СОДЕРЖАНИЕ

Введение

В первом разделе рассматриваются известные к настоящему времени способы совместной передачи трафиков речи и данных.

Во втором разделе приводится концепция разделения трафиков на АТС.

В третьем разделе согласно разработанной концепции рассматриваются вопросы организации точек присутствия Интернет. Рассмотрение вопросов использования модемных пулов, использования АТС с комбинированной системой коммутации оформлено в виде отдельных подразделов.

В данном материале рассматриваются решения ведущих производителей телекоммуникационного оборудования, приводятся соответствующие схемотехнические решения сбора и пропуска IP трафика.

1 Организация передачи голосового трафика и трафика Интернет

Существует несколько путей решения проблемы совместной передачи голосового трафика и трафика сети передачи данных, которые представлены на рисунке 1.

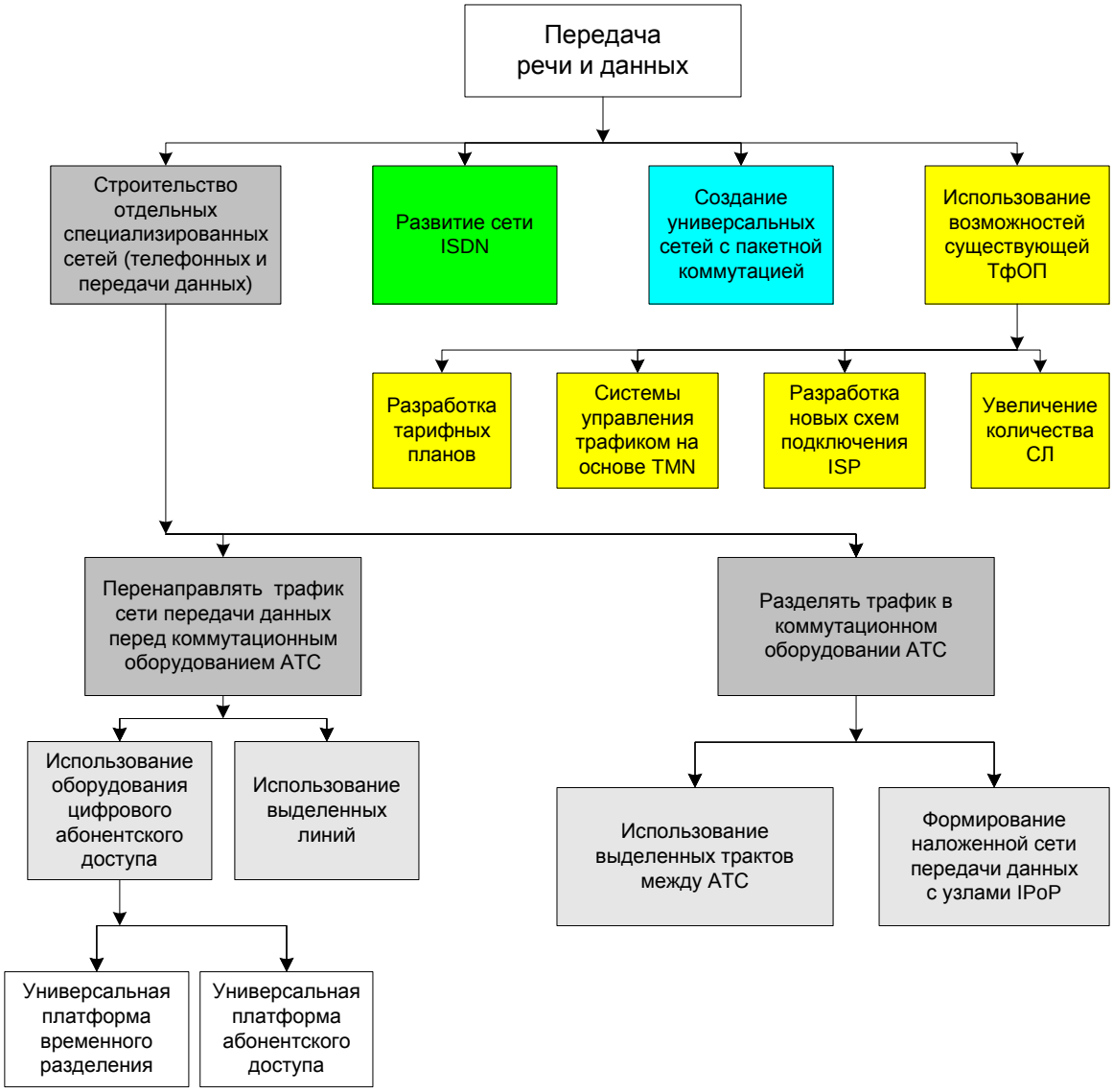


Рисунок 1 Пути организации совместной передачи голосового трафика и трафика сети передачи данных[1]

1.1 Строительство отдельных специализированных сетей

Строить новые сети всегда дорого, а создание и поддержка параллельных сетей предполагает удвоенные расходы. При этом понятно, что создавать необходимо именно сети передачи данных, поскольку традиционная ТфОП развита так, как никакая другая сеть. Следует учитывать также, что пакетная сеть может передавать голосовой трафик, позволяя получать дополнительные доходы.

[1] IPoP (Internet Point of Presence) – точка входа в сеть Интернет, обязательно имеющая уникальный IP-адрес.

1.1.1 Принципы разделения трафиков до оборудования коммутации

Разделение на входе станции «голосового» трафика и трафика Интернет является кардинальным решением проблемы. Этот способ распространен за рубежом и гарантирует, что указанная ранее проблема решена окончательно и не встанет снова при дельнейшем росте числа пользователей Интернет. Однако, он требует значительных затрат, так как требует установки на ТфОП дополнительного оборудования.

Тем не менее, для телефонного оператора данный способ имеет следующие преимущества:

- телефонный оператор уже является поставщиком услуг телефонии и имеет ту же зону потенциального охвата и для новых услуг;
- телефонный оператор имеет возможность предоставления комбинированных услуг на основе услуг телефонии и передачи данных;
- близость и объем клиентской базы будет привлекать других провайдеров услуг передачи данных и контента, которые в этом случае станут «субпровайдерами» телефонного оператора.

Крупный оператор может выступать в качестве «оператора операторов» всех видов услуг высокоскоростного мультимедийного доступа, организовав продажу или предоставление в аренду субпровайдерам емкости концентраторов доступа DSL и сети медных абонентских окончаний.

Телефонный оператор при этом будет обладать уникальными возможностями:

- создавать и предоставлять новые высокодоходные услуги;
- использовать услуги, созданные и предоставляемые «субпровайдерами», как строительные блоки для своих услуг;
- предоставлять свои услуги «субпровайдерам на коммерческой основе. «Субпровайдеры» могут осуществлять «розничную продажу» этих услуг своим корпоративным или индивидуальным клиентам, а также использовать эти услуги в качестве «строительных блоков» для создания своих услуг;
- осуществлять дифференцированный биллинг и взаиморасчеты по типам услуг между провайдерами нижнего уровня.

Телефонный оператор может предоставлять IP-услуги субпровайдерам, корпоративным клиентам и физическим лицам. Принимая во внимание традиционную направленность телефонных операторов на розничную продажу услуг[2], услуги первых двух типов также следует развивать, хотя бы потому, что оптовая продажа услуг может принести более быстрый возврат вложенных средств за счет отсутствия дополнительных затрат на развитие инфраструктуры, характерных для розничных продаж. Кроме того, оптовые продажи и продажи корпоративным клиентам могут в ряде случаев служить дополнительным средством привлечения клиентов.

1.1.1.1 Использование выделенных линий

В случаях, когда точки подключения (к узлу сети и пользовательскому оконечному устройству) расположены в пределах одного города или пригородов могут использоваться модемы для физических линий, позволяющих организовать высокоскоростные каналы связи на медных линиях городской телефонной сети. Как правило, модемы каждой фирмы-производителя имеют свой уникальный протокол, и поэтому должны использоваться в паре на обоих концах линии. Это не вызывает серьезных неудобств, так как модемы для

[2] Телефонный оператор, являясь «оператором операторов» и обладая подключенными провайдерами Интернет, может предоставлять дополнительную услугу динамического выбора провайдера (“service selection”) своим розничным клиентам, которые могут выбирать провайдеров или отдельные услуги, используя графический интерфейс своего компьютера. Это будет, с одной стороны, отдельным доходным бизнесом для телефонного оператора, с другой – дополнительным средством привлечения клиентов, получающих возможность всегда выбирать провайдера или услугу с минимальными тарифами. Наконец, телефонный оператор получает возможность всегда предлагать минимально возможные на рынке тарифы.

физических линий не работают через коммутируемую сеть, следовательно, каждое соединение организуется на длительное время и может быть оборудовано одинаковыми модемами. С точки зрения стыковки с оконечным оборудованием, модемы для физических линий стандартизованы по типам пользовательских интерфейсов. Как правило, это синхронные интерфейсы V.24, V.35 или G.703. Большинство модемов для физических линий основаны на технологиях xDSL.

1.1.1.2 Использование оборудования цифрового абонентского доступа

Технологии семейства цифрового абонентского доступа xDSL позволяют осуществлять высокоскоростную передачу по абонентской линии, но требуют специального оборудования как на интерфейсе со станцией, так и на стороне абонента (рисунок 2). С помощью этого оборудования организуется два потока передачи данных – входящий поток от сети к пользователю и исходящий поток от пользователя в сеть – и канал обычной телефонной связи. Канал телефонной связи выделяется с помощью фильтров, что гарантирует работу телефона даже при аварии соединения xDSL. В зависимости от разновидностей xDSL может обеспечивать симметричность или несимметричность потоков данных.

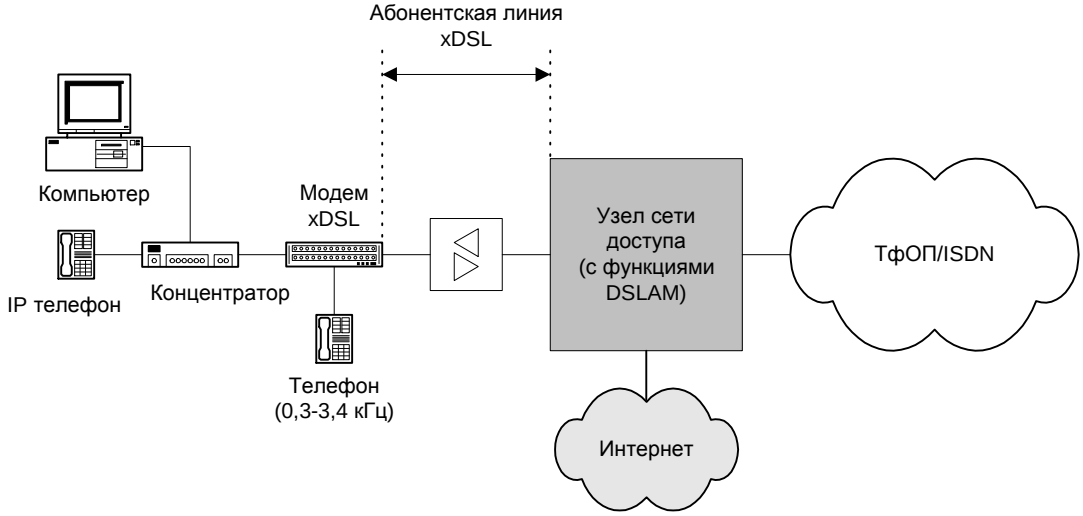


Рисунок 2 Разделение трафиков на уровне сети доступа[3]

Основные недостатки использования внешних xDSL устройств:

1. Необходимость развертывания собственной опорной сети передачи данных, что означает создание новой инфраструктуры, отдельной системы эксплуатации и техобслуживания и т.д. Все это ведет к высокой стоимости сети, как на этапе начальных инвестиций, так и в процессе работы.
2. Возможность использования технологии xDSL во многом зависит от качества и конструктивного исполнения кабельной сети.
3. Большинство технологий xDSL не переносят наличия высоких перекрестных помех между используемой парой проводов и другими парами, входящими в тот же пучок кабеля.
4. Неприспособленность Интернет в его теперешнем виде к предоставлению услуг связи в реальном масштабе времени с гарантированной доставкой информации и лимитированным временем задержки.

[3] Мультиплексор доступа DSLAM выделяет подканалы из общего канала и отправляет голосовой подканал в 3100 Гц на АТС, а высокоскоростные каналы данных направляет в маршрутизатор, который должен находиться рядом с DSLAM

Главными достоинствами технологий xDSL является:

1. использование обычных витых пар медных проводов телефонных кабелей (xDSL образует сеть, «наложенную» на существующую сеть телефонной связи);
2. не требуется дорогостоящей модернизации коммутационного оборудования.

1.1.1.2.1 Универсальная платформа временного разделения

Особенность данной технологии заключается в месте установки оборудования. Универсальная платформа временного разделения позволяет направлять «голосовой» трафик в телефонную сеть общего пользования, а IP-трафик – в сеть передачи данных, при этом разделение трафиков осуществляется в оборудовании, установленного у абонента, а трафик IP может и не попадать на местный узел связи.

Пример такой платформы, построенной на базе оборудования фирмы NATEKS, приведен на рисунке 3.

В этом рисунке использовались следующие обозначения:

- FlexDSL – xDSL модем абонентского доступа;
- CMU – модуль SNMP, выполняющий роль агента для группы из 32 устройств.
- FlexGain A/T 155 – волоконно-оптические системы передачи Синхронной Цифровой Иерархии (SDH);
- FlexGain 4XE – система кросс-коммутации, позволяющая оператору выделять отдельные тайм-слоты, делить поток E1 на несколько потоков, преобразовывать различные типы сигнализаций, организовывать асинхронный порт RS232 для дистанционного конфигурирования.
- DLC 1100E – цифровой мультиплексор абонентского выноса;
- FlexGainPlex – мультиплексор, предназначенный для выделения аналоговых окончаний (FXO, FXS и ТЧ) и канала передачи данных (V.35) из потока E1.
- FlexDSL Megatrans – магистральная система передачи, основанная на xDSL-технологиях;
- FlexGain FOM4 – мультиплексор, обеспечивающий передачу 4-х каналов E1 по волоконно-оптической связи.

Подключение пользователей по выделенным цифровым каналам (DS0, E1, PRI, E3,…) в данной работе рассматривается как частный случай реализации универсальной платформы временного разделения.

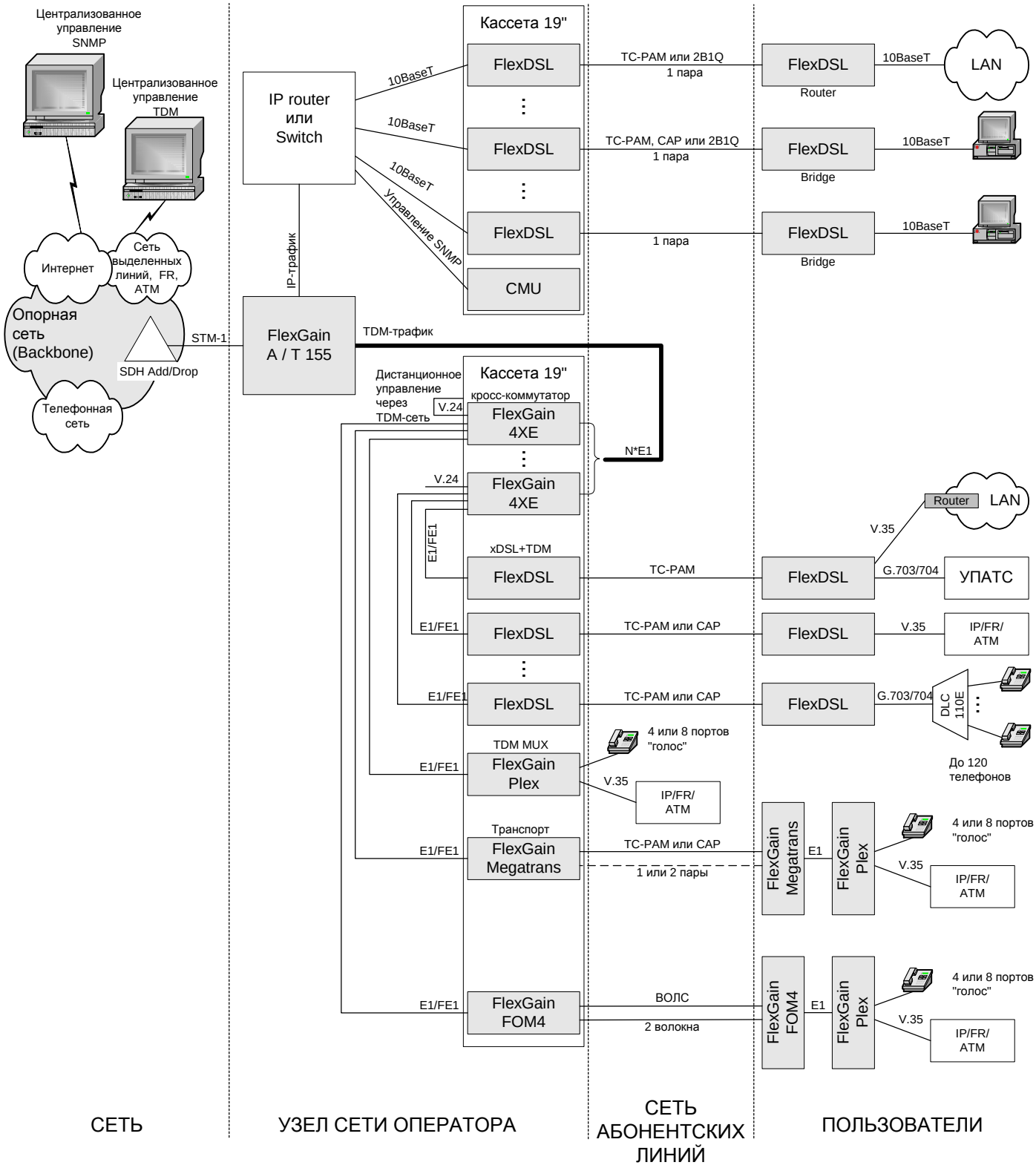


Рисунок 3 Универсальная платформа временного разделения

1.1.1.2.2 Универсальная платформа абонентского доступа

Универсальная платформа абонентского доступа, построенная на базе оборудования фирмы NATEKS, представлена на рисунке 4, где:

- NTU128 Voice – IDSL модем, предназначенный для организации высокоскоростного канала передачи данных и дополнительного телефонного

канала по двухпроводной физической линии и позволяет одновременно подключаться к телефонной сети и Интернет в режиме On-line.

- FlexGain UG5 – система уплотнения (передачи) ISDN линий.
- FlexGain PCM – система уплотнения абонентских линий (каждый канал передается методом ИКМ-кодирования со скоростью преобразования 64 кбит/с в соответствии с G.711).
- CAP Splitter – аналоговый разделитель, позволяет вести DSL-передачу «поверх» обычного телефонного разговора по абонентской линии.

