP-телефонии и делают вызовы другим абонентам ТфОП или на персональный компьютер .

Естественно, есть возможность напрямую без участия SIP-серверов связаться с необходимым адресатом, если известен его IP-адрес. Но тогда связь будет осуществляться через публичный Интернет, что плохо скажется на качестве речи. Кроме того, в таком случае пользователь не получит доступ ни к каким дополнительным услугам, которые в большинстве своем могут быть организованы только на базе SIP-сервера.

На рисунке 5 представлена структурная схема интегрированного узла доступа, т.е. узла, в котором кроме традиционных Интернет услуг могут быть организованы услуги IP-телефонии.

Сценарий установления соединения в этом случае похож на описанный выше с той разницей, что здесь вызываемым и вызывающим абонентами могут быть пользователи Интернет, подключенные с помощью модемов к данному провайдеру. Соединение, например, может быть установлено между таким пользователем и абонентом ТфОП через шлюз IP-телефонии. Более того, возможна организация такой услуги как вторая виртуальная линия (VL – Virtual Line). При ее заказе вызовы, приходящие на занятый модемным соединением телефон, будут переадресовываться на персональный компьютер.

Одним из самых больших достоинств такой интеграции служит то, что теперь речевой трафик можно будет «заворачивать» прямо у провайдера, что снизит задержки и

джиттер. SIP-сервером (или точнее специальным программным обеспечением) может быть запрошен определенный уровень качества обслуживания (QoS).

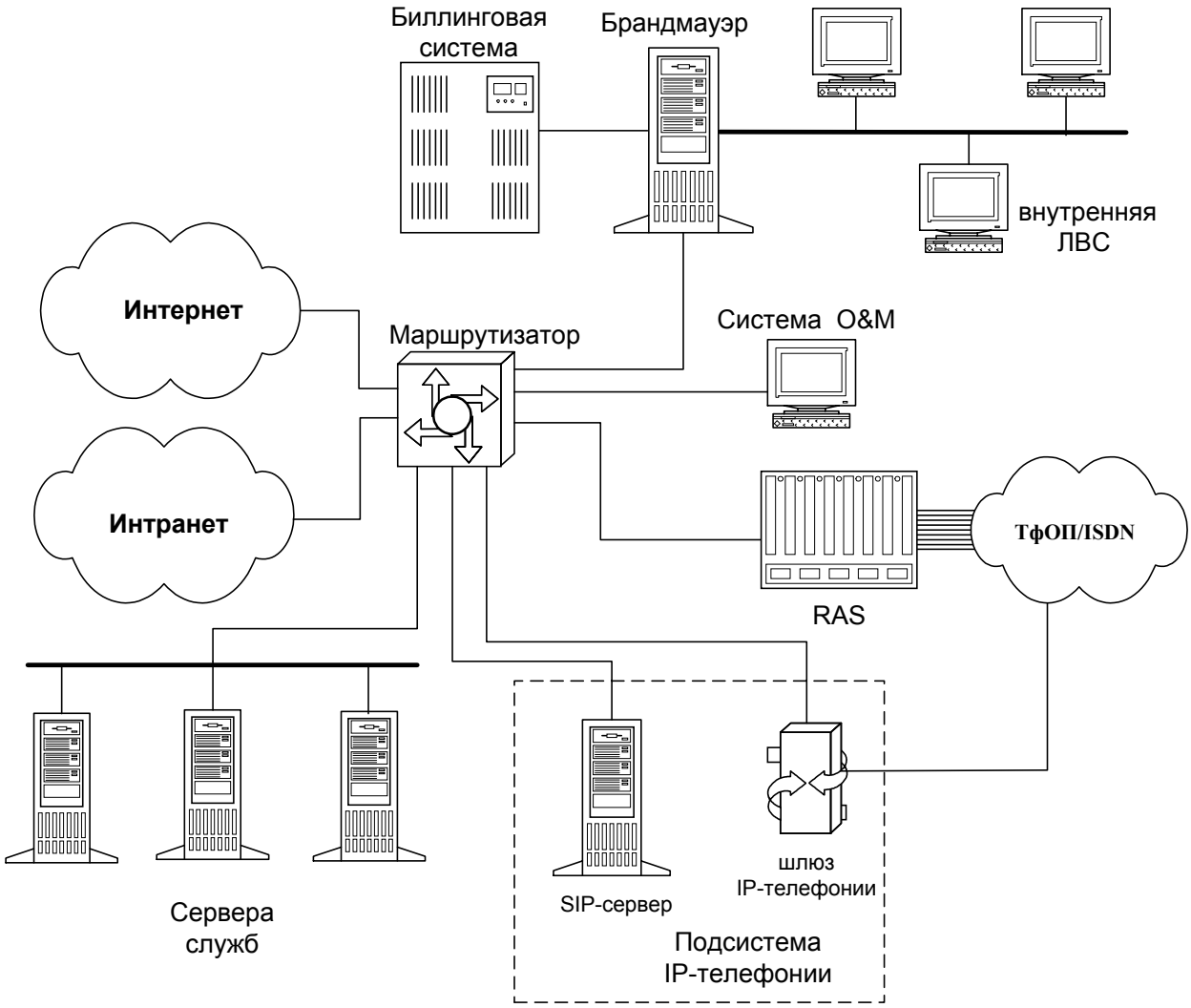

Рисунок 5 – Структурная схема интегрированного узла доступа

Другое достоинство такой системы – это централизованная база данных абонентов, входящая в состав биллинговой системы. В ней может храниться полная информация об индивидуальных настройках пользователей, которые могут, например, зайти на свою web-страницу, изменить набор предоставляемых услуг, посмотреть остаток на своем счету т.д.

Предоплаченные карты теперь могут быть использованы одновременно для расчета за услуги Интернет и за услуги IP-телефонии. Т.е. у пользователей будет единый счет, с которого будут сниматься единицы по мере того, как он будет использовать свою карту. Правда, тут возникает некоторая проблема, в случае, когда кто-то одновременно пользуется Интернетом и делает вызовы по IP-телефонии. Пример решения этой технической задачи будет приведен в следующем пункте.

С точки зрения протокола SIP все вызовы сначала приходят на SIP-сервер, который решает, как их обслуживать дальше. Как и раньше он может консультироваться с локальной или удаленной базой данных о местоположении вызываемого пользователя. Этот сервер будет также использоваться для учета длительности вызовов, связываясь по протоколу RADIUS с биллинговой системой. Последняя будет определять стоимость услуг IP-телефонии на основе уставленных тарифов. Более того, этот же сервер будет регистрировать пользователей в своей или удаленной базе данных.

На рисунке 5 шлюз и SIP-сервер представлены как отдельные структурные единицы, но в реальности они могут входить в состав серверов удаленного доступа (RAS). Примером такой системы является сервер доступа Cisco AS5300. Но чаще у провайдера стоят отдельные сервера для Интернет и для IP-телефонии.

5. Проблемы, возникающие при интеграции

В данном пункте попытаемся рассмотреть, какие же проблемы возникают при объединении ISP и IPTSP. При этом хочется обратить внимание, что автор не обещает, что круг задач возникающих при интеграции будет описан здесь полностью. Более того, приводятся не все пути решения, т.к., как правило, они (эти решения) очень сильно зависят от конкретного провайдера, от используемого оборудования и предполагаемых затрат на модернизацию узла (впрочем, как и любом оборудовании связи).

Итак, при предоставлении совместных услуг пользователю дается единая карта, пользуясь которой он может иметь доступ к глобальным ресурсам Интернет и делать телефонные вызовы по IP-телефонии. Но в таком случае возникает проблема с протоколом RADIUS. Ввиду того, что он работает по принципу «клиент-сервер», у биллинговой системы нет возможности сообщить, что предоплаченная сумма истекла, когда пользователь одновременно подключен к Интернет и пользуется IP-телефонией, и с его счета необходимо снимать деньги за обе услуги. Т.е. в протоколе не предусмотрена возможность, чтобы RADIUS-сервер сам инициировал сообщения. Он может только отвечать на запросы от RADIUS-клиента, который располагается на RAS или на SIP-сервере. Таким образом, необходимо придумать механизм, с помощью которого биллинговому серверу можно сообщить о том, что необходимо отключить пользователя. Для этого может служить протокол SNMP (Simple Network Management Protocol), который предназначен для управления сетью. На рисунке 6 показан сценарий обмена сообщениями для вышеописанного случая.

Пользователь инициирует модемное соединение с RAS провайдера. Кроме этого он решает сделать телефонный вызов, используя IP-телефонию и SIP-сервер провайдера.