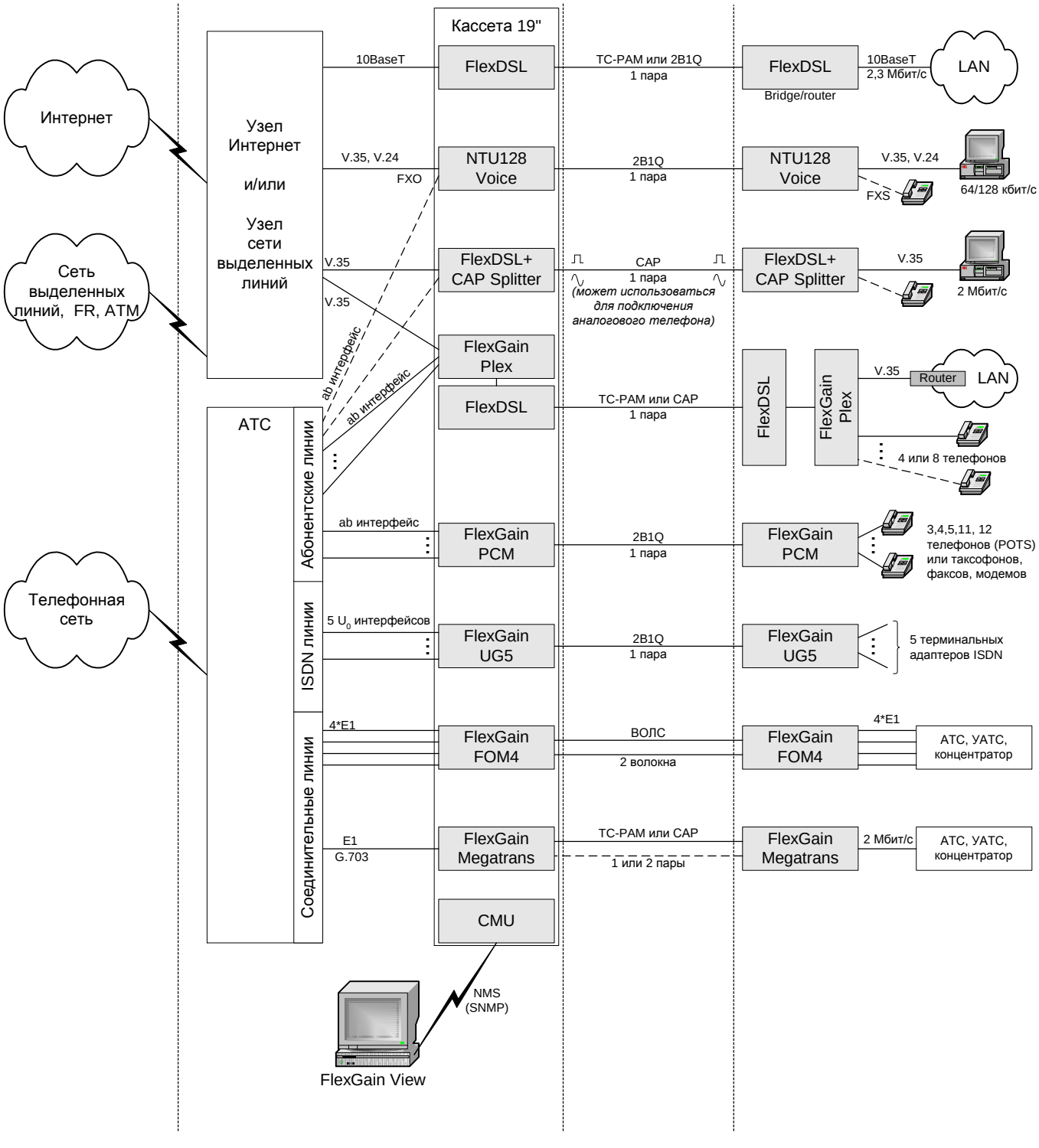


Рисунок 4 Универсальная платформа абонентского доступа

На сегодняшний день из-за высокой стоимости оборудования xDSL организовывать доступ в Интернет с использованием цифровых абонентских линий могут себе позволить лишь корпоративные пользователи услуг Интернет и немногие состоятельные квартирные абоненты. Рядовые же квартирные пользователи услуг Интернет вынуждены продолжать использовать ТфОП в качестве сети доступа к узлу ISP[4].

Для расширения сетей доступа в Интернет целесообразным представляется развертывание операторами ТфОП и ISP на городских телефонных сетях домашних компьютерных сетей. Поставщиками услуг Интернет домашние сети рассматриваются, как средство коллективного доступа в Интернет рядовых квартирных абонентов. Кроме постоянного, круглосуточного доступа в сеть Интернет пользователи домашних сетей получают те же сетевые услуги и возможности по образованию и развлечению, что и пользователи локальных компьютерных сетей отдельных предприятий.

Типичная схема домашней сети в пределах одного городского квартала или микрорайона представлена на рисунке 5.

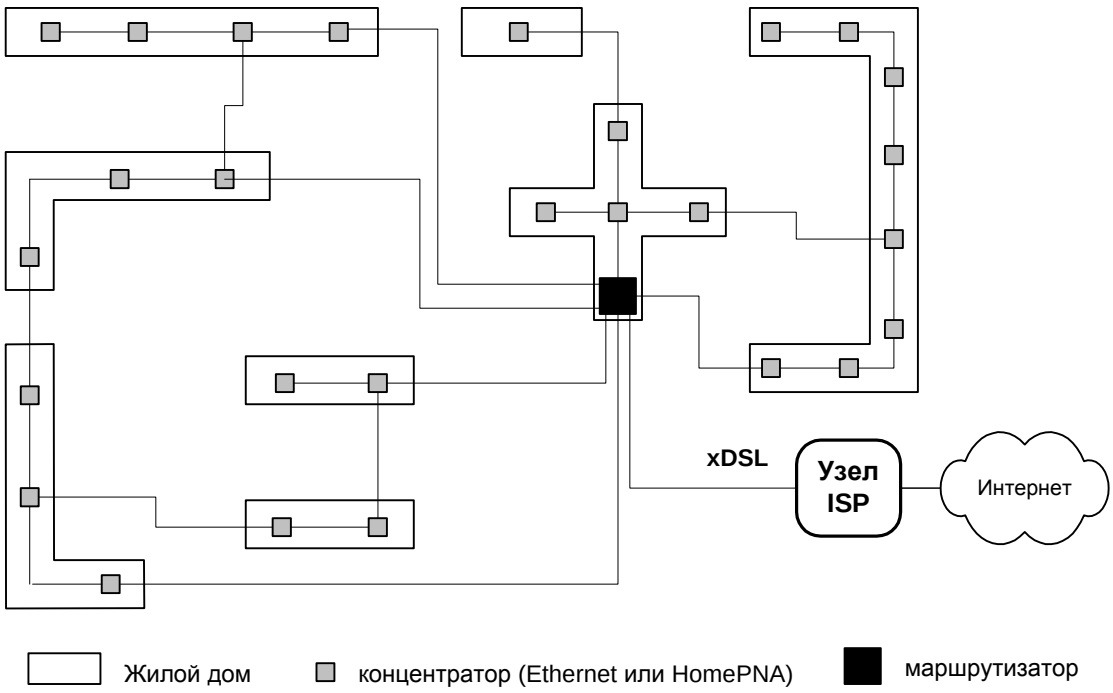


Рисунок 5 Схема домашней сети масштаба городского квартала

В квартале выбирается точка присутствия ISP и в ней устанавливается маршрутизатор. Вся маршрутизация информационных потоков пользователей домашней сети квартала будет происходить в данной точке. К маршрутизатор подключаются отдельные дома квартала. В подъездах домов устанавливаются концентраторы, в которые включаются пользователи домашней сети.

Домашняя сеть отдельного городского квартала является распределительной подсетью общегородской сети доступа в Интернет.

На участке сети от маршрутизатора квартала до узла ISP используется канал, построенный на оборудовании цифровых абонентских линий (ADSL, VDSL, HDSL, SDSL). В данном случае расходы по установке, использованию и обслуживанию цифровой абонентской линии распределяется между всеми абонентами микрорайона, пожелавшими стать пользователями домашней сети, и являются не столь высокими, как в случае индивидуального использования одним абонентом цифровой абонентской линии.

На участке от маршрутизатора квартала до подъезда дома квартала и внутри подъездов дома могут использоваться технологии Ethernet и HomePNA.

[4] ISP – поставщик услуг Интернет (провайдер).

Технология Ethernet является лидером среди технологий локальных компьютерных сетей и ее использование при построении домашних сетей является предпочтительным. Однако использование Ethernet потребует как минимум прокладки внутри здания кабеля на витой паре не ниже 4 категории, что значительно увеличит стоимость организации домашней сети и потребует дополнительных расходов от пользователей.

Технология HomePNA позволяет избежать дополнительных затрат на прокладку кабелей, так как дает возможность использовать в качестве среды передачи сигналов существующую абонентскую проводку телефонной сети (провод марки ТРП). Кроме этого, технология HomePNA может работать и по линиям городской радиотрансляционной сети.

При использовании абонентской проводки телефонной сети телефонной розетка в квартире может использоваться не только для подключения телефонного аппарата, но также становится сетевым портом домашней сети.

Технология HomePNA обладает следующими характеристиками:

- в HomePNA применяется методика IEEE 802.3 CSMA/CD, используемый диапазон частот 5,5-9,5 МГц.
- HomePNA версии 1.0 обеспечивает работу сети с расстоянием между узлами не менее 150 м. Следующая версия стандарта (HomePNA 2.0) обеспечивает дальность не менее 350 м;
- скорость передачи информации в стандарте HomePNA 1.0 составляет 1 Мбит/с. Спецификация HomePNA 2.0 обеспечивает скорость передачи данных 10 Мбит/с при совместимости с оборудованием предыдущей версии;
- HomePNA позволяет повышать скорость передачи данных и расширять функциональные возможности сети, сохраняя при этом ее совместимость с предыдущими спецификациями технологии;
- Домашняя сеть, базирующаяся на HomePNA не оказывают никакого влияния и не препятствуют работе существующей телефонной связи и цифровых абонентских линий. Для одновременного использования одной телефонной линии и для существующих телефонных служб, и для передачи сетевого трафика используется принцип частотного разделения - каждой службе выделяется свой частотный спектр, который не пересекается со спектрами других служб. Благодаря использованию частотно-избирательных фильтров устройства, относящиеся к одной службе, могут обмениваться информацией, не оказывая никакого влияния на устройства, работающие в другом частотном диапазоне;
- HomePNA дает возможность использования случайных и нестандартных топологий проводки, так как структура телефонной проводки внутри каждой квартиры или дома не только не может быть известна заранее, но и изменяется день ото дня;
- HomePNA дает возможность работы в условиях сильного затухания сигнала и его отражений, которые характерны для разветвленных топологий проводки, так как передаваемый по такой проводке электрический импульс в значительной мере теряет свою энергию, проходя по проводам;
- HomePNA обладает высоким уровнем защиты от шумов изменяющегося уровня бытовых приборов, кондиционеров воздуха и других электрических приборов;
- HomePNA не восприимчива к динамическим изменениям характеристик линии передачи, являющихся следствием изменения в широких пределах рабочих характеристик телефонных аппаратов и других устройств, подключаемых к телефонной линии;
- HomePNA предусматривает использование той же модели драйвера Windows NDIS, который используется сетевыми картами Ethernet. Работа по принципу Plug-and-Play, поддерживаемая операционными системами Microsoft Windows, полностью освобождает пользователя от необходимости заниматься сложными настройками программного обеспечения.

1.1.1.3 Решения производителей

1.1.1.3.1 Siemens – EWSD InterNode

EWSD InterNode в различных версиях EWSD предлагает высокоскоростной доступ с помощью модулей xDSL:

- UDSL (Universal Digital Subscriber Line) – обеспечивает скорость передачи до 1,5 Мбит/с к абоненту (длина линии до 4,5 км) и 512 кбит/с – от абонента;
- SDSL (Symmetrical Digital Subscriber Line). Технология SDSL обеспечивает скорость передачи до 2,3 Мбит/с (длина линии до 4 км) в обе стороны. SDSL-модуль обеспечивает 32×64 кбит/с каналов в дополнение к стандартным 2B+D-каналам базового доступа, которые в зависимости от типа трафика могут быть соединены с сетями с коммутацией каналов или пакетов. При этом все стандартные ISDN-услуги полностью доступны.
- ADSL (Asymmetrical Digital Subscriber Line). Доступ по ADSL обеспечивает скорость передачи до 8 Мбит/с к абоненту (длина линии до 4,5 км) и 768 кбит/с – от абонента.

EWSD InterNode интегрирует эти новые линейные карты в уже существующие станции EWSD как часть цифрового абонентского блока DLU. Все новые модули полностью совместимы с классическими аналоговыми и ISDN-модулями и могут быть установлены в существующие DLU.

1.1.1.3.2 IskraTel – SI 2000

В модули абонентского доступа интегрирована технология ADSL.

1.1.2 Принципы разделения трафиков в оборудовании коммутации

Управление трафиком Интернет как частью трафика ТфОП, обеспечивая прямой контроль за абонентскими линиями за счет использования уже существующей инфраструктуры, позволяет оператору ТфОП стать провайдером услуг сети Интернет, не только сохраняя, но даже увеличивая количество своих абонентов.

В зависимости от структуры сети разделение трафиков может осуществляться на уровне транзитных узлов (ТУ) – УИС/УВС, УВТС, ЦС или на уровне РАТС, ОС, УСС. При этом возможен такой вариант, когда ISP имеет, например, для каждого узлового района свой номер (первые одна или две цифры которого совпадали бы с соответствующими цифрами номера вызывающего абонента, а остальные были бы одинаковы на всей местной сети). В случае если АТС вызывающего абонента не принадлежит узловому району (где определен серийный номер), соединение не предоставляется. Одновременно может выдаваться сообщение о необходимости использования другого серийного номера. Может использоваться и другая схема, когда как только абонент использует связь с серийным номером вне своего узлового района, используется повременной тариф междугородного соединения. Для тех абонентов, у которых в их узловом районе вообще отсутствуют серверы доступа, временно может использоваться обратное соединение «call back»[5] с ближайшего сервера доступа.

Такой подход потребует установки маршрутизаторов на необходимых узлах и аренды выделенных трактов между АТС либо использования выделенной сети передачи данных. Конкретные места установки могут определяться совместно с оператором местной сети связи.

Таким образом, принципиально существуют два варианта разделения трафиков на уровне коммутационного оборудования:

[5] Функция “call back ” заключается в том, что после аутентификации пользователя оборудование провайдера обрывает связь с модемом пользователя и выполняет звонок по номеру телефона, введенному самим пользователем или зарегистрированному за ним. При использовании этой функции за телефонный звонок платит не пользователь, а сам провайдер.

1. выделение отдельных направлений на ТфОП/ISDN для подключения к провайдеру (выделение трактов между АТС);
2. разделять трафик в узлах IPoP, образующих наложенную сеть доступа к Интернет.

1.1.2.1 Выделение отдельных соединительных линий между АТС для передачи трафика данных

Сущность данного метода заключается в том, что из пучков СЛ, связывающих АТС, выделяются отдельные СЛ (субтранки), которые используются для обслуживания определенного серийного номера провайдера. Организация субтранков между АТС ТфОП/ISDN для подключения к провайдеру абонентов представлена на рисунке 6.

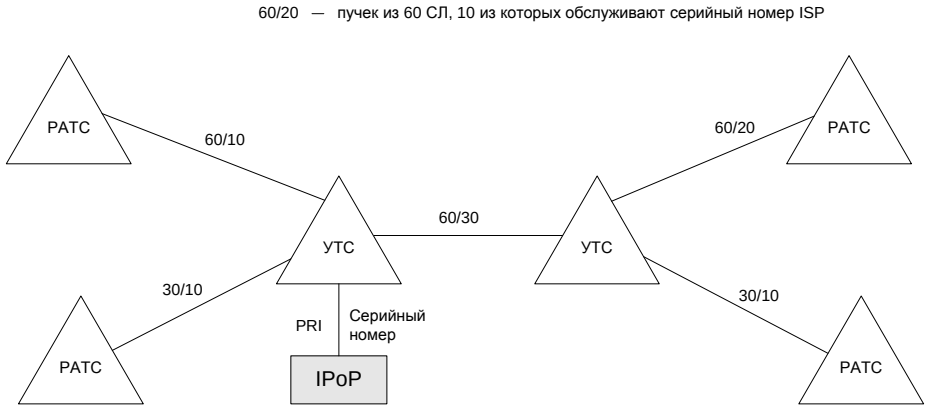


Рисунок 6 Организация субтранков в пучках СЛ для обслуживания серийного номера ISP

Как видно из рисунка 6, рассматриваемый вариант делится на несколько подвариантов, определяемых точкой организации серийного номера:

- исходящая станция (рисунок 7);
- входящая станция (рисунок 8),
- транзитный узел (рисунок 9, рисунок 10)[6].

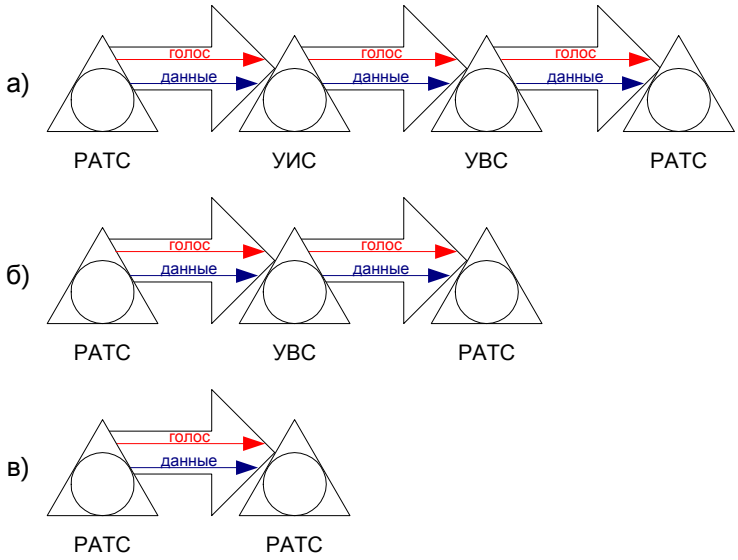


Рисунок 7 Выделение субтранков в исходящих СЛ на РАТС пользователя Интернет

Представленные на рисунке 7 варианты разделения трафиков могут использоваться в следующих случаях:

[6] На Рисунок 7 – Рисунок 10 «данные» – «модемный» вызов

- вариант а) может быть использован только на тех ГТС, где началось создание УИС/УВС;
- вариант б) может быть использован на ГТС, где используется районированная с узлами входящих сообщений схема построения сети;
- вариант в) может быть использован на ГТС, где применяется районированная без узлообразования схема построения сети.

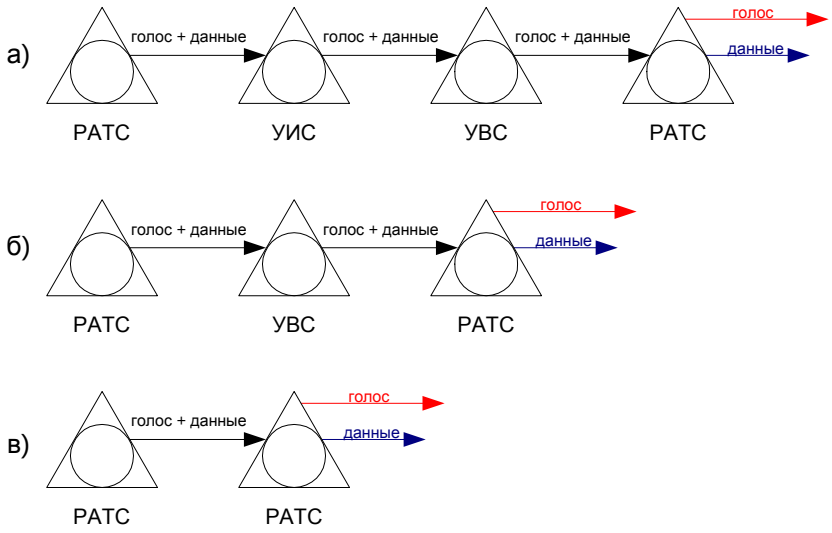


Рисунок 8 Разделение «голосового» трафика и трафика передачи данных на РАТС ISP

Представленные на рисунке 8 варианты разделения трафиков никоим образом не решают обозначенные ранее проблемы совместной передачи «голосового» трафика и трафика передачи данных, поэтому из дальнейшего рассмотрения их следует исключить.

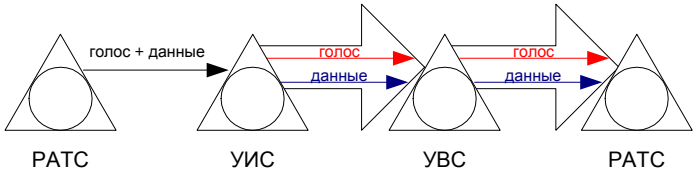


Рисунок 9 Выделение субтранков в исходящих СЛ на УИС

Представленный на рисунке 9 вариант разделения трафиков может быть использован на ГТС с УИС.

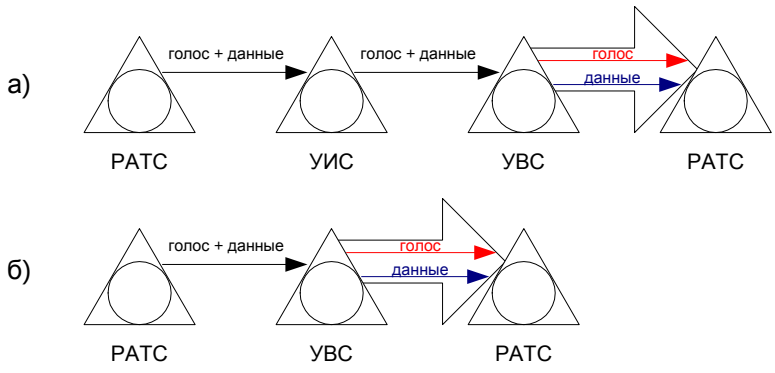


Рисунок 10 Выделение субтранков в исходящих СЛ на УВС

Представленный на рисунке 10 вариант а) характерен для ГТС с УИС, вариант б) характерен для ГТС с УВС.

На основе анализа рисунков 7–10, а также с учетом предполагаемого включения провайдеров в транзитные узлы телефонной сети, может быть составлена таблица 1.

Таблица 1

Схема построения ГТС	Точка разделения трафиков			
	исходящая РАТС	УИС	УВС	Входящая РАТС
ГТС с УИС/УВС	Рисунок 7 а)	Рисунок 9	Рисунок 10 а) точка подключения ISP	Отсутствует
ГТС с УВС	Рисунок 7 б)	Отсутствует	Рисунок 10 б) точка подключения ISP	Отсутствует
ГТС без узлообразования	Рисунок 7 в)	Отсутствует	отсутствует	Отсутствует

На СТС разделение трафиков речи и данных возможно на уровне ЦС. При доступе к Интернет через АМТС, при связи каждой РАТС с АМТС по ЗСЛ, организация субтранков может быть осуществлена на уровне РАТС.

Реализация варианта организации субтранков в пучках СЛ имеет следующие особенности:

- реализация данного варианта возможна только на цифровых АТС;
- производители АТС гарантируют организацию субтранков только в окружении АТС собственного производства;
- необходимо внесение изменений в программное обеспечение на АТС, где осуществляется организация субтранка, а также на АТС, где организован серийный номер;
- выбор направления будет осуществляться только после набора всех цифр номера;
- для каждого серийного номера организуется свой субтранк в пучках СЛ;
- должны быть определены серийные номера коммутируемого доступа провайдеров и определен механизм их своевременного конфигурирования.

Существуют следующие варианты облегчения решения задачи:

1. в качестве серийного номера будет использоваться специфический номер (например, один из номеров узла спецсвязи);
2. использование сигнализации ОКС №7.

Рассматривая первый вариант, стоит отметить постановление Госкомсвязи РФ №10-1 от 28.04.98 г., где предусматривается возможность выделения для нужд ISP в отношении местных телефонных сетей сокращенных индексов спецслужб (рисунок 11). В этом случае устанавливать оборудование доступа можно только на узле спецслужб. Однако с учетом возрастающей нагрузки в данном направлении потребуется увеличить емкости пучков соединительных линий, идущих от всех узлов ГТС к УСС.

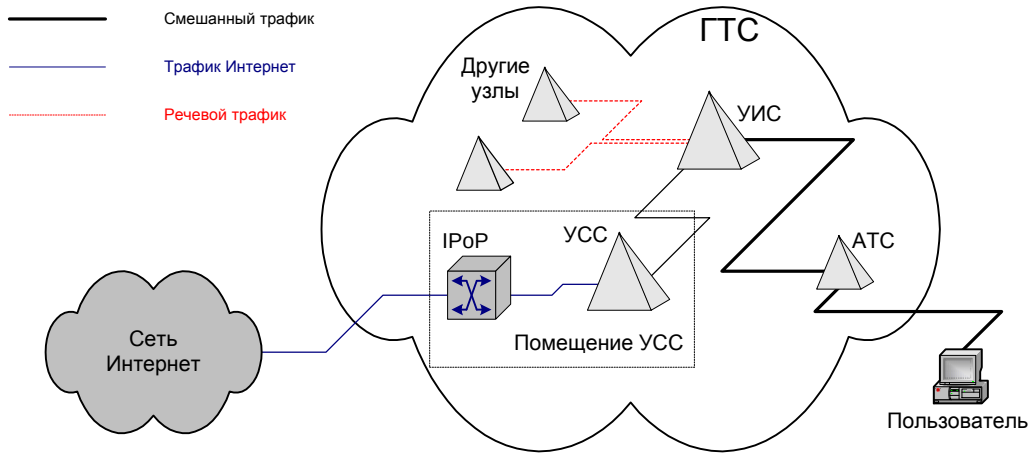


Рисунок 11 Включение оборудования доступа на ГТС с разделением трафика на УСС

Во втором случае, использование сигнализации ОКС №7 позволяет:

- отказаться от конфигурирования программного обеспечения АТС;
- упрощает процедуру организации субтранков в пучках СЛ;
- облегчает своевременное конфигурирование серийных номеров ISP.

Так как услуга «call back» белорусскими провайдерами практически не применяется, ранее рассматривался трафик, создаваемый в направлении пользователь Интернет – ISP. Однако при использовании ISP для доступа к Интернет услуги «call back» происходит перенос нагрузки с входящих пучков СЛ АТС включения ISP на исходящие пучки СЛ.

1.1.2.2 Формирование на ТфОП наложенной сети передачи данных с узлами IPoP

Сеть передачи данных с узлами IPoP, взаимодействуя с магистральной сетью Интернет, обеспечивает отвод трафика IP пакетов от местной телефонной сети. Так как трафик сети передачи данных с узлами IPoP составляют IP пакеты, то на канальном, сетевом и транспортном уровнях целесообразно использовать технологии, работающие со стеком протоколов TCP/IP.

Рассматриваемый вариант неизбежно приводит к перераспределению функций поставщиков услуг при предоставлении доступа к сети Интернет. Оператор сети связи общего пользования в данном случае может частично или полностью взять на себя функции провайдера услуг передачи данных, что реально рассматривается как защита инвестиций оператора ТфОП при конвергенции этих сетей.

Использование на ТфОП оборудования с окончаниями IP с формированием наложенной сети IPoP предполагает реализацию окончаний IP как на уровне сети доступа, так и на уровне оконечных и транзитных станций (рисунок 12).

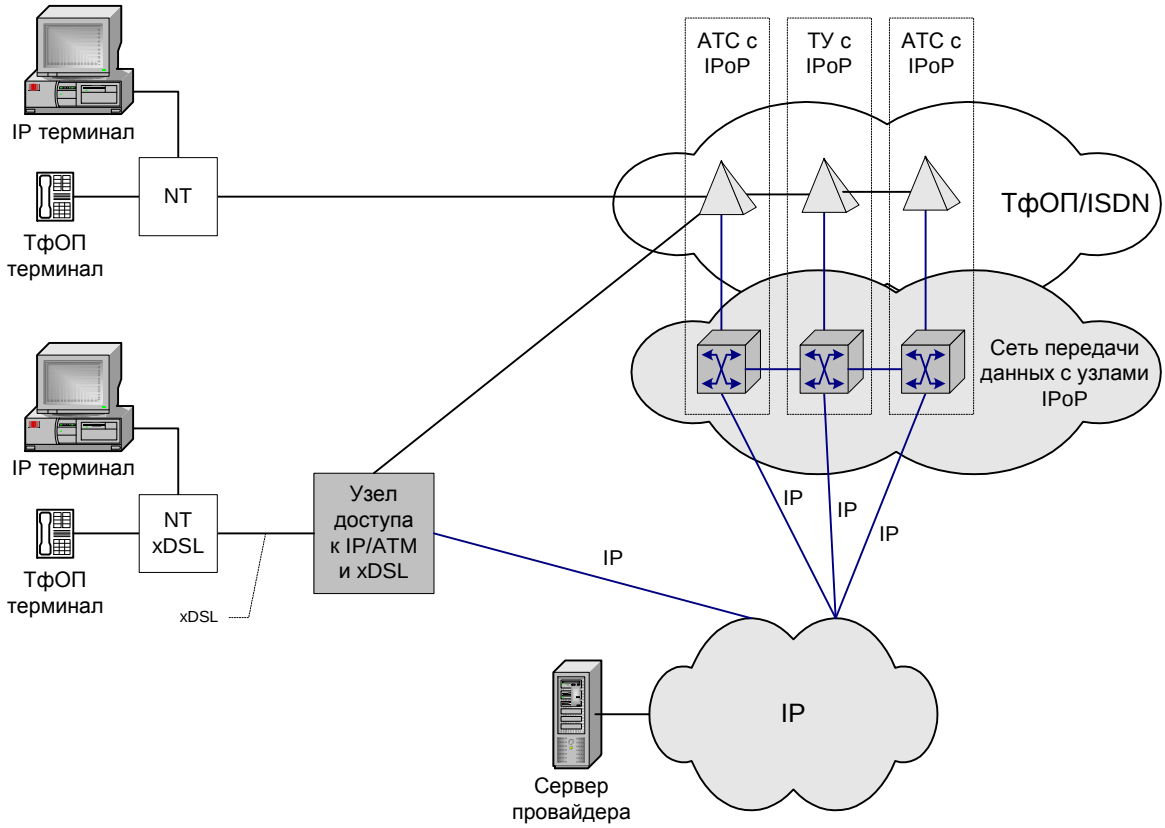


Рисунок 12 Организация взаимодействия сетей ТфОП/ISDN и IP с использованием оборудования IPoP

Конфигурация сети доступа с узлами IPoP может быть выполнена в следующих вариантах:

- узлы IPoP размещаются на АТС в качестве шлюзов передачи данных, направляя вызовы, поступившие на модемный пул по сети IPoP до узла, где установлен RAS провайдера (используется оптовая продажа портов – см. приложение А);
- сеть IPoP является распределенной сетью Интернет, при этом подключение ISP осуществляется к пограничному маршрутизатору.

Однако и в первом, и во втором случаях, сеть передачи данных с узлами IPoP, посредством которой пользователи подключаются к сети Интернет, должны обеспечивать:

- возможность выбора, как вида услуг, так и их поставщика;
- множественный доступ услуг к потребителю от различных конкурирующих поставщиков.

Более подробно вопросы подключения ISP к сети IPoP рассматриваются в разделе «Подключение поставщиков услуг Интернет».

1.2 Развитие сети ISDN

Цифровая сеть с интеграцией служб – Integrated Services Digital Network, ISDN, объединяет службы с коммутацией каналов и с пакетной коммутацией, предоставляя пользователям широкий набор услуг цифровой телефонии, возможность одновременной передачи данных, а также услуги видеоконференц-связи. ISDN-сети состоят из ISDN-АТС, которые коммутируют цифровые потоки.

Абонирование линии базового доступа ISDN и приобретение соответствующего оконечного оборудования является простым, но никак не кардинальным решением проблемы. Такой подход позволит частично решить проблему за счет использования цифровой передачи сигнала вплоть до абонентской установки и предоставления двух независимых каналов на интерфейсе пользователя, так как в технологии ISDN есть свои проблемы:

- необходимость замены программного обеспечения каждой АТС при введении услуг ISDN. При этом время службы коммутационного оборудования составляет несколько десятков лет, и менять его программное обеспечение оказывается дорого;
- высокая стоимость оборудования ISDN;
- подключение к сетям ISDN осуществляется несколько сложнее, чем к телефонным;
- услуги ISDN в настоящее время могут быть абонированы не везде.

Тем не менее, построение наложенной сети на базе удаленных узлов сети доступа, размещаемые в автозалах существующих АТС, позволяет решать проблему при относительно небольших инвестициях оператора сети связи общего пользования. Однако следует учитывать, что для эффективного использования скоростей доступа более 64 или 128 кбит/с при массовом внедрении Интернет необходимо иметь высокоскоростные каналы между узлами сети, что потребует больших капиталовложений.

1.3 Создание универсальных сетей с пакетной коммутацией

Вопросы конвергенции существенным образом затрагивают телефонные сети общего пользования. Согласно рекомендации Y.105 ITU-T они рассматриваются как один из элементов сети доступа к Интернет с точки зрения информатизации общества и создания глобальных и национальных инфраструктур (GII и NII). Последние несколько лет совершенно четко просматривается тенденция слияния ТфОП и сетей с пакетной коммутацией – это видно из документов, разрабатываемых в ETSI, ITU-T, IETF, а также следует из анализа последних разработок всех крупнейших производителей телекоммуникационного оборудования (Lucent Technologies, Siemens, Alcatel, Ericsson, Nortel Networks и др.).

Новая идеология базируется на передаче голосового (и не только голосового) трафика между всеми элементами ТфОП – абонентами, станциями, транзитными коммутаторами – по единой универсальной сети с коммутацией пакетов. Здесь универсальность понимается в двух аспектах. С одной стороны, сеть должна обеспечивать эффективную передачу разнородного трафика, с другой стороны, сеть должна использоваться как для передачи клиентского трафика, так и для передачи технологической информации оператора.

Общей технологической основой универсальных (конвергентных) сетей являются универсальные среды, осуществляющие передачу цифровых потоков, несущих любую мультимедийную информацию, и специальные транспортные протоколы, позволяющие осуществлять эту передачу с заданной скоростью и качеством.

Сети общего пользования нового поколения (рисунок 13), которые основаны на принципах коммутации пакетов и протоколах, разработанных для передачи данных, обещают как более низкие цены, так и большую функциональность. Представленная на рисунке 13 структура обусловлена тем, что именно IP является движущей силой конвергенции сетей связи, информационных технологий и мультимедийных продуктов. На сетевом уровне IP создает единую управляемую приложениями интерактивную сеть, способную обеспечить высокоскоростную пакетную сеть с любыми беспроводными или проводными абонентскими устройствами проще и дешевле чем традиционные сети.

В основе такого подхода лежат такие достижения последних лет, как:

- разработка телекоммуникационных сетей с очень высокой пропускной способностью;
- разработка эффективных методов сжатия информации в цифровых потоках;
- разработка эффективных методов контроля и обеспечения качества передачи разнородной цифровой информации в транспортных средах.

Решение, представленное на рисунке 13, устраняет проблему дефицита коммутационных мощностей ТфОП (вместо них будут использоваться сравнительно легко наращиваемые маршрутизаторы) и позволяет оператору сосредоточиться на поддержке

необходимой пропускной способности своих каналов, то есть на строительство мощных транспортных сетей.

Новые сети будут представлять собой исключительно сети передачи данных. Для голосового трафика операторы построят шлюзы в ТфОП и ISDN, преобразующие речевой поток в набор пакетов.

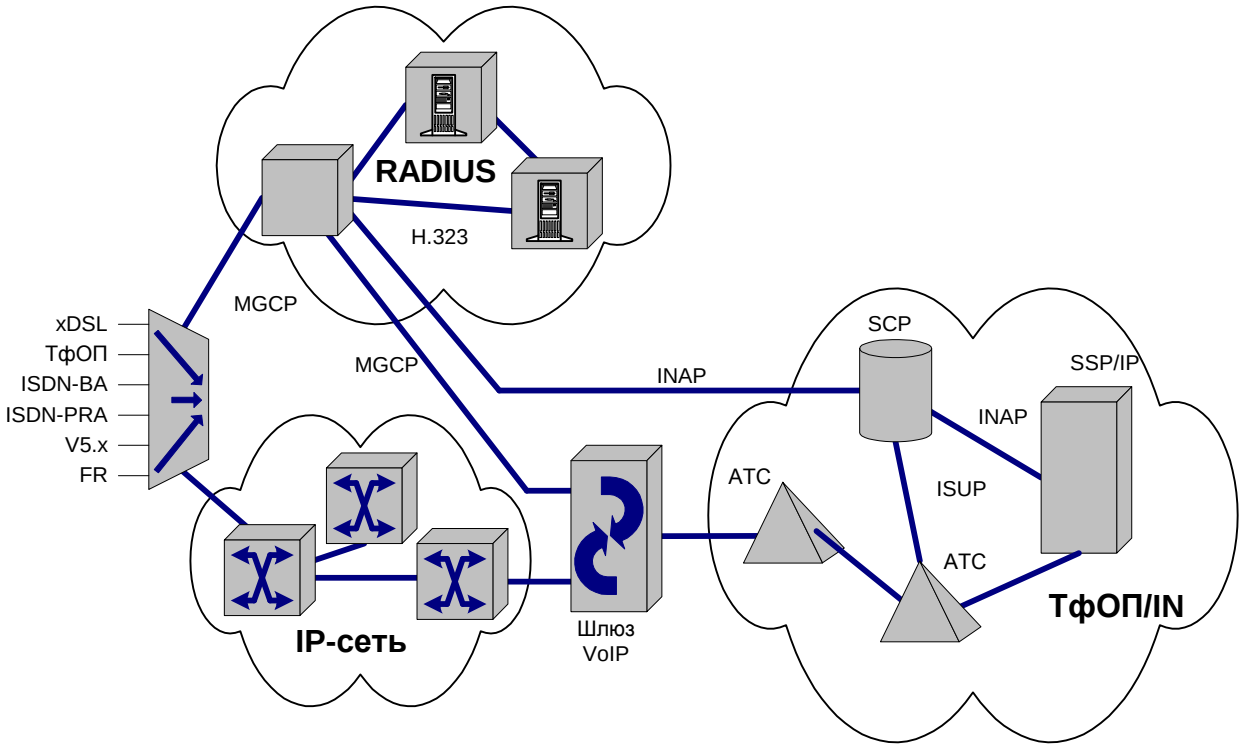


Рисунок 13 Мультисервисная сеть связи

В этой связи интересно отметить, что целый ряд операторов в США и Европе (AT&T, British Telecom, GTS, Qwest и др.) уже объявили о строительстве магистральных транспортных сетей на основе технологий «IP over DWDM» или «IP over SDH». Такие сети позволят передавать смешанный трафик данных со скоростью до нескольких десятков Гбит/с.

1.3.1 TIPHON как платформа конвергенции сетей

1.3.1.1 Архитектура системы

В отличие от концепции гибридных сетей, коммутирующих и пакеты, и каналы, которые основаны на гибридных пакетно-канальных коммутаторах со встроенным программным обеспечением обработки вызовов, концепция мультисервисной сети основана на отделении средств обработки вызовов от средств физической коммутации трафика с использованием стандартного протокола для их взаимодействия (рисунок 14).

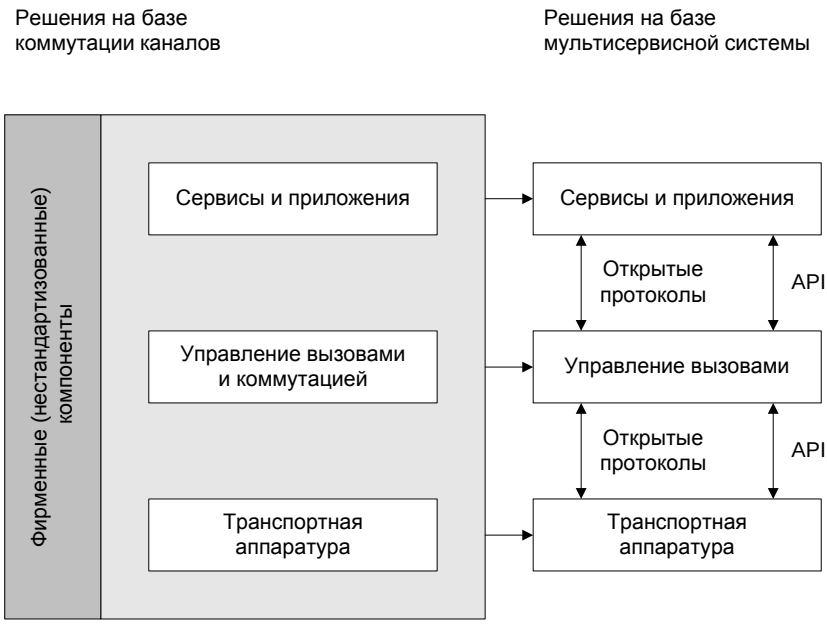


Рисунок 14 Решения на базе коммутации каналов и мультисервисной сети

В этом направлении первые существенные шаги предприняли, выступив инициаторами, известные компании: Alcatel, Belgacom, Ericsson, KPN, Lucent Technologies, Nokia, Siemens и Telia. В апреле 1997 г. по их инициативе ETSI был начат проект TIPHON (Telecommunications and Internet Protocol Harmonization over Network). Он направлен на разработку единых подходов и стандартов в области IP телефонии. Его основным назначением является решение проблем взаимодействия между IP-сетями и сетями с коммутацией каналов в части работы речевых и схожих с ними по требуемой пропускной способности приложений (например, факсимильных). В разработках этого проекта в настоящее время принимает участие 40 крупнейших телекоммуникационных компаний.

Предлагаемая ими модель состоит из тех же компонентов, что и модель H.323 – диспетчера, шлюза и терминала (приложение Б).

Диспетчер отвечает за контроль и управление объектами сети (например, преобразует телефонные номера в соответствующие IP-адреса H.323 и обратно) и маршрутизацию вызовов. Кроме функций, определенных для диспетчера протоколом H.323, он отвечает за тарификацию, взаиморасчеты, составление отчетов по использованию ресурсов и пр.

Предложенная в проекте распределенная архитектура телефонного **шлюза** обеспечивает очень хорошую масштабируемость и позволяет строить сеть с использованием компонентов разных фирм. Согласно подходу IETF, шлюз моделируется на архитектуре, объединяющей три основных элемента:

- шлюз сигнализации ОКС №7 (SG);
- транспортный шлюз (MG);
- контроллер транспортного шлюза (MGC).

Шлюз сигнализации служит промежуточным звеном сигнализации между сетями IP и сетями с коммутацией каналов, передавая через IP сеть сообщения TUP и ISUP из сети ОКС №7 к различным MGC и от MGC в сеть ОКС №7. MGC выполняет обработку вызова, основанную на сообщениях TUP и ISUP, взаимодействуя с SG, предоставляя доступ к сети Интернет, а также соединения типа VoIP[7] и FoIP[8]. Шлюз сигнализации ОКС №7 выполняет функцию транзитного пункта сигнализации (STP) для сети с коммутацией каналов и упаковывает сигнальные сообщения ОКС №7 в транспортные протоколы IP-сети.

[7] Voice over IP – передача голоса «поверх» IP-сети.
[8] Fax over IP – передача факсимильных сообщений «поверх» IP-сети.

Главной функцией *транспортного шлюза* является преобразование ИКМ-трафика в IP-пакеты и обратно. Он транслирует адреса, подавляет эхо, передает различные сообщения для абонентов, принимает и передает цифры абонентского номера в стандарте DTMF. Этим элементом могут являться разные устройства, такие, как шлюзы и серверы доступа, системы передачи речи по ATM, серверы интерактивных речевых сообщений и т.п.