Получается, что он кроме обычной услуги Интернет должен заплатить за дополнительную услугу IP-телефонии.

Биллинговая система содержит всю информацию о том, сколько единиц осталось на счету пользователя. Но в данную систему необходимо добавить возможность самой, параллельно с RAS или SIP-сервером, считать продолжительность занятия каналов и по тарифам производить вычисление остатка на карточке.

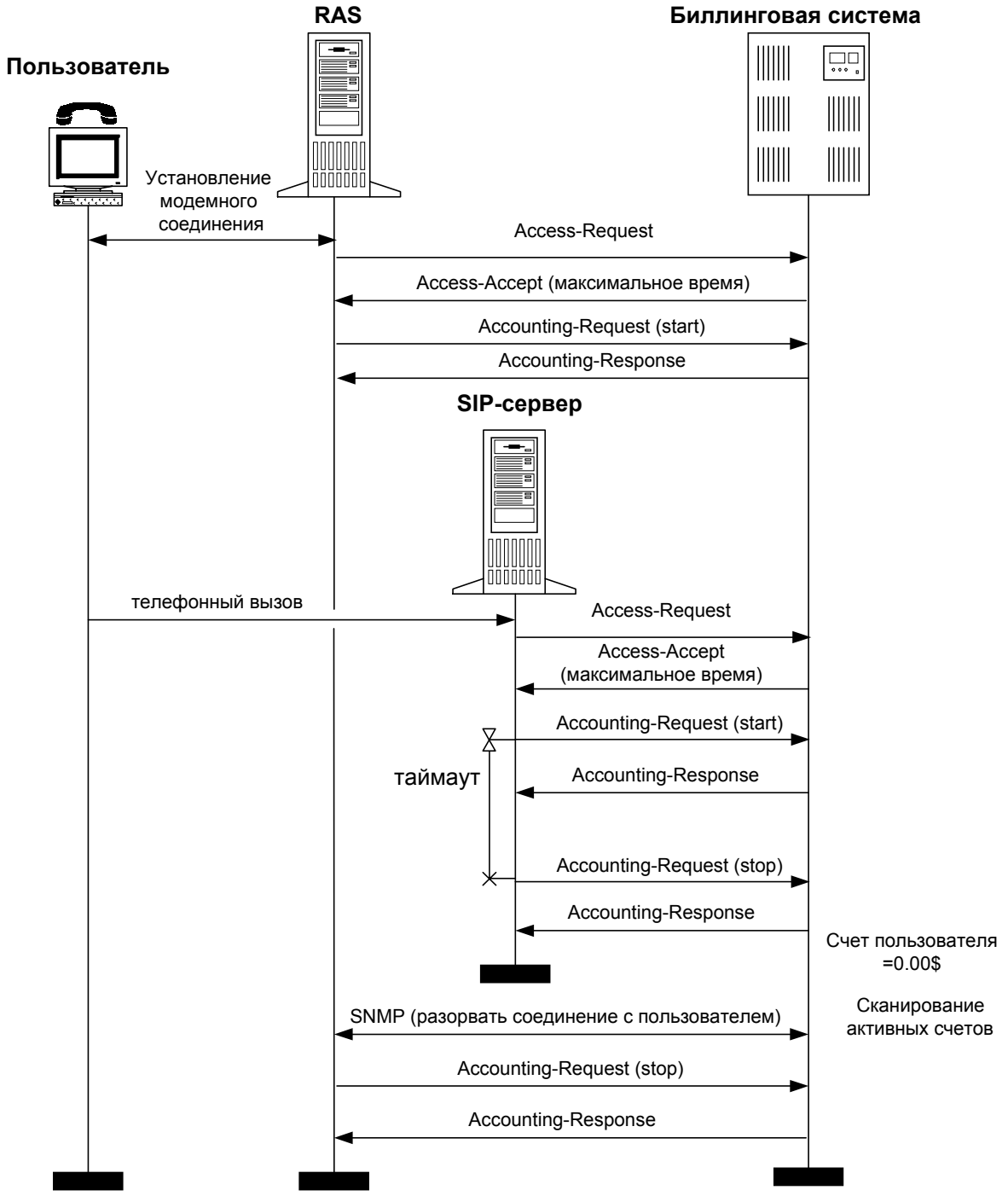

Рисунок 6 – Сценарий обмена сообщениям с биллинговой системой

После того, как биллинговая система принимает RADIUS-сообщение Access-Request от SIP-сервера, она проверяет, есть ли активные соединения, относящиеся к данному пользователю (карте). Если они есть, то необходимо вычислить время, отводимое для телефонного соединения. Возможно, что это время можно найти по формуле

$$t = \frac{S_{общ} - T_{пр} * t_{пр}}{T_{Internet} + T_{ip-telepnony}}$$

где *t – длительность разговора;*

$S_{общ}$ – сумма на счету с начала использования первой услуги (в данном случае Интернет);