Основной задачей *контроллера транспортного шлюза* является управление работой транспортного шлюза. Контроллер обеспечивает регистрацию, управление ресурсами транспортного шлюза и преобразование протоколов сигнализации ТфОП и IP-телефонии: выполняет процедуры сигнализации по протоколу H.323, которые определены в рекомендациях H.323, H.225 (RAS и Q.931) и H.245, преобразуя сообщения сигнализации сети с коммутацией каналов в сообщения сигнализации H.323. Следует учитывать, что контроллер MGC не предназначен для полнофункционального управления вызовами, так как он осуществляет управление физическими элементами MG и проходящими через них информационными потоками. Управление поступающими вызовами возлагается еще на один элемент управления, например, на диспетчер H.323 или сервер SIP.

Модель сети, состоящая из функциональных элементов и интерфейсов между ними, представлена на рисунке 15.

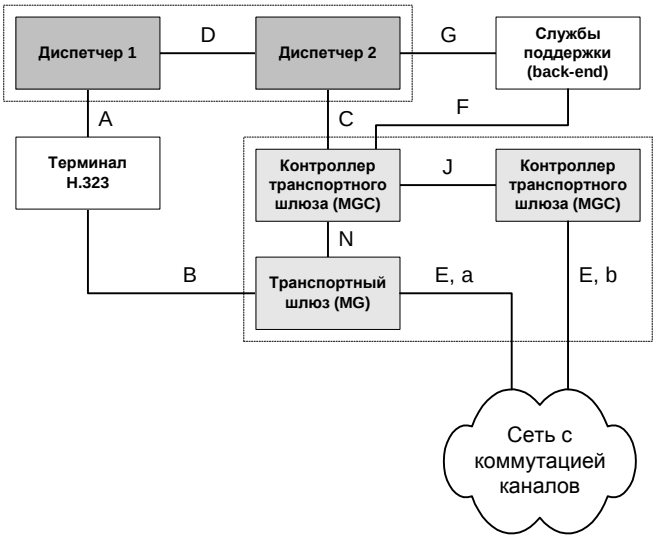


Рисунок 15 Функциональная архитектура сети, предложенная в рамках проекта TIPHON

В данной архитектуре присутствуют следующие интерфейсы:

- E, a – интерфейс для передачи информации между IP-сетью и сети с коммутацией каналов;
- E, b – интерфейс для передачи сигнальных сообщений между IP-сетью и сети с коммутацией каналов;
- D предназначен для маршрутизации вызовов между диспетчерами;
- C – для взаимодействия между шлюзом (компонентом MGC) и диспетчером;
- N определяет особенности взаимодействия между объектами MGC и MG.

Они могут взаимодействовать в момент создания, модификации и разъединения соединений передачи информации, определения требуемого формата информации, включения в поток тональных сигналов и различных речевых уведомлений, запроса отчетов о событиях, связанных с обслуживанием потока информации.

Шлюз на основе такой архитектуры воспринимается элементами сети как единая система (рисунок 16).

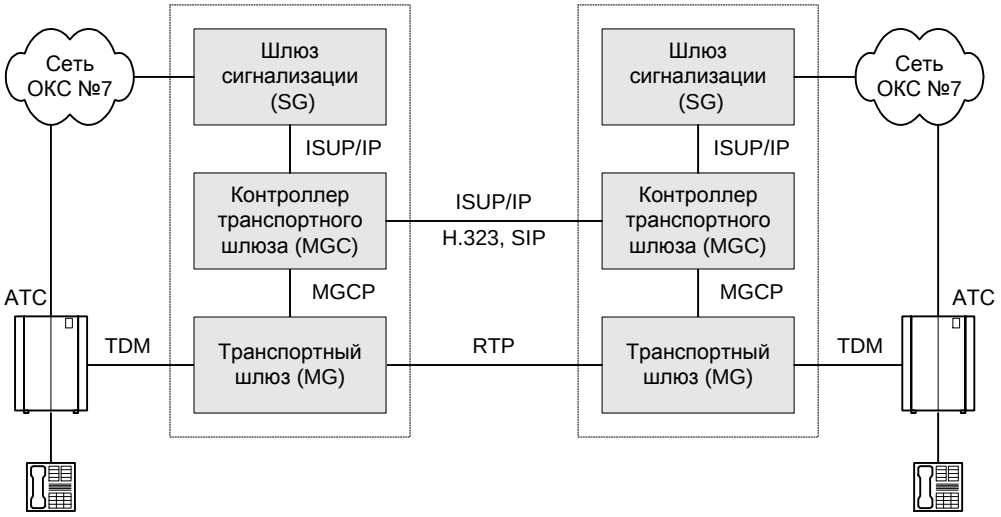


Рисунок 16 Функциональная модель сети (шлюз имеет три компонента)

Указанные три элемента шлюза могут не быть физически разделены, однако их разделение дает преимущество – возможность обрабатывать большее количество вызовов, поскольку при таком разделении разные функции распределяются по отдельным процессорам. Как правило, такие элементы должны иметь стандартные интерфейсы, что дает возможность оператору использовать оборудование разных фирм. В данной модели один шлюз сигнализации с целью более экономичного развертывания сети может быть использован для обслуживания большого числа транспортных шлюзов.

1.3.1.2 Взаимодействие элементов системы

Рабочая группа IETF Sigtran разрабатывает модель взаимодействия контроллера транспортного шлюза и шлюза сигнализации. Шлюз сигнализации должен принимать пакеты сигнализации трех нижних уровней модели ОКС №7 (уровней передачи сообщений MTP) и передавать сигнальные сообщения верхнего (пользовательского) уровня на контроллер MGC. Основное внимание уделяется вопросам обеспечения наиболее надежной передачи сигнальной информации по IP-сети. С этой целью предлагается использовать протокол Reliable UDP.

В случае использования сигнализации ОКС №7 в контроллер MGC по IP-сети будут передаваться сообщения ISUP[9]. В случае же применения сигнализации по выделенному сигнальному каналу ВСК (CAS), сигнальные сообщения сначала вместе с информацией абонента поступят в транспортный шлюз, а затем уже будут выделены в контроллер MGC. Например, MGC может контролировать действующий сервер удаленного доступа на базе ISDN PRI за счет туннелирования сигнализации Q.931 от сервера удаленного доступа.

MGC анализирует информацию сигнализации и передает управляющую информацию в транспортный шлюз с помощью специального протокола управления, среди задач которого, – обеспечение управления различными ресурсами (системой интерактивного речевого ответа, мостами конференц-связи и т.д.), прием и формирование сигналов DTMF, формирование тональных сигналов (готовность к набору номера, контроля посылки вызова, сигнала «занято» и пр.), эхоподавление, использование кодеков (G.711, G.723.1, G.729, GSM и т.д.), сбор статистики, тестирование конечных точек, резервирование, разъединение и блокировка конечных точек, шифрование.

[9] Протокол ОКС №7 ISUP обеспечивает сигнальные функции для установления соединений с возможностью предоставления услуг ISDN. До принятия ISUP функции управления телефонными вызовами выполняла TUP. Подсистема ISUP включает в себя все функции TUP и, кроме того, реализует ряд дополнительных функций, связанных с услугами ISDN.

1.3.1.3 Используемые протоколы

В шлюзах пакетной коммутации, соединяющих сети с коммутацией пакетов и каналов, а также в других используемых устройствах применяется множество различных протоколов, среди которых, в частности, стек протоколов H.323, SIP (Session-Initiation Protocol), MGCP (Media Gateway Control Protocol) и Megaco/H.248 (МСЭ). Даже если протокол выбран, остаются производители аппаратуры, и нет гарантии, что протокол, реализованный в оборудовании одного производителя, будет взаимодействовать с таким же протоколом другого производителя.

Протокол управления шлюзами **MGCP** является универсальным протоколом, способным обеспечить распределенное управление различными типами транспортных шлюзов, в частности телефонными шлюзами и серверами доступа. Он может использоваться как для установления соединения, так и для выполнения различных функций обслуживания. Результатом дальнейшей работы над протоколом MGCP стало появление протокола **Megaco/H.248**. Принципиальное отличие технологии Megaco/H.248 от MGCP заключается в том, что первая из них поддерживает мультимедиа-потоки (аудио + видео), в то время как вторая – ориентирована только на работу с аудиопотоками. Кроме того, Megaco/H.248 базируется на более общей модели обработки вызовов, поэтому лучше подходит для взаимодействия со шлюзами, не являющимися классическими IP-телефонными (IP-TDM), например, со шлюзами ATM-TDM или TDM-TDM[10].

Временные задержки или разброс времени доставки пакетов (джиттер), характерные для IP-сетей существенно искажают информацию реального времени, делая ее абсолютно непригодной для восприятия. Причем разница в задержке последовательных пакетов гораздо сильнее влияет на субъективно оцениваемое качество передачи, чем само абсолютное значение задержки. Работа по созданию методов уменьшения значений джиттера и задержек ведется длительное время. На сетевом уровне для этого могут применяться гарантирующие пользователю заданный уровень качества механизмы RSVP, MPLS, Diff-Serv, ATM и др. Они существенно улучшают качество услуг, предоставляемых сетью, но не могут полностью исключить образование очередей в сетевых устройствах, а, следовательно, и совсем убрать джиттер. Компенсировать его негативное влияние позволяет протокол прикладного уровня RTP, который используется известными технологиями H.323 и SIP.

Протокол **RTP** 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 других параметров качества услуг (это осуществляют нижележащие протоколы), и не обеспечивает все функции, которые, как правило, предоставляют транспортные протоколы, в частности функции по исправлению ошибок или управлению потоком. Обычно RTP работает поверх UDP и использует его службы, но может функционировать поверх других транспортных протоколов.

Доставка RTP-пакетов контролируется специальным управляющим протоколом **RTCP**, который обеспечивает обратную связь с передающей стороной и другими участниками сеанса. RTCP периодически рассылает свои управляющие пакеты, используя механизм распределения, аналогичный тому, который применяется и для RTP-пакетов с пользовательской информацией.

Основная функция RTCP – это организация обратной связи с приложением для отчета о 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. В RTCP также предусматривается идентификация участников сеанса.

[10] TDM (Time Division Multiplexing) – уплотнение каналов на основе временного разделения.

1.3.1.4 Практический аспект решений TIPHON

1.3.1.4.1 Объединение голосовой связи и передачи данных.

Предлагаемый путь интеграции состоит из нескольких этапов, первый из которых – это предложение о внедрении в шлюзы IP-телефонии функций поддержки ISUP, чтобы они могли создавать, контролировать и разрушать соединения с конечными точками в телефонной сети. Шлюз получает возможность обмениваться сообщениями с телефонными узлами (точкой коммутации сервиса в терминах ОКС №7 – Service Switching Point, SSP) по выделенным сигнальным каналам, которые в обязательном порядке (важна очень высокая надежность) должны быть продублированы на случай выхода из строя одного из них. Подобный вариант реализации (рисунок 17) имеет существенный недостаток, заключающийся в том, что в настоящее время шлюзы IP-телефонии не поддерживают достаточного количества голосовых линий для того, чтобы организация канала ОКС №7 в телефонную сеть была оправдана. Более целесообразна реализация шлюза между IP и ОКС №7 для обслуживания нескольких шлюзов IP-телефонии. Следует также отметить, что внедрение поддержки ISUP не обеспечивает доступа к базам данных интеллектуальной сети, а только позволяет снизить нагрузку на телефонные каналы, не занимая их при установлении соединения. Поэтому второй этап интеграции учитывает реализацию прикладной части поддержки транзакций TCAP (Transaction Capabilities Application Part) в виде точки коммутации сервиса IP-телефонии IT-SSP (IP Telephony Service Switching Point).

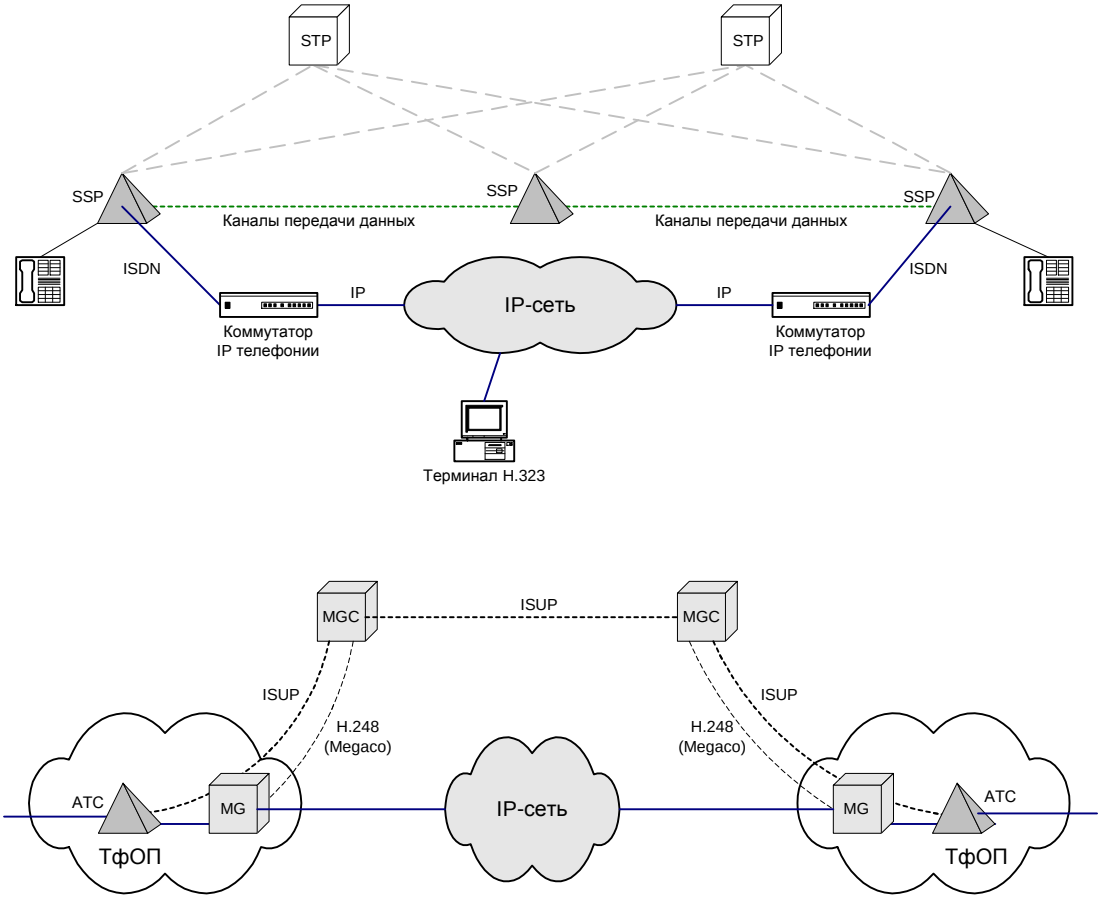


Рисунок 17 Первый этап конвергенции

IT-SSP объединяет в себе шлюзы и диспетчеры IP-телефонии, а также шлюз из IP в ОКС №7 с поддержкой ОКС №7 ISUP и TCAP (рисунок 18). Шлюз из IP в ОКС №7 может подавать запросы TCAP к базам данных интеллектуальной сети на точках контроля сервиса SCP (Service Control Point). Благодаря такому шлюзу пользователи терминалов H.323 получают доступ ко всем услугам интеллектуальной сети.

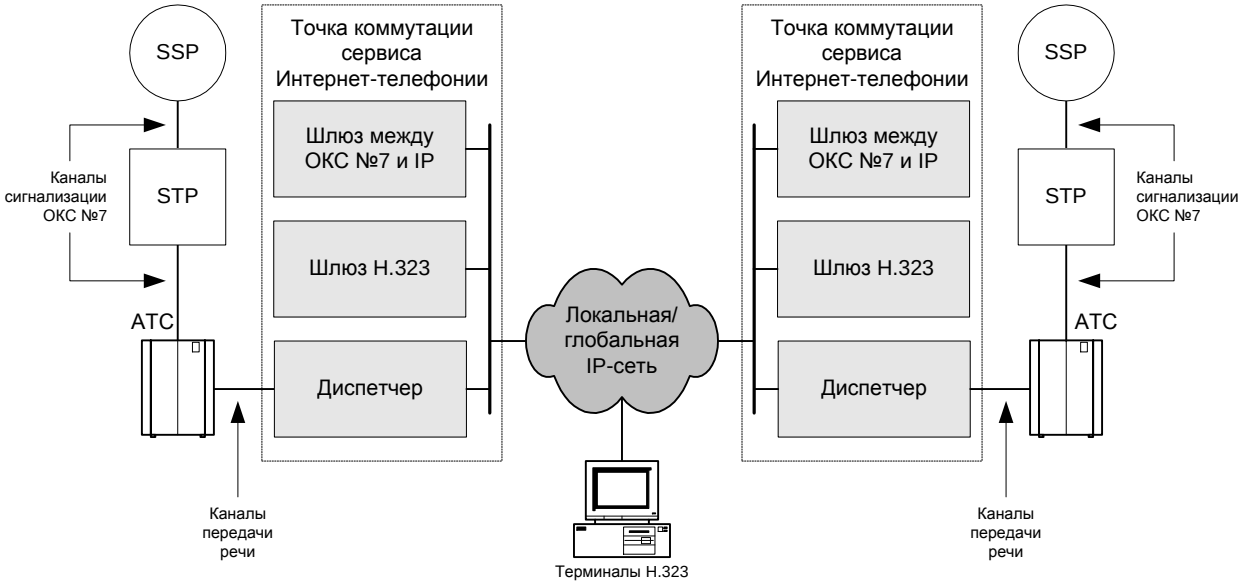


Рисунок 18 Точка коммутации сервиса IP-телефонии (шлюз, диспетчер H.323 и шлюз ОКС №7)

1.3.1.4.2 Услуги интеллектуальных сетей.

Мультисервисная платформа может использовать встроенные интеллектуальные платформы, а может работать и с внешними платформами. В последнем случае система фактически может выступать как в качестве пункта коммутации услуг (SSP), так и в качестве пункта контроля услуг (SCP), обеспечивая обработку запросов в формате протокола TCAP и взаимодействуя с внешними SCP.

1.3.1.4.3 Организация виртуальных модемных пулов и разгрузка телефонных сетей

Предлагаемое решение состоит в маршрутизации всех предназначенных провайдеру Интернет вызовов пользователей напрямую на сервер удаленного доступа провайдера в обход транзитных узлов коммутации через выделенные для этого порты (рисунок 19).

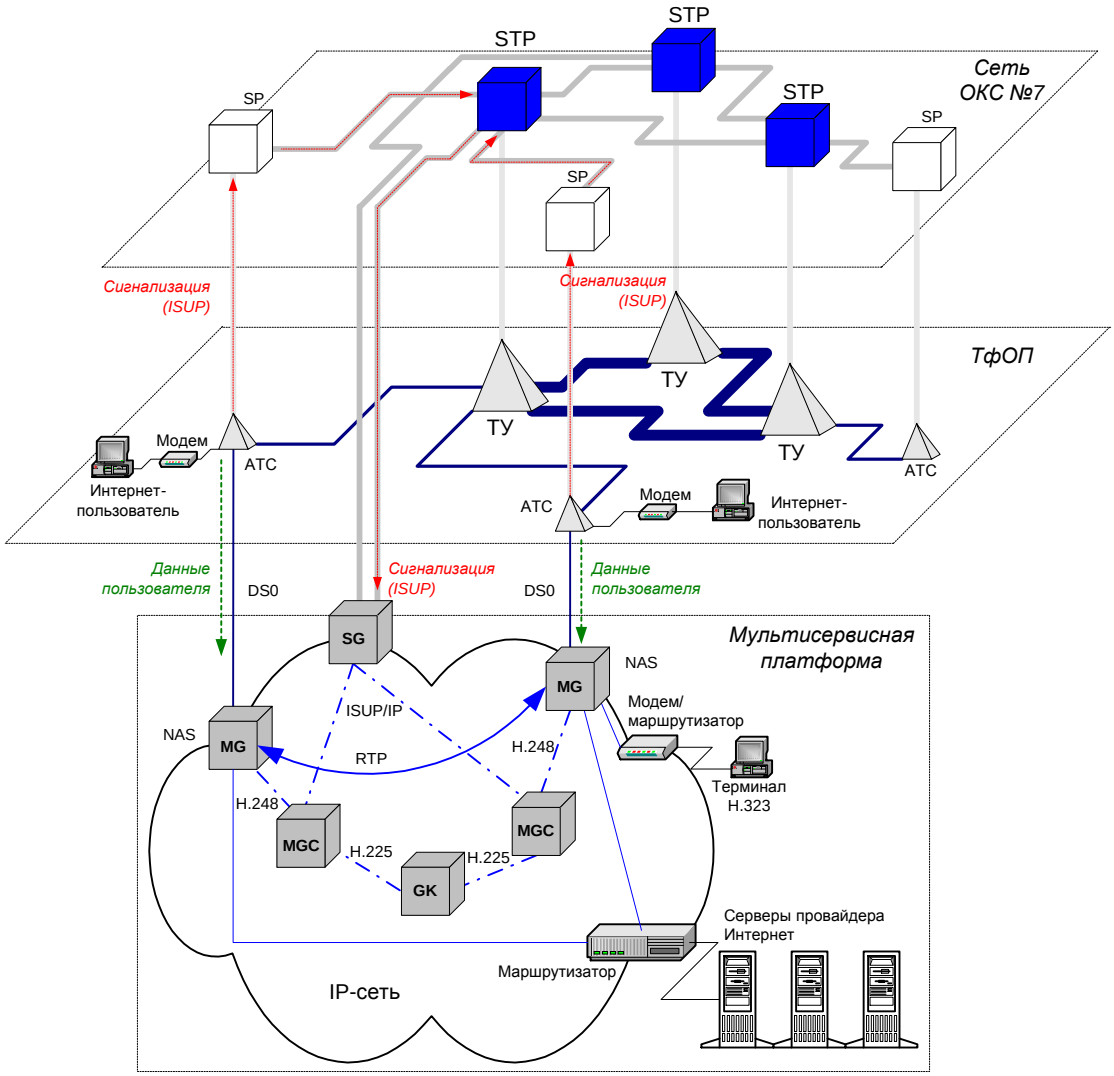


Рисунок 19 Организация обходного пути для связи с провайдером Интернет

По такой схеме серверы доступа в сеть провайдера Интернет или серверы доступа к сети NAS (Network Access Server) могут быть размещены как на телефонных станциях ГТС, так и непосредственно у провайдера. Каждый вызов к провайдеру идентифицируется по набранному номеру и направляется на одну из выделенных линии, ведущих к модемному пулу (то есть к NAS). Идентификация номера производится средствами интеллектуальной сети. Сообщения ISUP для данного вызова маршрутизируются через STP на шлюз ОКС №7. Шлюз преобразует их в эквивалентные сообщения и передает по выделенной глобальной сети IP на соответствующее устройство NAS. Один шлюз ОКС №7 способен обслуживать множество устройств NAS с сотнями и тысячами портов. Сами серверы NAS подключаются к двум сетям: к одной для обмена информацией между шлюзом ОКС №7 и NAS, а к другой – для передачи данных между конечным пользователем и провайдером Интернет.

Таким образом, интеграция сетей IP и ТфОП на первом этапе предполагает параллельное существование IP и телефонных сетей и использование сети в качестве своего рода вспомогательного (обходного) маршрута для телефонной сети в целях сокращения общего телефонного трафика на сеть ТфОП.

1.3.2 Мультисервисные платформы различных производителей

Характеристики мультисервисных платформ производства Alcatel, Cisco, Lucent, Nortel Networks приведены в приложении В.

1.3.2.1 Lucent Softswitch от Lucent Technologies

На рисунке 20 показано, как функции канального коммутатора, представленного в виде модели слева, разделяются и распределяются по пакетной магистрали с использованием программного коммутатора Lucent Softswitch (модель справа). При этом происходит ряд замен: информационные интерфейсы коммутатора каналов (линейные и трактовые платы) – на шлюзы среды передачи, преобразующие потоки временного разделения каналов (ВРК) в потоки пакетов IP или ATM; коммутационное поле – на высокопроизводительную пакетную магистраль; контроллер коммутатора, управляющий коммутацией временных интервалов в коммутационной матрице, – на программный коммутатор Lucent Softswitch, который управляет коммутацией и маршрутизацией информационных пакетов между шлюзами среды передачи пакетной магистрали. В обоих случаях контроллер коммутации реализует сервисную логику, как, например, в случае триггеров протокола INAP (Intelligent Network Application Protocol) в интеллектуальной сети AIN 0.1. Кроме того, в управляемые им коммуникационные потоки могут быть добавлены и другие услуги, например, посредством взаимодействия с сетью ОКС №7, в случае услуг интеллектуальной сети (ИС), или через другие базы данных, серверы функций и серверы среды передачи.

Оконечные устройства соединительных линий или шлюзы СЛ используются для подключения СЛ, связанных с управляющими звеньями ОКС № 7. Шлюзами могут являться концентраторы доступа Lucent MAX и Lucent PSAX. Эти СЛ, работающие в режиме временного разделения каналов, передают информационные потоки от ближайшего коммутатора традиционной сети с коммутацией каналов.

Шлюзы доступа используются в качестве оконечных устройств сигнальных и информационных каналов ТфОП. Примером такого применения служит оборудование, размещаемое в помещении клиента, или телефонная станция. Более специфическим примером является семейство серверов доступа Lucent MAX, в котором заканчиваются информационные потоки, поддерживающие внутриканальную сигнализацию или сигнализацию по общему каналу.

Отличительные характеристики Lucent Softswitch:

- программируемая система обработки вызовов, поддерживающая различные протоколы ТфОП, ATM и IP
- функционирует на обычных компьютерах под управлением традиционных операционных систем,
- управляет внешними шлюзами СЛ, шлюзами доступа, серверами удаленного доступа, например. Lucent Softswitch в сочетании с:
  - шлюзом СЛ заменяет транзитный/междугородный коммутатор с магистральной передачей голоса поверх IP (VolP) или голоса и телефонии поверх ATM (VTOA),
  - шлюзом доступа заменяет виртуальную частную сеть или выделенную линии с магистральной передачей голоса поверх IP,
  - сервером удаленного доступа обеспечивает управляемую модемную службу с использованием СЛ совместного пользования (т. е. модемная сигнализация проходит через подсистему пользователя ISDN ОКС № 7 (ISUP),
  - шлюзом СЛ и локальным функциональным сервером заменяют местную телефонную станцию с магистральной передачей VolP или VTOA,
- использует службы ИС через открытый и гибкий интерфейс каталогов Примером может служить архитектура с функциями каталогов с доступом к RDBMS, LDAP и каталогам подсистемы TCAP (transaction-capabilities applications part).
- предоставляет открытые прикладные интерфейсы API для сторонних разработчиков с целью создания услуг третьего поколения[11],

[11] Поставщик услуг может разрабатывать и вводить разнообразные новые услуги в контролируемую Lucent Softswitch сеть. Более того, эти модули услуг (аплеты) могут разрабатываться независимыми разработчиками

- реализует программируемые функции внутренней обработки (back-office), в том числе программируемая запись событий и запись данных о вызовах в систему регистрации событий оператора.
- управляет всеми программными компонентами на базе сервера правил использование интерфейса SNMP 2.0 для всех компонентов, наличие языка описания правил и системы создания и обеспечения заданных правил.

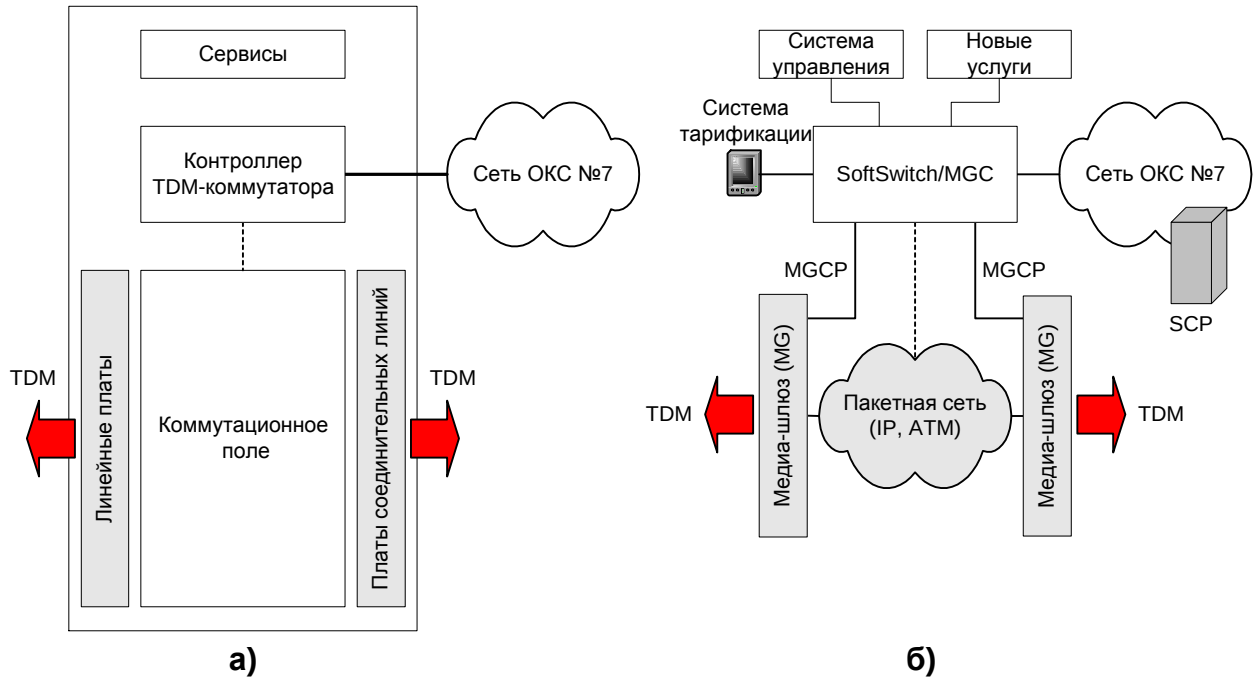


Рисунок 20 Структура традиционных АТС (а) и сетевых решений на базе систем Lucent Softswitch (б)

1.3.2.2 SURPASS от Siemens

Ядром концепции SURPASS компании Siemens служит центральный сервер обработки речевых вызовов и сигнализации HiQ, управляющий шлюзами на границах сети передачи данных. Основные характеристики этой платформы:

- поддержка большинства протоколов сигнализации (ISUP, INAP, H.323/SIP, MGCP/H.248);
- обслуживание вызовов интеллектуальных сетей;
- наличие API для взаимодействия с программными продуктами третьей стороны;
- реализация Gatekeeper и RADIUS, позволяющая выполнять функции диспетчера и производить идентификацию удаленных пользователей и др.

Транспортные шлюзы SURPASS hiG обеспечивают VoIP, VoATM и функции сервера удаленного доступа RAS. Платформа SURPASS hiQ обрабатывает трафик ТфОП, обслуживает цифровые абонентские линии xDSL и выполняет функции сервера удаленного доступа.

программного обеспечения. Функциональные аплеты могут загружаться в соответствии с различными правилами. В частности, аплет можно загрузить с хост-компьютера разработчика, тогда он подчиняется определенным правилам безопасности, предотвращающим доступ к определенным сетевым компонентам и ресурсам и контролирующим объем генерируемого аплетами трафика. Примеры таких услуг, разработанных третьими фирмами: виртуальные операторские центры, системы интерактивного речевого взаимодействия, частные телефонные сети, услуга единого номера.

1.3.2.3 Alcatel 1000 Softswitch

Alcatel 1000 Softswitch является «интеллектом» в сети с распределенной коммутацией/ маршрутизацией, использующим шлюзы (Магистральные, Доступа, Резидентные, Беспроводные Шлюзы) для преобразования исходного способа передачи трафика в способ, используемый в сетях данных. Softswitch обеспечивает реализацию функций управления для передачи голоса через сеть с коммутацией пакетов. Он обеспечивает управление трафиком всех видов, включая голос, данные, мультимедиа, видео и музыку. Основные функции устройства Softswitch – Интегрированный УСС (Узел Спецслужб), Шлюз сигнализации, Сервер Управления Вызовом. Alcatel 1000 Softswitch отличается наличием интерфейсов к Интеллектуальной сети и Платформам TMN для поддержки реализованных сегодня услуг и огромным набором услуг для абонентов.

1.3.2.4 Tigris от Ericsson

Семейство оборудования Tigris обеспечивает шлюз между сетями с коммутацией каналов и IP-сетями (рисунок 21) и позволяет осуществлять обычные телефонные соединения по IP-сетям. В комбинации со специальным программным обеспечением AccessOS это оборудование создает платформу множественного доступа с огромным разнообразием услуг. Платформа Tigris используется для организации множества различных типов доступа, таких как: модемный, ISDN, беспроводная передача данных, VoIP[12] и факс.

Под мультисервисностью платформы Tigris понимается совокупность различных приложений, реализованных на базе одной аппаратно-программной платформы. В частности, это означает поддержку передачи голоса, данных, видео и других услуг по IP-сетям. Мультисервисность в платформе Tigris реализована динамически. Это означает, например, что трафик данных, поступивший на порт устройства Tigris по коммутируемому модемному каналу, можно направить в IP-сеть, а в следующий момент этот же порт преобразует в IP-пакеты речевые сигналы. Данная функция реализуется на платформе интеллектуальной сети, у которой запрашивается информация для аутентификации услуги и подтверждения наличия необходимых ресурсов для каждого вызова.

Для определения типа сервиса при коммутируемом доступе утилита разделения доступа использует для каждого вызова профили услуг и соответствующие разделы доступа. Группа набираемых номеров соответствует определенному профилю услуг. Профиль услуг может быть реализован в трех вариантах:

- многопротокольная мостовая маршрутизация;
- маршрутизация в соответствии с набранным номером;
- туннелирование в соответствии с протоколом туннелирования L2TP.

Коммутируемые вызовы обычно маршрутизируются в соответствии с адресами назначения входящих пакетов. Профили услуг, представленные для маршрутизации, в зависимости от набранного номера перенаправляют входящий трафик напрямую к IP-адресу следующего узла соответствующего раздела доступа или от IP-адреса, назначенного RADIUS-сервером, в ответ на запрос авторизации доступа.

Профили услуг, предоставляемые для L2TP, туннелируют модемный трафик к IP адресу соответствующего раздела доступа или от IP-адреса, назначенного RADIUS-сервером, в ответ на запрос авторизации доступа.

Профили услуг могут быть настроены для предоставления возможностей проверки набранных номеров, организации модемных пулов и разделов доступа.

Профиль услуг может быть настроен таким образом, чтобы проверять группы набираемых номеров. Подобная проверка позволяет блокировать или, наоборот, подключать как индивидуальные номера, так и группы номеров. При этом проверка номера производится до начала обработки вызовов.

[12] Архитектура VoIP на платформе Tigris реализована на трех основных опорах: шлюз сигнализации ОКС №7, контроллер транспортного шлюза, транспортный шлюз.

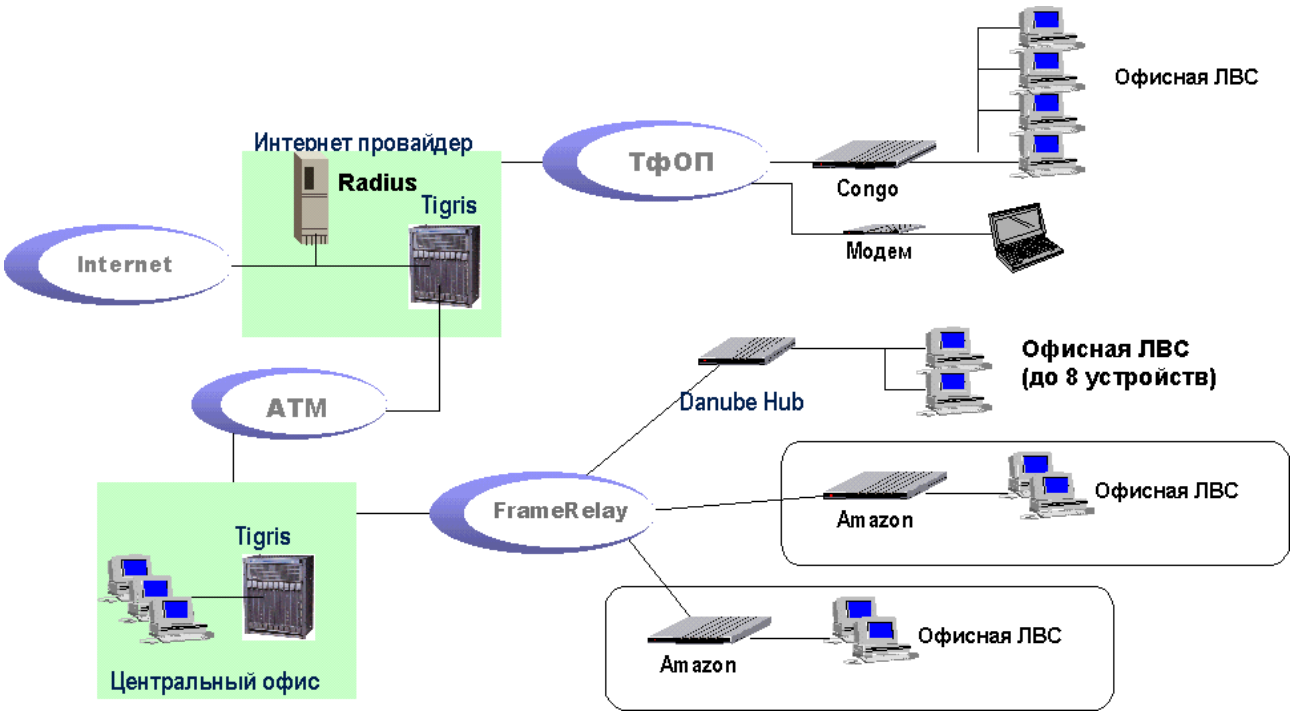


Рисунок 21 Платформа Tigris

1.3.2.5 SUCCESSION от Nortel Networks

Первое промышленного оборудование класса Softswitch было представлено компанией Nortel Networks в 1998 г. на базе DMS-500. При возникновении перегрузок вместо расширения емкости к DMS было пристроено оборудование GSX-9000 Open Service Switch производства компании SONUS, с помощью которого поступающий от пользовательских модемов и предназначенный для серверов удаленного доступа трафик передавался в обход коммутатора телефонной станции. Таким образом, коммутационный узел DMS разгружался для обслуживания исключительно телефонных соединений.

1.4 Использование средств существующей ТфОП

Учитывая развитую инфраструктуру медных пар абонентский линий перспективное использование существующей инфраструктуры ТфОП представляется в использовании технологий xDSL.

Тем не менее, к доступным решениям можно отнести:

- разработку системы гибких тарифов для операторов, на основе системы повременной оплаты местных разговоров;
- регулирование потоков трафика на ТфОП посредством задействованной системы управления трафиком, построенные на основе TMN, которые позволяют улучшать качество связи путем перераспределения ресурсов сети в реальном масштабе времени, однако их возможности ограничены в пределах задействованных ресурсов сети;
- разработку типовых схем подключения провайдеров через серийный номер электронных АТС различных систем на основе специально разработанной нормативно-технической базы (нормирование параметров качества доступа пользователей к сети Интернет через телефонную сеть); исходя из необходимости снижения дополнительной нагрузки на местную телефонную сеть, следует контролировать, как минимум, два параметра – вероятность отказа в обслуживании вызовов (позволит свести к минимуму паразитную нагрузку от повторных вызовов) и эффективную скорость передачи данных (позволит уменьшить время передачи информации);

- определение порядка использования ТфОП для доступа к Интернет.

Развитие фотонных сетей DWDM может стать базой для возвращения операторов к использованию в магистральных сетях метода коммутации каналов. Причина этого – уменьшение стоимости канальных ресурсов в связи с ростом пропускных способностей магистральных сетей.

В фотонных сетях на базе DWDM вся информация передается только в виде оптического сигнала. Оптический сигнал обрабатывают все компоненты, в том числе и коммутационные системы, только в источнике и приемнике осуществляется преобразование электрического сигнала в оптический и обратно. Уже к середине этого десятилетия возможно появление полностью оптических узлов, без электронной регенерации сигналов, где будут обрабатываться сотни длин волн при скоростях передачи в интерфейсах узлов до нескольких десятков Гбит/с.

Таким образом, использование технологии DWDM на местных сетях связи способно практически исключить рассматриваемую в настоящее время проблему.

2 Концепция разделения трафиков на АТС

Рассмотрев варианты организации передачи голосового трафика и трафика сети передачи данных, представляется целесообразным доступ к сети Интернет на местных сетях связи организовать через наложенную сеть доступа с узлами IPoP. Доступ посредством наложенной сети передачи данных является наиболее прогрессивным способом организации доступа пользователей к компьютерным сетям. При его использовании может быть задействована существующая инфраструктура некоммутируемых медных телефонных кабелей, сети SDH, ATM, а также специализированные волоконно-оптические кабели.

Организация доступа к компьютерным сетям посредством наложенной сети передачи данных не затрагивает ТфОП и, соответственно, не оказывает влияния на ее качественные показатели. В дальнейшем, по мере развития выделенных сетей передачи данных, при обеспечении массового доступа к компьютерным сетям этот способ должен стать приоритетным.

Кроме того, внедрение мультимедийных услуг на сетях связи потребует интеграции специализированных сетей предоставления услуг. Согласно концепции построения сетей, предложенной компанией Ericsson, структура прозрачной для всех типов предоставляемых услуг сети (многоуровневая взаимоувязанная сеть), представлена на рисунке 22.