$T_{пр}$ – тариф за первую услугу;

$t_{пр}$ – время между началом использования первой и второй услугами;

$T_{internet}$ – тариф за Интернет;

$T_{ip-telephony}$ - тариф за IP-телефонию.

Это время содержится в сообщении Access-Accept, посылаемом на SIP-сервер. На нем запускается таймер на время t. После его истечения, сервер посылает SIP-запросы BYE обоим пользователям и телефонное соединение разрывается. Кроме того, об окончании соединения сообщается биллинговому серверу с помощью RADIUS.

Биллинговый сервер непрерывно сканирует состояния счета и в случае его опустошения посылает SNMP сообщение на RAS о том, что необходимо разорвать модемное соединение, что он и делает.

При организации учета стоимости на базе SIP-сервера, ввиду особенностей протокола SIP, может возникнуть ситуация, когда сообщения о завершении сеанса связи пойдет не через этот сервер, а напрямую к другому пользователю. Т.е. запрос принять участие в сеансе связи - INVITE - вызывает посылку сообщения Access-Request. После установления разговорного соединения (прием ответа 200 OK) SIP-сервер шлет на RADIUS-сервер сообщение Accounting-Request (start). В ответе 200 OK в поле `Contact` может быть «прямой» адрес вызываемого пользователя и запрос BYE – означающий, что один из участников положил трубку, будет направлен на этот адрес, а не на адрес SIP-сервера. Для того, чтобы этого не произошло в протоколе SIP предусмотрены поля `Route` и `Record-Route`. Поле `Record-Route` добавляется SIP-сервером, который «хочет» быть на пути следующих запросов. Теперь все дальнейшие сообщения будут проходить через сервер, и он сможет посылать корректную биллинговую информацию.

При увеличении одновременного использования разных служб потребуются решение более сложных задач биллинга. Но ввиду того, что эта статья не посвящена построению биллинговых систем, оставим рассмотрение этих вопросов на будущее.

Для того чтобы ограничить использование ресурсов SIP-сервера и Интранета необходимо, во-первых, определить процедуры аутентификации клиентов на сервере, а во-вторых, настроить маршрутизатор так, чтобы он пропускал в выделенную сеть пакеты только с определенных IP-адресов, например, только с адреса SIP-сервера.

Первая задача решается с помощью процедуры аутентификации, предложенной в RFC 2543 и основанной на том, что SIP-сервер выдает в поле `Proxy-Authenticate` случайное число клиенту. Тот на основании указанного алгоритма, пароля и имени пользователя вычисляет в поле `Proxy-Authorization` ответное число и посылает его обратно серверу. По этому число сервер решает допускать или не допускать пользователя к услугам IP-телефонии.

Теперь необходимо, чтобы к ресурсам Интранет не имели доступ случайные люди. Для этого необходимо на маршрутизаторе прописать таблицы маршрутизации, так что пакеты, приходящие только с SIP-сервера, направлялись в Интранет. Но тут есть некоторые «подводные камни»: SIP-сервер обрабатывает исключительно сигнальные сообщения и обработкой речевых пакетов не занимается. Т.о. нельзя никак проследить за тем, чтобы речевые пакеты от пользователей, неоплативших услуги IP-телефонии, не пропускались в Интранет. Существует, как минимум, два пути решения этой проблемы. Первый - установить на узле межсетевой экран, совмещенный с SIP-сервером. В таком случае программное обеспечения сервера будет сообщать ему, какие порты необходимо открыть, а какие закрыть. Второй – это пропускание всего речевого трафика через SIP-сервер. Тогда достаточно маршрутизатор настроить так, чтобы он принимал пакеты только с IP-адреса этого сервера. Число обслуживаемых RTP-каналов (а, как известно, в IP-телефонии для передачи речевой информации используется протокол RTP – *Real-Time Protocol* [9]) ограничено быстродействием аппаратного обеспечения SIP-сервера.