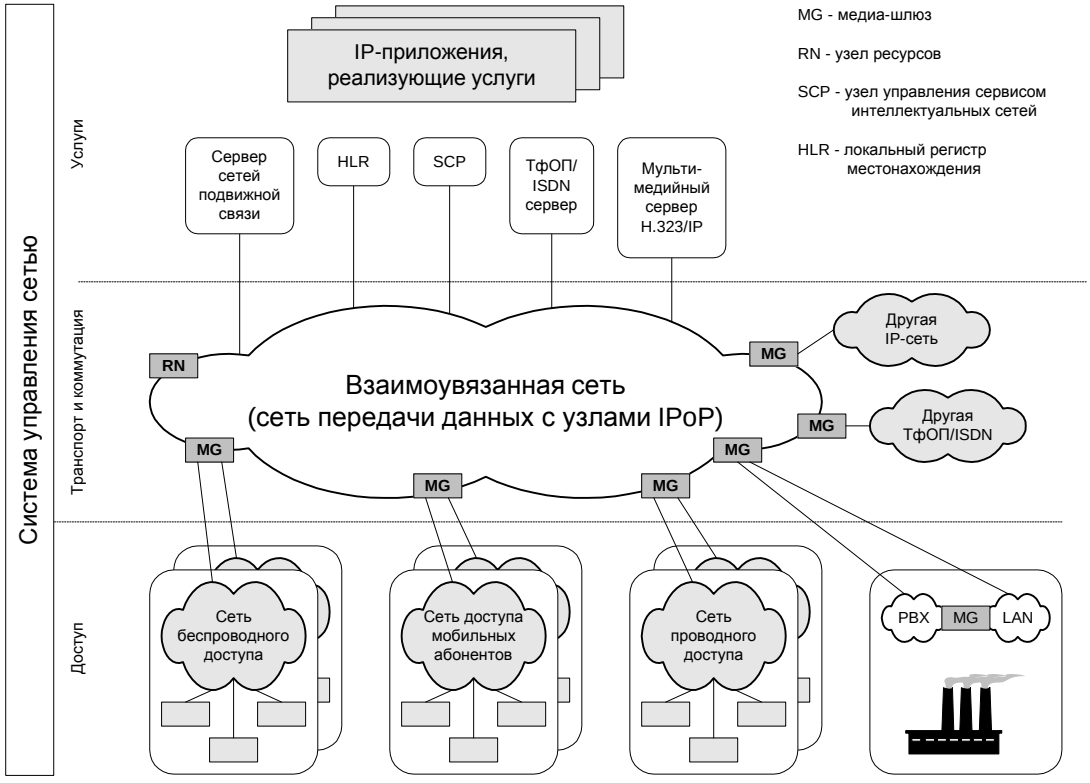


Рисунок 22 Структура многоуровневой взаимоувязанной сети

На верхнем уровне сети находятся узлы реализации услуг, которые могут представлять собой как «традиционные» системы предоставления услуг, например, SCP (Service Control Point – узел управления сервисом интеллектуальных сетей) или HLR (Home Location Register – опорный регистр местонахождения), так и системы, использующие IP-приложения при реализации всей номенклатуры услуг. В будущем системы второго типа заменят собой «традиционные» узлы, так как IP-технологии обеспечивают большую гибкость при создании, модернизации и модификации приложений.

Средний уровень – взаимоувязанная траспортно-коммутационная сеть – состоит из узлов ресурсов (Resource Node – RN) и медиа-шлюзов (Media Gateway – MG). Задача узлов

ресурсов заключается в коммутации и транспорте сервиса к соответствующему медиа-шлюзу, который в свою очередь обеспечивает интерфейсы для подключения сетей доступа (а также любых других сетей) к взаимоувязанной транспортно-коммутационной сети.

Сеть доступа (нижний уровень) представляет собой совокупность всех существующих и перспективных технологий обеспечения доступа. В некоторых случаях медиа-шлюз может выступать составным элементом сети доступа.

Концепция построения многоуровневой сети предусматривает единую для всех уровней систему управления сетью.

Сеть передачи данных с узлами IPoP позволит поэтапно перейти вышеназванной многоуровневой взаимоувязанной сети.

Сети доступа, посредством который пользователи подключаются к сети передачи данных с узлами IPoP, должны быть мультисервисными (т.е. доставлять различные услуги потребителю) и обеспечивать возможность множественного доступа. В настоящее время оператор не может и не должен ориентировать на единственную технологию доступа: условия рынка, изменчивость спроса и технологий не позволяют ему рисковать.

В общем виде сетевую архитектуру можно разделить на 3 основные компоненты - сеть доступа, транспортная (базовая) сеть и службы (рисунок 23).

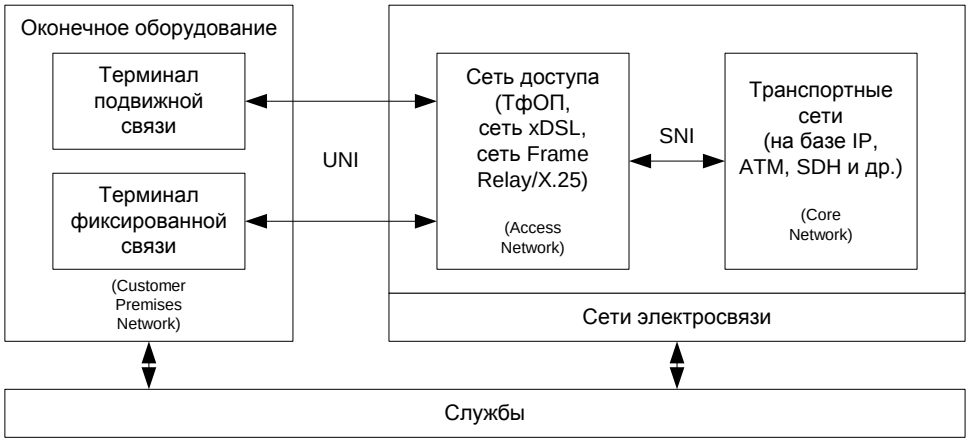


Рисунок 23 Сетевая архитектура сети доступа

Основное назначение сети доступа – это обеспечение доступа пользователю к услугам и в упрощенном виде идея доступа к услугам представлена на рисунке 24.

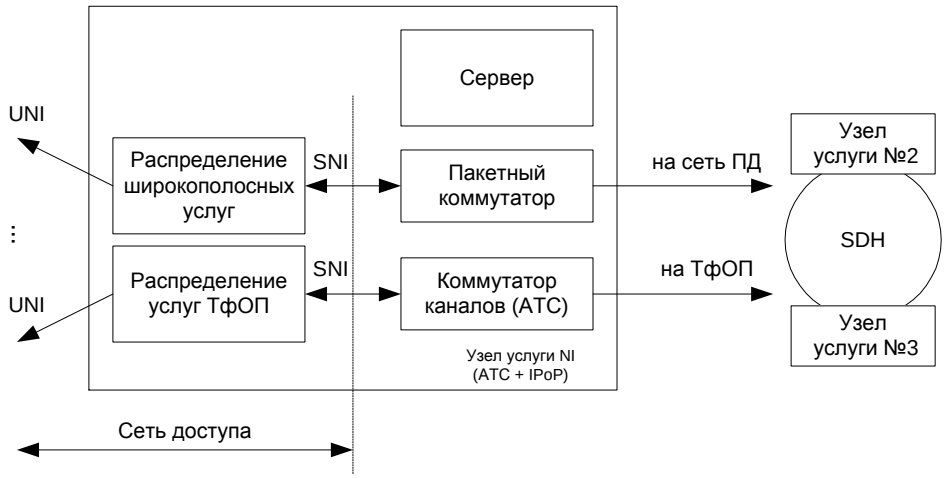


Рисунок 24 Доступ к услугам

Пользователь получает услуги от узлов услуг, которые представляют собой, АТС (телефонные услуги) с размещенным на ней узлом IPoP. В этом случае услуги Интернет или

передачи данных поддерживаются местным сервером или удаленным, расположенным на других узлах.

В данной работе основными ориентирами служили подходы ITU-T и ETSI. Рекомендация G.902 ITU-T является рамочной относительно архитектуры и функций сети доступа. Она определяет виды доступа, управление и характеризует некоторые аспекты узла услуг. Границы сети доступа согласно этой Рекомендации заключаются между пользовательским интерфейсом UNI и интерфейсом узла доступа SNI. Рекомендация построена на концепции, которая была разработана ETSI в контексте узкополосного интерфейса SNI (V5) и широкополосного (VB5).

В последние годы ITU-T разработал Рекомендацию Y.120, которая расширяет видение сети доступа в Глобальной информационной инфраструктуре (GII).

Обобщая вышеизложенное можно сделать вывод, что сетями доступа к сети передачи данных с узлами IPoP являются в Республике Беларусь:

- телефонная сеть общего пользования;
- наложенная цифровая сеть ISDN;
- сеть передачи данных X.25/Frame Relay;
- платформа цифрового абонентского доступа;
- сети провайдеров.

Реализация на местных телефонных сетях мер по исключению перегрузок из-за пропуска нагрузки, создаваемой пользователями сети Интернет, может предусматривать разумное сочетание различных технических решений (рисунок 25).

Реализация представленных на рисунке 25 способов доступа будет определяться:

1. **Уровнем развития сети** – наличие сети ISDN, внедрение ОКС №7, распространенность технологий xDSL, функционирование мультисервисных сетей.
2. **Нагрузкой, создаваемой пользователями Интернет.** На местных сетях, где количество пользователей сети Интернет крайне незначительно, и нагрузка, создаваемая ими пренебрежительно мала, необходимость в изменении существующей схемы подключения организации доступа к сети Интернет отсутствует.
3. **Экономической эффективностью** – размер платформы абонентского цифрового доступа определяется количеством пользователей, нуждающихся в xDSL технологиях; выделение субтранков в пучках СЛ АТС возможно при экономической нецелесообразности размещения на соответствующей АТС сервера доступа.
4. **Техническими возможностями.** Количество выделенных линий определяется их наличием, возможностью их использования и т.д.

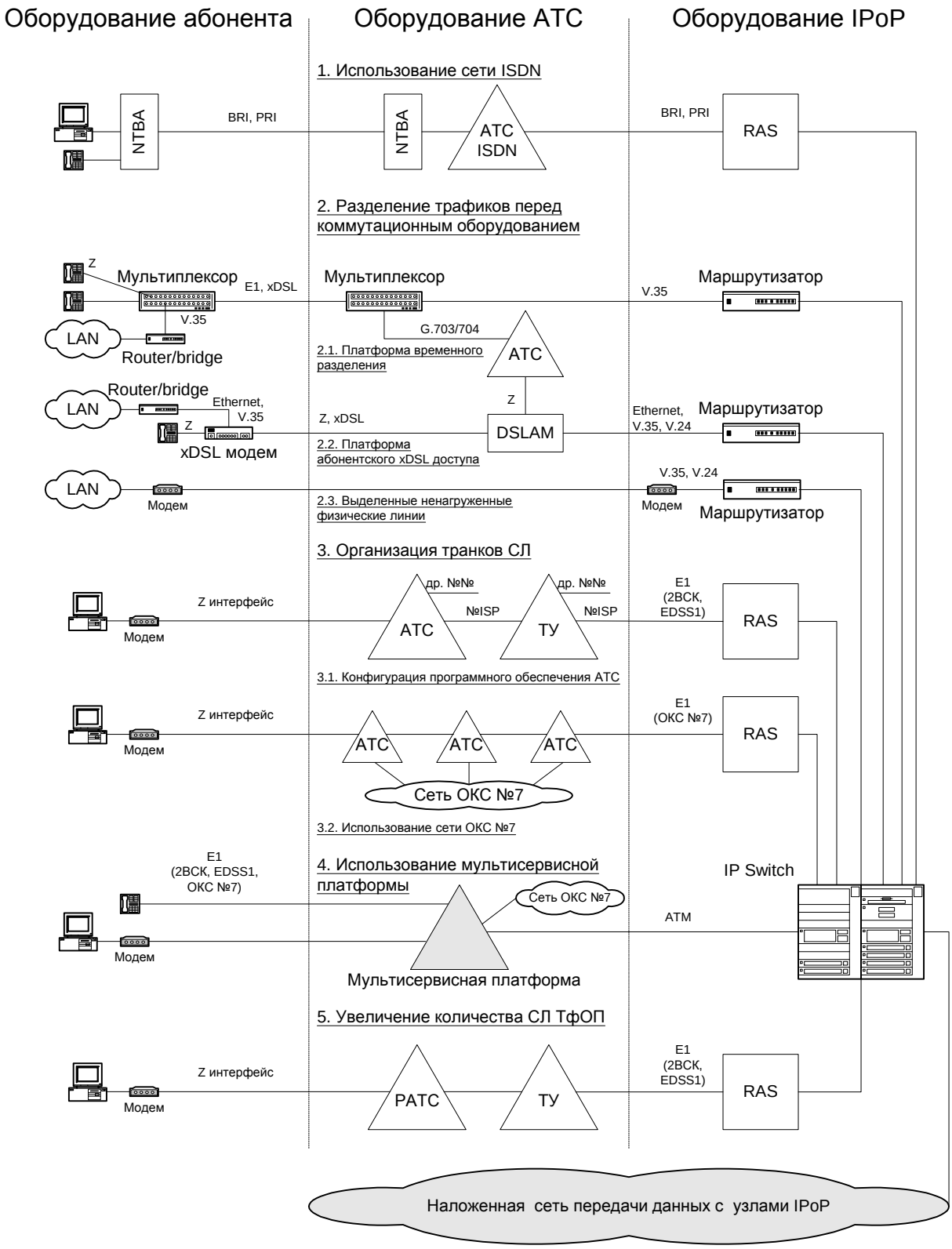


Рисунок 25 Способы подключения к наложенной сети передачи данных с узлами IPoP

3 Организация точек присутствия Интернет

3.1 Структурная схема узла IPoP

Структурная схема узла сети передачи данных с узлами рисунках 26 и 27.

3.1.1 Функциональные узлы блока доступа IPoP

Состав основных модулей узла IPoP телефонного оператора определяется основными сервисами, которые он будет предоставлять.

Базовые услуги провайдера – это фундамент его развития, как в плане наращивания его технических мощностей, так и в плане увеличения клиентской массы. В настоящее время таким набором услуг Интернет-провайдера являются:

- коммутируемый доступ в сеть Интернет;
- доступ в Интернет по выделенной линии;
- электронная почта;
- электронные новости;
- размещение персональной странички в Интернет;
- регистрация доменного имени.

Набор дополнительных услуг определяется гибкостью предлагаемого различными производителями телекоммуникационного оборудования. Одной из самых популярных дополнительных услуг среди Интернет-провайдеров является в настоящее время услуга Интернет-телефонии. Не менее популярны и услуги, связанные с размещением 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).

На рисунке 26 приводится логическая структура узла IPoP.

Разделение на виртуальные локальные сети осуществляется с помощью коммутатора локальной сети. Также в отдельный порт коммутатора, а также и в отдельную виртуальную локальную сеть, подключен пограничный маршрутизатор узла. Желательно, чтобы и маршрутизатор, и коммутатор поддерживали спецификацию IEEE 802.1q передачи сигнализации VLAN, так как в этом случае маршрутизатор может осуществлять маршрутизацию и фильтрацию IP-пакетов между всеми виртуальными сетями.

Пограничный маршрутизатор. Главной компонентой узла является пограничный маршрутизатор узла. Он обеспечивает следующие функции:

- связь с провайдерами Интернет более высокого уровня и/или связь с точкой обмена Интернет-трафиком;
- передачу трафика между различными компонентами узла;
- фильтрацию трафика и отражение атак на узел на первичном уровне;
- регулировку полосы пропускания между клиентами узла и серверами приложений;
- регулировку полосы пропускания между серверами приложений, web-hosting серверами и сетью Интернет;
- перенаправление HTTP-трафика в кэш-сервер.

К числу требований, предъявляемых к пограничному маршрутизатору узла, можно отнести поддержку протоколов BGP-4 и OSPF, достаточный объем оперативной памяти для размещения полных таблиц маршрутизации. Однако сегодня на первый план выходят расширенные требования к производительности, набору дополнительных услуг и их реализации.

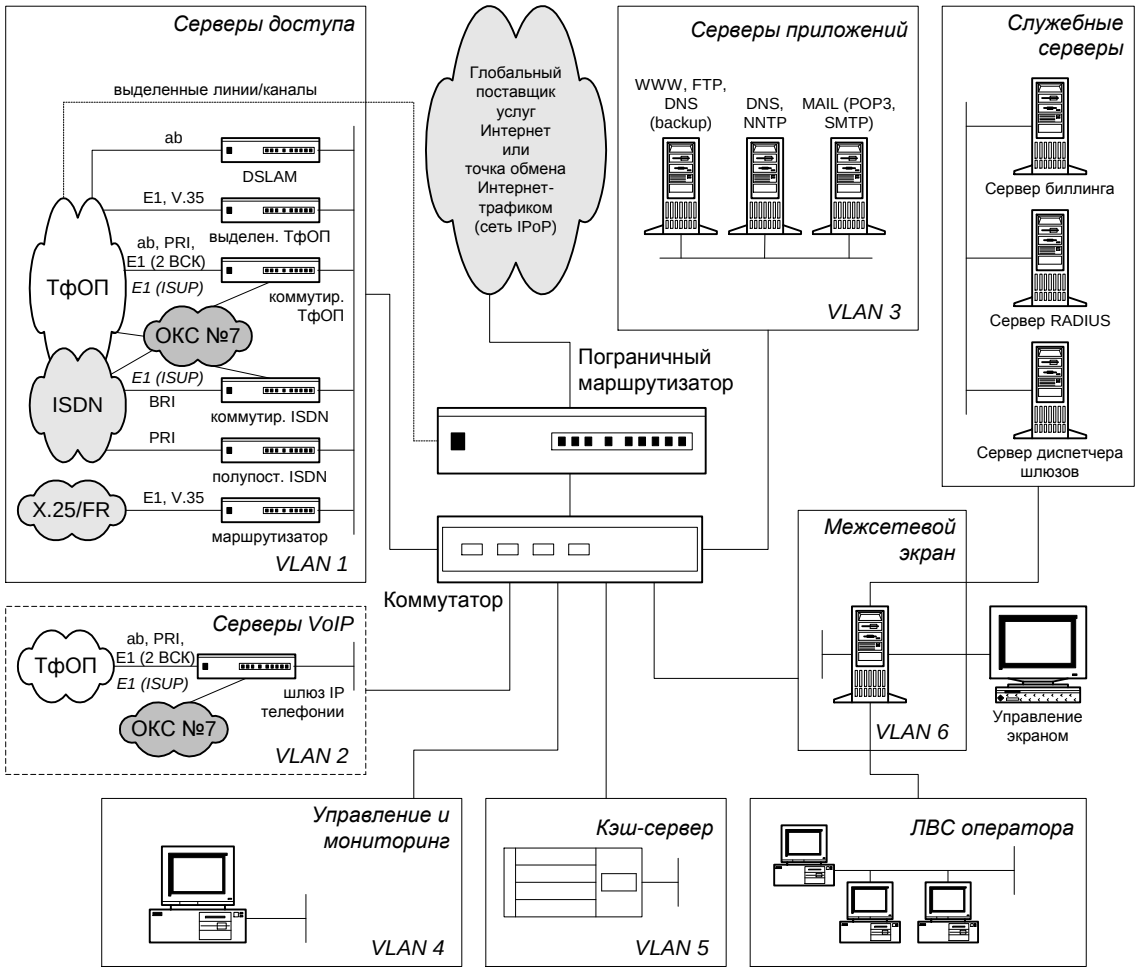


Рисунок 26 Диаграмма логической структуры узла IPoP наложенной сети доступа

Серверы доступа. Основными компонентами узла, ответственными за базовые услуги являются серверы доступа. В них агрегируются потоки трафика от пользователей коммутируемого доступа, также с их помощью подключаются клиенты, использующие выделенные линии для доступа в Интернет. В случае необходимости для подключения выделенных линий можно использовать и порты пограничного маршрутизатора.

Сервер удаленного доступа принимает от абонента аутентификационную информацию в соответствии с протоколами CHAP/PAP, взаимодействует с сервером аутентификации с целью проверки учетной информации пользователя и модификации его счета и устанавливает PPP-соединение[13].

Серверы доступ можно разделить на две функциональные части:

- модемный пул;
- сервер Dial-up обеспечивающий транспортировку сообщений TCP/IP по коммутируемой линии согласно протоколу PPP.

Рассмотрение вопросов подключения модемных пулов (серверов доступа) рассматриваются в разделе «Использование модемных пулов» настоящей работы.

Серверы VoIP. В концепции разделения услуг на базовые и дополнительные, данные сервера относятся к обеспечивающим функционирование дополнительных услуг.

[13] PPP – Point-to-Point-Protocol – протокол канального уровня, позволяющий транспортировать IP-пакеты по каналу «точка-точка», который может быть либо асинхронным, либо синхронным каналом. Стал фактически стандартом для глобальных линий связи при соединении удаленных клиентов с серверами и для образования соединений между маршрутизаторами. Для целей аутентификации PPP предлагает по умолчанию протокол PAP (Password Authentication Protocol), передающий пароль по линии связи в открытом виде, или протокол CHAP (Challenge Handshake Authentication Protocol), не передающий пароль по линии связи и поэтому обеспечивающий большую безопасность сети.

В настоящее время, несмотря на бурное развитие технологий в области конвергенции IP-сетей и сетей классической телефонии, качество передачи голоса по IP-сетям вообще, и тем более по Интернет, оставляет желать лучшего. Тем не менее, анализ нагрузки пользователей сети Интернет, включенных через ТфОП[14], показал, что при средней интенсивности исходящей нагрузки в 0,12 Эрл на соединения Интернет приходится 0,05 Эрл, а на телефонные соединения – 0,07 Эрл. Возможно, что для таких абонентов, являющихся пользователями Интернет, передача речи по IP-телефонии окажется привлекательной. Учитывая специфику данной услуги, необходимо осознавать тот факт, что пользователи будут требовать от этой услуги качества, соответствующего качеству классической телефонии.

Услуга IP телефонии обеспечивается использованием шлюзов IP телефонии и соответствующим программным обеспечением «диспетчер шлюзов».

Управление и мониторинг. Средства управления и мониторинга сетью обеспечивают контроль за состоянием портов серверов доступа, своевременное обнаружение канальных сбоев и исследование связанной с их использованием статистики.

Комплекс приложений сетевого управления и управления услугами, позволяет поставщикам услуг предлагать своим клиентам новые, необходимые им услуги. В числе типичных примеров: виртуальные частные сети, 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

Кэш-сервер. Практически все провайдеры в настоящее время используют серверы, занимающиеся кэшированием содержимого web-серверов. Использование кэширующих серверов преследует две основные цели:

- улучшение производительности: снижение нагрузки на каналы провайдера, используемые для выхода в Интернет и уменьшение времени ожидания загрузки страниц для клиентов провайдера;
- сокращение затрат: размер трафика на канал в Интернет после установки кэширующих серверов уменьшится, что приведет к снижению платежей за передачу информации по этим каналам.

Межсетевой экран – это система, которая отслеживает и ограничивает прохождение через нее пакетов. Существуют два основных типа межсетевых экранов – это пакетные фильтры и шлюзы уровня приложений. Межсетевой экран выполняет две функции:

- препятствует несанкционированному доступу к сети;
- препятствует несанкционированному выходу информации из сети.

Пакетные фильтры работают на уровне моста локальной сети, просеивая пакеты в основном по их адресам, и обеспечивают анализ, учет и, при необходимости, блокировку проходящего через него трафика. Такие устройства могут быть установлены на любой участок сети, требующий защиты.

Шлюзы уровня приложений ограничивают прохождение пакетов на основании типа приложения.

На первоначальном этапе целесообразно осуществить защиту с помощью межсетевого экрана двух наиболее важных элементов сети телефонного оператора: сегмента служебных серверов (автоматизированная система расчетов, диспетчер шлюзов VoIP, RADIUS-сервер) и офисной сети телефонного оператора. Безопасность серверов доступа, приложений, кэш-сервера и системы мониторинга предлагается организовать с помощью фильтров на пограничном маршрутизаторе узла.

Служебные серверы. Сервер аутентификации – централизованное хранилище зарегистрированных у провайдера пользователей с указанием пароля, окна доступа, состояния счета и т.д. Сервер аутентификации позволяет проводить аутентификацию

[14] Анализ производился специалистами ЛОНИИС, Россия.

пользователей при dial-up соединениях, а также хранить такую информацию для доступных пользователю сервисов.

Как правило, серверы доступа позволяют проводить аутентификацию, авторизацию и учет с помощью RADIUS, некоторые могут использовать для этих целей TACACS+[15]. Однако это не значит, что все сервера доступа выдают одну и ту же информацию о характеристиках модемной сессии пользователя. RADIUS значительно легче адаптируется к различного рода расширениям отчетной информации, генерируемой серверами доступа, и позволяет собирать ряд дополнительных сведений о скорости соединения модема пользователя, типе модуляции, причине завершения сеанса связи, когда требуется представлять отчет о сеансе пользователя не в стандартном, а расширенном виде.

Необходимой компонентой любого узла, предоставляющего коммерческие Интернет-услуги, является автоматизированная система расчетов. От ее гибкости в значительной мере зависит возможность предоставлять новые типы услуг, предлагать новые тарифные планы для привлечения новых пользователей.

Серверы приложений объединены в виртуальную локальную сеть VLAN 3. В своем составе содержат сервера DNS, FTP, SMTP, HTTP, NNTP.

Сервер DNS (Domain Name Server) – сервер именования доменов. Поддерживает таблицу соответствия IP-адресов доменным именам для принадлежащих провайдеру доменов (primary name servers). Обычно он хранит такие таблицы еще для нескольких доменов по договоренности с их владельцами (secondary name servers).

Сервисы Интернет верхнего уровня обеспечивают сервера:

- FTP (File Transfer Protocol) – протокол передачи файлов;
- SMTP (Simple Mail Transfer Protocol) – простой протокол электронной почты;
- HTTP (Hypertext Transfer Protocol) – протокол передачи гипертекстов;
- NNTP (New Network Protocol) – протокол передачи сетевых новостей.

3.1.2 Использование модемных пулов

Сетевое оборудование сети Интернет, обслуживающее пользователей, подключается к телефонной сети либо пучками серийных абонентских линий, либо соединительными линиями на правах станций. Сетевое оборудование, как в первом, так и во втором случае к оборудованию телефонной сети подключается посредством модемных пулов.

3.1.2.1 Назначение и предъявляемые требования

Модемные пулы предназначены для работы в узлах доступа телекоммуникационных сетей. Обычно модемный пул выпускается в стоечном исполнении, при этом на одной плате размещаются несколько модемов. Модемы находятся в режиме автоответа и соединяются с

[15] TACACS – Terminal Access Controller Access System – централизованная служба авторизации и аутентификации. Выполнена в архитектуре «клиент-сервер». Предполагается, что в организации установлен один сервер TACACS. На этом сервере хранится центральная база учетной информации пользователей – имена, пароли, списки прав доступа (определяющие подсети, компьютеры и сервисы, с которыми может работать данный пользователь, временные ограничения и т.п.), данные аудита (фиксация каждого логического входа, продолжительности сессии, время использования отдельных ресурсов сети). Клиентами сервера TACACS являются серверы удаленного доступа. В каждый такой сервер встроено программное обеспечение, реализующее стандартный протокол, по которому они взаимодействуют с сервером TACACS. Этот протокол также называется TACACS. В протоколе определено несколько типов запросов, с которыми клиенты обращаются к серверу TACACS. На эти запросы сервер должен ответить соответствующим сообщением. С помощью этих сообщений серверы удаленного доступа перенаправляют поток запросов на логическое подключение пользователей к сети в целом или к отдельным ее ресурсам серверу TACACS. Компания Cisco поддерживает в настоящее время в своих маршрутизаторах и серверах удаленного доступа усовершенствованный вариант протокола, названный ею TACACS+. В TACACS+ пароль уже не передается в открытом виде по сети, а шифруется с помощью алгоритма MD5. Учтены особенности большинства используемых в настоящее время протоколов аутентификации, в частности PAP, CHAP и в стандартном Telnet. Предусмотрен последовательный обмен несколькими словами-вызовами и ответами, как это делается в некоторых системах, использующих одноразовые пароли. Улучшено взаимодействие с системой Kerberos.

хост-компьютером или терминальным сервером. Платы монтируются в кассету 19-дюймового стандарта. Модемный пул имеет функцию централизованного сетевого управления. Это позволяет обеспечить большое число входов, энергонезависимое питание с резервированием, гарантирует работоспособность в круглосуточном и необслуживаемом режимах работы. Кроме того, стоечное исполнение предусматривает создание всего комплекса в едином конструктиве с использованием высоконадежных хост-компьютеров, сетевых устройств, внешней памяти.

В числе требований, относящихся к модемам, устанавливаемым на коммутируемых входах в узлах сетей, необходимо отметить следующее:

- возможность регулировки уровня выходного сигнала;
- корректная отработка команд и сигналов RS232 хост-компьютера;
- исключение «зависания» модемов;
- отработка алгоритмов работы при серийном включении в АТС;
- наличие достаточной внешней индикации и конфигурирования с панели;
- наличие дополнительных функций диагностики и статистики;
- наличие стоечной версии (при большом числе каналов).

3.1.2.2 Подключение к АТС

Модемный пул устанавливается на АТС или вблизи от нее и соединяется с ее оборудованием через ступень свободного искания. В последнее время получили большое распространение цифровые модемы, подключаемые к АТС по стыку Е1. Такой вариант включения, помимо снижения затрат на аппаратуру, дает и другие преимущества, прежде всего работа на скоростях 56 кбит/с. Модемная пул V.90 содержит группу модемов, обеспечивающих подключение к Интернет через оборудование IPoP абонентов АТС, использующих протокол PPP со скоростью 56 кбит/с.

Распространены следующие способы подключения провайдеров:

- через серийные номера по потокам PRI ISDN на узлах ведомственных телефонных станций (УВТС), которые, как правило, совмещены с узлами входящих сообщений (ГТС) или ЦС (СТС);
- через АМТС (серийный номер 8-600-100, потоки PRI ISDN).

Подключение провайдеров через серийные номера на оконечных АТС (или через учрежденческую АТС (УПАТС) к оконечной АТС) в Беларуси распространения не получили. «Общие технические требования к цифровым городским АТС» и «Общие технические требования к цифровым сельским АТС» определяют, что при организации абонентских линий с серийными номерами должна обеспечиваться возможность организации групп с серийным исканием до 64 линий в группе. При занятости всех линий в группе абонент отмечается недоступным.

С целью подключения серверов доступа к опорной АТС большинство ISP используют интерфейс Е1 первичного доступа ISDN с системой сигнализации DSS1 (PRI). Данное обстоятельство объясняется тем, что применение на ТфОП сигнализации R2 нормативно ограничено, а R1,5 редко поддерживается крупными зарубежными производителями оборудования. В то же время, использование сигнализации ОКС №7 для подключения серверов доступа к АТС практикуется крупными провайдерами.

Преимущества первого варианта подключения заключаются в следующем:

- высокая скорость установления соединения;
- большая надежность, обусловленная отсутствием многочастотных приемопередатчиков и внутренними процедурами самого протокола DSS1;
- высокая степень стандартизации протокола EDSS1.

Однако стоит отметить несколько моментов, сдерживающих внедрение протокола EDSS1 на ТфОП стран СНГ при подключении оборудования доступа ISP.

1. Большинство узлов не оснащены необходимым оборудованием, и даже на цифровых АТС установленные версии ПО не всегда обеспечивают возможность поддержки интерфейсов ISDN.
2. При существующей инфраструктуре городских сетей применение сигнализации EDSS1 делает невозможным использование некоторых услуг, обеспечиваемых серверами доступа, например, таких как «call back». Для применения данной услуги требуется, как минимум, определение номера абонента при входящей связи. Протокол EDSS1 не содержит средств принудительного запроса информации о номере вызывающего абонента. Номер поступит на оборудование, подключенное по EDSS1, только в том случае, если опорная АТС передаст его в сообщении SETUP при установлении соединения (услуга CLIP). Для этого опорная АТС должна получить номер вызывающего абонента от встречной АТС, что возможно либо при наличии между АТС системы сигнализации ОКС №7, либо при условии, что во время всех входящих соединений осуществляется запрос АОН. Первый вариант в настоящее время может быть реализован в единичном числе случаев, второй же практически неприменим, так как повлечет за собой перегрузку аппаратуры АОН встречных АТС электромеханических систем.

   Данная проблема решается использованием конвертеров сигнализации при подключении к опорным АТС по протоколу 2 ВСК.

Следует отметить, что присоединение серверов доступа напрямую к станции наталкивается на ограничение максимальной нагрузки на ее абонентские линии (0,15 Эрл).

3.1.3 Использование АТС с комбинированной системой коммутации

АТС с комбинированной системой коммутации (АТС-КСК) может быть использована для развития ТфОП с одновременным предоставлением услуг Интернет, не ухудшающим качество работы ТфОП.

3.1.3.1 Требования, предъявляемые к АТС-КСК

Переход к сети нового поколения требует от современных коммутационных узлов унифицированного взаимодействия с транспортными сетями, базирующимися на временном разделении каналов, и с сетями ОКС №7 наравне с IP-сетями. Кроме того, они должны поддерживать услуги, предоставляемые интеллектуальной сетью. Таким образом, речь идет об оборудовании, равноправно пропускающим трафик IP и трафик коммутации каналов с одновременной реализацией современных услуг, как входящих в перечень услуг интеллектуальной сети, так и некоторых новых.

Функции обслуживания вызовов в АТС-КСК должны быть в максимальной степени независимыми от:

- систем сигнализации (2ВСК, ОКС-7, EDSS1);
- типа среды передачи информации (TDM или IP);
- метода кодирования информации (G.711, G.723 или G.729).

Важно также, чтобы АТС-КСК поддерживали как интерфейсы сетей с коммутацией каналов, так и интерфейсы IP/Ethernet сетей, а также открытые интерфейсы, специфицированные ITU-T, ETSI, IETF и другими отраслевыми органами стандартизации, стандарты интеллектуальных сетей, включая наборы функциональных возможностей CS1 и CS2, и внешние интерфейсы, такие как PARLAY-совместимые интерфейсы, интерфейсы MGCP, H.323 и SIP.

3.1.3.2 Структура АТС с комбинированной системой коммутации

Структурная схема АТС-КСК приведена на рисунке 27 и имеет аналогичные функциональные узлы, как и на рисунке 26. К некоторым из них ниже приводятся дополнительные пояснения.

Блок VoIP служит для передачи речевого трафика через IP-сеть. Рекомендация H.323 определяет четыре компонента системы связи: диспетчер (gatekeeper), шлюз (gate), устройство управления многоточечной конференцией (MCU) и терминал. Устройство MCU необходимо для организации конференц-связи между тремя и более оконечными точками. И, наконец, терминал – это приложение, например клиент на ПК, отвечающее требованиям H.323.

PC Workstation обеспечивает функции техобслуживания, в том числе сбора учетной информации стоимости трафика сети Интернет. Примером ее функция являются контроль работы серверов, изменение параметров серверов, добавление новых зон в DNS и/или коррекции старых зон, исключение из сети пользователя и т.д.

Коммутатор Ethernet является стандартным устройством с функциями коммутации со скоростью 10/100/1000 Мбит/с и обеспечивает передачу пакетов между устройствами локальной сети провайдера – оператора ТфОП.

Коммутатор ATM обеспечивает преобразование выходных сообщений коммутатора Ethernet в потоки ячеек формата ATM со скоростью 155 Мбит/с для передачи их в широкополосную сеть ATM.

На основе традиционной цифровой системы коммутации 64 кбит/с в КС1 обеспечиваются следующие пользовательские интерфейсы:

- интерфейс для подключения к АТС-КСК аналоговых абонентов;
- базовый (2B+D) и первичный (30B+D) доступы для включения в ISDN оконечных абонентских устройств по протоколу EDSS1;
- терминальное оборудование (ПЭВМ и модем) для вхождения в сеть Интернет через АТС-КСК по протоколам TCP/IP.

С сетевой стороны АТС должна содержать стандартные входы в ТфОП с использованием систем сигнализации 2ВСК, EDSS1, ОКС-7 (ISUP), а также другие необходимые национальные системы сигнализации. При наличии на ТфОП высокоскоростной транспортной сети, построенной на базе SDH, в КС1 АТС-КСК осуществляется преобразование N-ISUP в B-ISUP по технологии ATM для стандартного подключения АТС-КСК к широкополосной цифровой сети.

На базе широкополосной системы коммутации КС2 АТС-КСК строится блок доступа в сеть Интернет (IAM). Входы КС2 АТС-КСК разбиваются на две группы:

1. входы, связанные с выходами Е1 системы КС1 с помощью модемных протоколов V.90;
2. входы арендованных (выделенных) линий от локальных вычислительных сетей и/или от блоков IAM других АТС ТфОП.

Последнее позволяет организовать территориальные сети доступа в Интернет. Выходы КС2 АТС-КСК в свою очередь разбиваются на два подмножества:

- выходы n×155 Мбит/с в стандарте ATM для подключения АТС-КСК к широкополосной сети Интернет;
- потоки Е1 к провайдерам сети Интернет, оперирующим потоками с данными скоростями.

Для выполнения техобслуживания АТС-КСК, в том числе тарификации услуг, предоставляемых Интернет, используется рабочая станция Workstation.

В КС2 АТС-КСК предлагаемой структуры существует возможность организации трех уровней коммутации для обеспечения взаимосвязи между пользователями услуг Интернет в АТС-КСК:

- уровень 1 – в блоке RAS;
- уровень 2 – в коммутаторе Ethernet Switch;
- уровень 3 – в ATM коммутаторе.

Применение нескольких уровней коммутации дает возможность равномерно распределить нагрузку на различные функциональные устройства КС2 АТС-КСК.

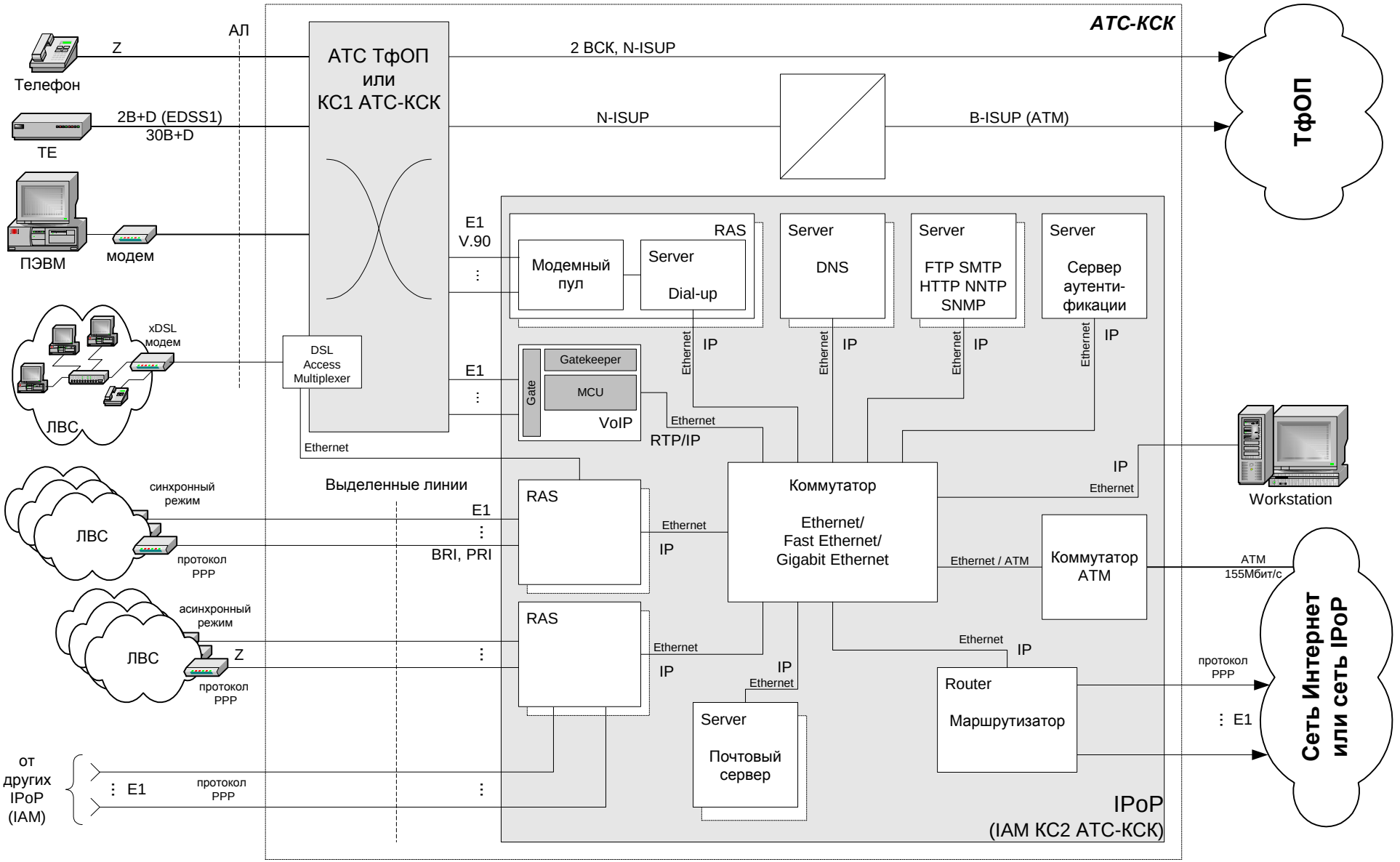


Рисунок 27 Структурная схема АТС с комбинированной системой коммутации

3.1.3.3 Преимущества АТС-КСК

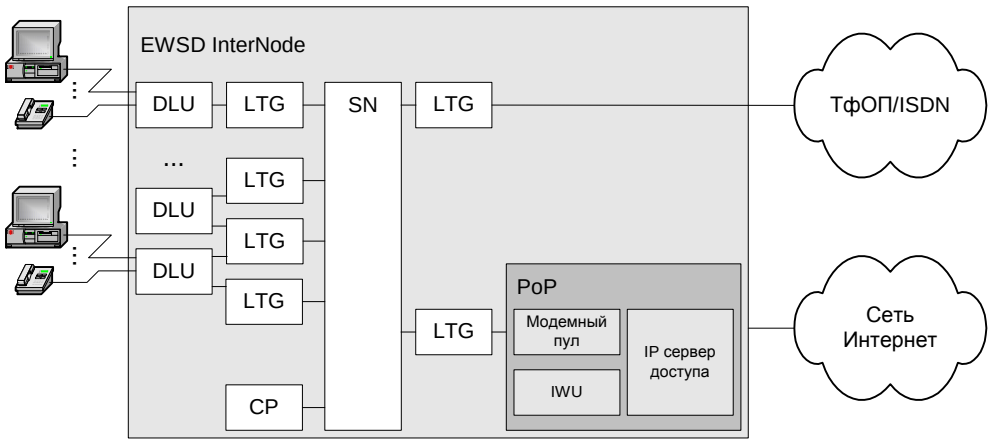
Преимущества интеграции IPoP в АТС-КСК:

- Подключение удаленного абонента (аналогового или ISDN) к сети Интернет.
- Физическая интеграция IPoP облегчает управление сетью.
- Модемный пул может быть встроен в удаленный абонентский концентратор.
- Упрощается реализация VoIP.
- Реализация функций шлюза IP-телефонии дает возможность использовать сети с коммутацией пакетов для предоставления услуг дешевой междугородной и международной связи.
- PC – телефон: передача голоса не блокирует сеанс Интернет.
- Телефон – PC: установление соединения с абонентом, занятом в сеансе Интернет (вызов переадресуется телефонной станцией к шлюзу)[16].
- Дополнительные Интернет-услуги, которые могут быть предложены только оператором ТфОП, выступающим одновременно в роли провайдера Интернет.