Все пользователи IP-телефонии у себя на персональных компьютерах будут иметь специализированное ПО, работающее по протоколу SIP. Ввиду того, что все вызовы будут направляться на локальный SIP-сервер, принадлежащий провайдеру, было бы неплохо, чтобы пользователю не приходилось вручную настраивать адрес этого сервера. И это можно сделать с использованием протокола динамической конфигурации узла - DHCP (Dynamic Host Configuration Protocol) [10]. Для этого в черновиках IETF [11] были предложены специальные поля, в которых содержится информация о местоположении SIP-сервера, установленном на узле провайдера. DHCP-клиент, например, при запуске SIP-клиента на персональном компьютере пользователя, посылает DHCP-серверу широковещательный запрос с просьбой предоставить ему адрес SIP-сервера. В ответе DHCP-сервер возвращает этот адрес. Провайдер имеет возможность предотвратить передачу широковещательных запросов дальше в IP-сети.

Этим, конечно, не ограничивается круг проблем, но автор берет на себя смелость оставить их дальнейшее перечисление на будущее, а сейчас перейти к сделанным выводам.

6. Выводы

Какие же выводы, можно сделать из проведенного анализа?

Явное достоинство интеграции – это привлечение клиентов дополнительными возможностями. Кроме всех прочих услуг по доступу в Интернет, теперь они могут, не отходя от компьютера, сделать телефонные вызовы, а при организации услуги VL – они могут быть доступны для абонентов ТфОП, которые пытаются им позвонить.

Оплата за все услуги производится по единой карте. Единая биллинговая система производит все операции, необходимые для этого. Более того, при усовершенствовании биллинговой системы так, как описано выше, услуги можно использовать одновременно. Т.е. одни пользователи подключаются к Интернет, а другие могут в это время делать телефонные вызовы.

Провайдеру Интернет легче организовать доступ пользователей IP-телефонии к выделенным IP-сетям. Это исключает на пути соединения звенья с плохими характеристиками по задержке и джиттеру. Провайдер может при необходимости обеспечить необходимое качество обслуживания (QoS), что позволит существенно улучшить качество связи.

Возможно, что при некоторой модернизации серверов доступа, они смогут автоматически регистрировать пользователей на сервере местоположения, т.к. они назначают им IP-адреса и знают их текущее состояние.

Конечно, все эти возможности требуют некоторых затрат денежных средств и сил, но, возможно, они позволят провайдерам, получить от их внедрения доход, намного больший, чем они предполагают.

Список литературы:

1. World Telecommunication Policy Forum (WTPF 2001) "Report of the Secretary-General on IP Telephony" 31 January 2001**,** Geneva
2. RFC 1661. The Point-to-Point Protocol (PPP)/ W. Simpson, Editor. July 1994.
3. RFC 1157 Simple Network Management Protocol (SNMP)/ J.D. Case, M. Fedor, M.L. Schoffstall, C. Davin. May-01-1990.
4. RFC 2865. Remote Authentication Dial In User Service (RADIUS)/ C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000
5. ITU-T Recommendation H.323. Packet based multimedia communication systems. – Geneva, 1998.
6. RFC 2543. SIP: Session Initiation Protocol. M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg. March 1999.
7. RFC 2705. Media Gateway Control Protocol (MGCP) Version 1.0. / M. Arango, A. Dugan, I. Elliott, C. Huitema, S. Pickett. October 1999.
8. Б.С. Гольдштейн, А.В. Пинчук, А.Л. Суховицкий/ "IP-ТЕЛЕФОНИЯ". М.:Радио и связь, 2001 г.
9. RFC 1889. RTP: A Transport Protocol for Real-Time Applications/ Audio-Video Transport Working Group, H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. January 1996.
10. RFC 1531. Dynamic Host Configuration Protocol/ R. Droms. October 1993.
11. H.Schulzrinne, G.Nair "DHCP Option for SIP Servers", Internet Draft, Internet Engineering Task Force March 24, 2001, Work in progress.
12. N. Marly, D. Chantrain, J. Hofkens "Exploiting Similarities Between SIP and RAS: The Role Of The RAS Provider In Internet Telephony".
13. http://www.protei.ru