3.1.3.4 Коммутационные системы различных производителей

3.1.3.4.1 EWSD InterNode от Siemens

Коммутационная система EWSD фирмы Siemens с встроенным оборудованием доступа к Интернет показана на рисунке 28.



CP - Coordination Processor(координационный процессор)
DLU - Digital Line Unit (цифровой абонентский блок)
LTG - Line/Trunk group (линейная группа)
IWU - Interworking Unit (блок межсетевого обмена)

Рисунок 28 Архитектура EWSD, включающая оборудование сопряжения с Интернет

Взаимодействие EWSD с непосредственными и удаленными dial-up абонентами (характеризуемыми своими IP-адресами) основано на интеграции шлюза доступа к Интернет – PoP (Point of Presence) – в систему EWSD. В дополнение к обычным функциям шлюза Интернет PoP выполняет функции обработки вызова (рисунок 29).

[16] Абоненту, подписавшемуся на такую услугу должен быть присвоен внутристанционный номер, на который переадресуется вызов при работе абонента в сети Интернет.

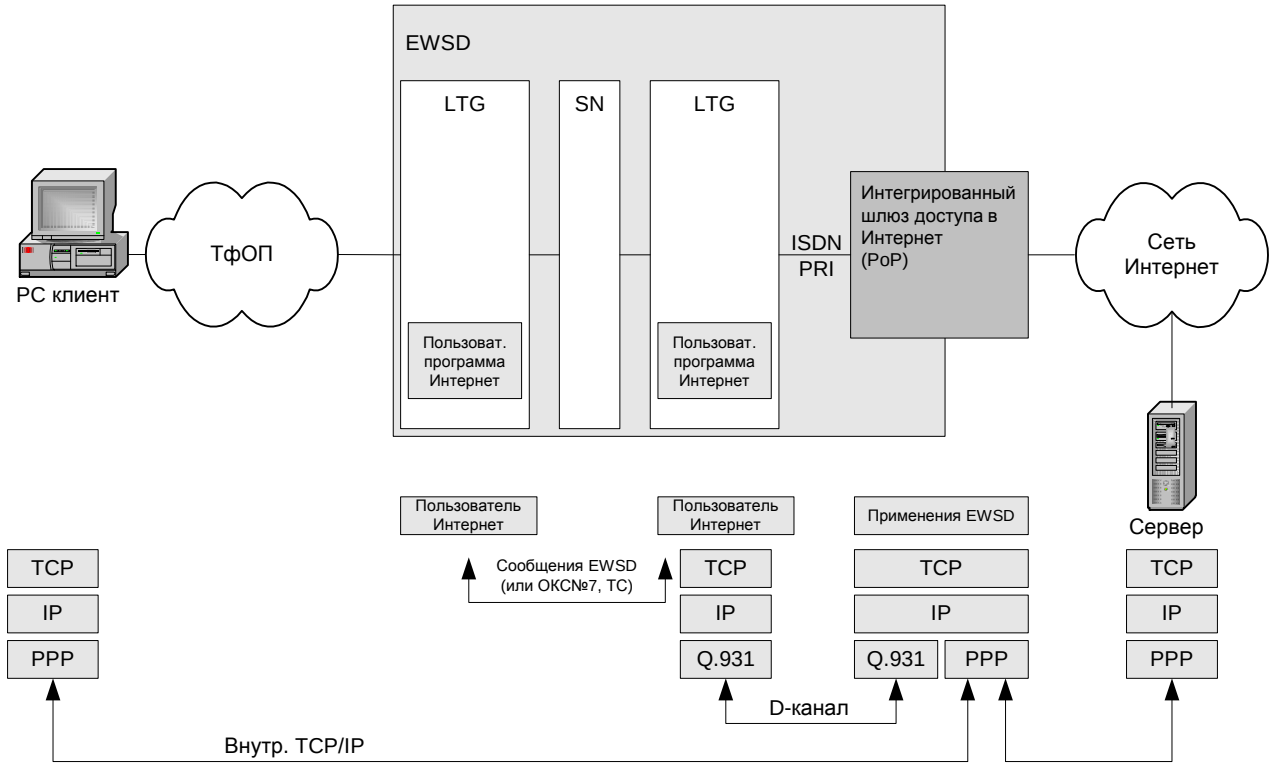


Рисунок 29 Управление вызовом и взаимодействие через IP

Как показано на рисунке 29, архитектура PoP максимально открыта. Поэтому PoP может быть легко интегрирован в уже работающую систему EWSD (при наличии соответствующего программного обеспечения для управления).

Дополнительные услуги в EWSD InterNode (ISS) представляют собой пакет программного обеспечения, распределенного среди аппаратных средств (рисунок 30). Его элементы, в зависимости от выполняемых функций, находятся:

- на станции EWSD,
- на соответствующем PoP,
- на EWI-сервере, и на абонентском компьютере.

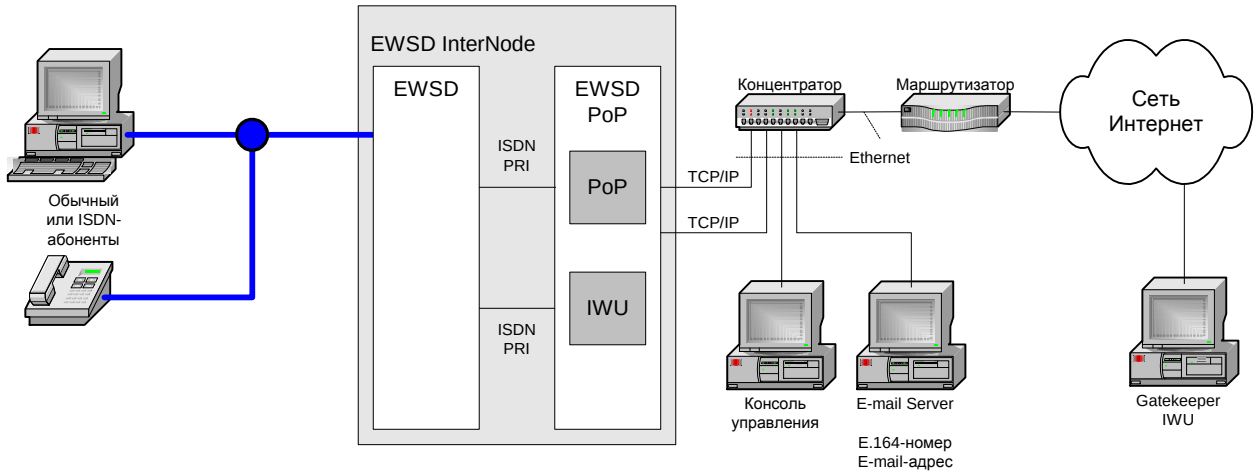


Рисунок 30 Структура сети, построенной на базе EWSD InterNode

EWSD обеспечивает PRI-интерфейсы для связи PoP/IWU и управления дополнительными услугами Интернет.

К **шлюзу доступа в Интернет – PoP** – пользователь Интернет подключается по аналоговой или цифровой (ISDN) линии, далее через коммутационное поле EWSD и LTG,

которая соединена с PoP по PRI-интерфейсу. Станция EWSD управляет шлюзом доступа как учрежденческой АТС с PRI. PoP включается в сеть данных через интерфейс Ethernet 10/100 BaseT.

Блок межсетевого обмена IWU является «воротами» между ТфОП и IP-сетью. IWU преобразует и уплотняет ИКМ-кодированный речевой сигнал в пакет и наоборот. IWU необходим для реализации функции VoIP и ее разновидностей. Он включается в сеть данных через интерфейс Ethernet 10/100 BaseT.

Консоль управления выполняет функции управления PoP/IWU.

Почтовый сервер информирует PoP каждый раз, когда изменяется статус электронной почты обслуживаемого абонента («пришло новое сообщение», «сообщение прочитано» и т.д.). Это делается с помощью специальной программы на почтовом сервере, соотносящей идентификатор электронной почты с соответствующим номером E.164 (используя корреляционную базу данных). Почтовый сервер передает номер E.164 и статус электронной почты дальше на PoP.

Диспетчер (gatekeeper) необходим для передачи голоса через Интернет. Является важнейшим компонентом сети H.323. Выполняет функции управления вызовом: перевод номера E.164 в IP-адрес и обратно, управление полосой пропускания. Соединяется с PoP через Ethernet. Для больших конфигураций требуется подключение внешнего диспетчера.

Концентратор/маршрутизатор. В функции концентратора входит соединение всех устройств, расположенных на станции, с IP-интерфейсами и подключение к Интернет через маршрутизатор. Маршрутизатор – устройство для пересылки трафика между сетями.

3.1.3.4.2 7R/E от Lucent Technologies

(Revolutionary/Evolutionary) Packet Solutions, которое представляет Lucent, позволяет операторам создавать надежные и масштабируемые пакетные сети. PTS (Packet Toll/Transit Solution) – компонент этого набора решений – предоставляет им возможность преобразовать существующие TDM-транспортные сети в сети, основанные на пакетных протоколах ATM или IP за счет дооборудования коммутатора 5ESS интерфейсом пакетной передачи.

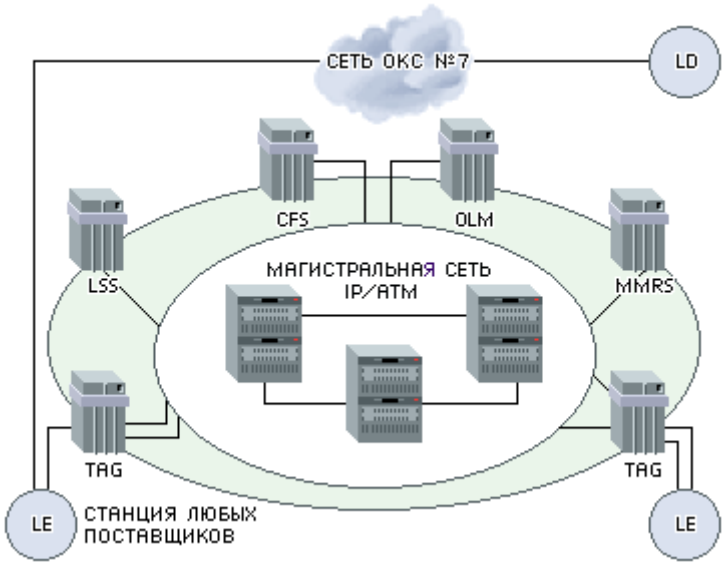


Рисунок 31 Транзитное решение 7R/E (PTS)

Элементами концепции 7R/E являются (рисунок 31):

- **7R/E Call Feature Server.** Отвечает за обработку вызова в концепции 7R/E и обеспечивает совместимость со всеми услугами, которые использовались в классической цифровой телефонной станции. Сервер поддерживает до 3000 функций, и в том числе, услуги интеллектуальной сети.

- **7R/E Packet Driver.** Модуль, который позволяет владельцам 5ESS плавно и безболезненно перейти от систем с временным уплотнением к пакетным системам.
- **7R/E Programmable Feature Server.** Основан на продукте Lucent Softswitch и позволяет операторам самостоятельно или с привлечением третьей стороны разрабатывать собственные услуги.
- **7 R/E Multimedia Resource Server.** Позволяет создавать услуги со сложной обработкой речевой и другой информации. Например, распознавание речи и изображения.
- **7 R/E One Link Manager.** Система управления элементами концепции 7 R/E.
- **7 R/E Packet Gateway.** Оборудование доступа для объединения различных источников включая DSL, кабельные модемы и беспроводной доступ.
- **7 R/E Trunk Access Gateway.** Обеспечивает связь пакетной сети PTS с ТфОП.

3.1.3.4.3 ПРОТЕЙ ЛОНИИС

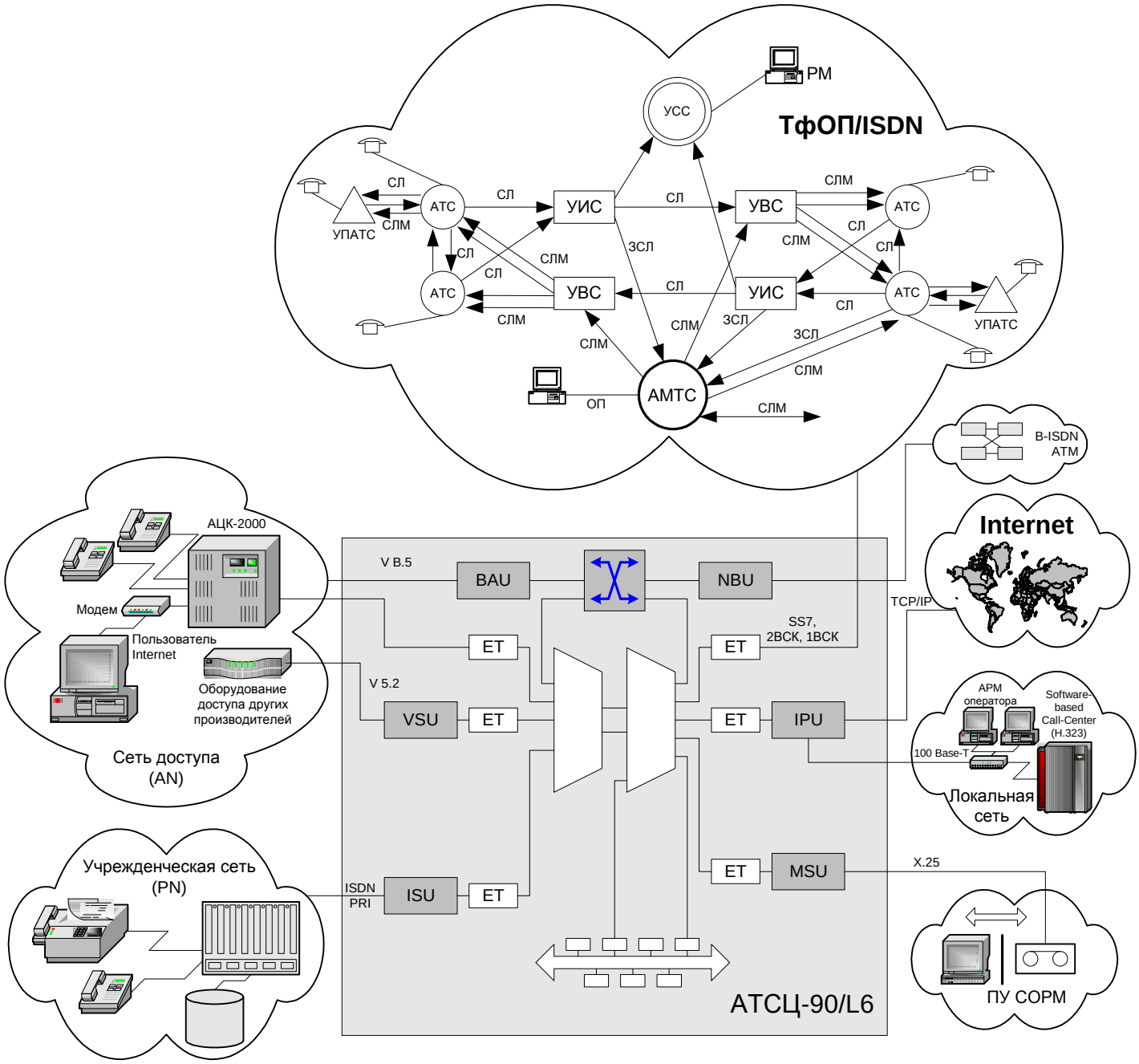
Для решения проблемы отвода трафика сети Интернет от СЛ ТфОП в коммутационном оборудовании АТСЦ-90 выбран вариант организации точки присутствия Интернет.

Модуль IPU (рисунок 32), входящий в комплекс оборудования АТСЦ-90, позволяет организовать интеграцию оборудования коммутации каналов АТСЦ-90 с сетями на основе коммутации пакетов. Модуль IPU является интегрированным сервером доступа: в качестве шлюза IP-телефонии от обеспечивает передачу речевого трафика и факсимильных сообщений по сетям с маршрутизацией пакетов IP, а в качестве сервера удаленного доступа к IP-сетям предоставляет абонентам ТфОП доступ к сети Интернет или к удаленным ЛВС по коммутируемым линиям.

Модуль IPU подключается к АТСЦ-90 (или к любой другой АТС) по цифровым трактам Е1 с использованием систем сигнализации ОКС№7 (ISUP) или EDSS1, а к сетям с маршрутизацией пакетов IP – с помощью интерфейса 10/100 BaseT. Сервер автоматически (по набранному номеру) распознает, какое из приложений должно быть использовано для обслуживания поступившего вызова.

Кроме интегрированного сервера доступа в состав программно-аппаратного комплекса оборудования АТСЦ-90 входит диспетчер сети IP-телефонии (Gatekeeper). Он выполняет функции управления зоной сети IP-телефонии, в которую входят терминалы, шлюзы и устройства управления конференциями, зарегистрированными в диспетчере.

Для организации информационно-справочных служб в составе АТСЦ-90 создан Центр обработки вызовов, реализованный на базе технологии IP-телефонии с поддержкой протокола H.323.



- Блок VSU обеспечивает интерфейс V5.2 сети доступа
- Блок BAU обеспечивает широкополосный абонентский доступ
- Блок ISU организует PRI ISDN
- Блок NBU обеспечивает включение АТСЦ-90 в широкополосную сеть B-ISDN, ATM
- Блок MSU поддерживает функции СОРМ
- Блок IPU обеспечивает взаимодействие оборудование АТС с сетями на базе коммутации пакетов, обеспечивая доступ абонентов ТфОП к ресурсам сети Интернет, функции VoIP, FoIP

Рисунок 32 Структура АТСЦ-90

3.2 Размещение узлов IPoP на сети

3.2.1 Конфигурация АТС с размещенным на ней узлом IPoP

Любому из абонентов АТС с размещенным на ней узлом IPoP (АТС-КСК) предоставляется возможность выхода в ТфОП через коммутационную систему каналов (КС1 АТС-КСК) по коммутируемым абонентским линиям (АЛ). Абоненты АТС с размещенным на ней узлом IPoP (АТС-КСК), одновременно являющиеся пользователями услуг сети Интернет, должны быть оснащены соответствующим терминальным оборудование (ПЭВМ и модемом) и подключаться через АТС (КС1 АТС-КСК) ко входам блока IPoP (КС2 АТС-КСК) согласно модемным протоколам V.90.

Локальным вычислительным сетям (ЛВС), имеющим интенсивный трафик через сеть Интернет (в пределах нескольких десятков Мбит/с), экономически эффективно использовать арендованные (выделенные) линии, подключаемые к Интернет через блок IPoP.

Чтобы АТС ТфОП предоставляла своим абонентам услуги Интернет, ее следует сконфигурировать по одному из двух вариантов:

1. Выделить в зависимости от интенсивности предполагаемого трафика одну или несколько линий Е1, включаемых на встречной стороне по межстанционной связи в АТС (КС1 АТС-КСК) далее транзитом в IPoP (КС2 АТС-КСК) по линиям Е1 с протоколом V.90 (рисунок 33).

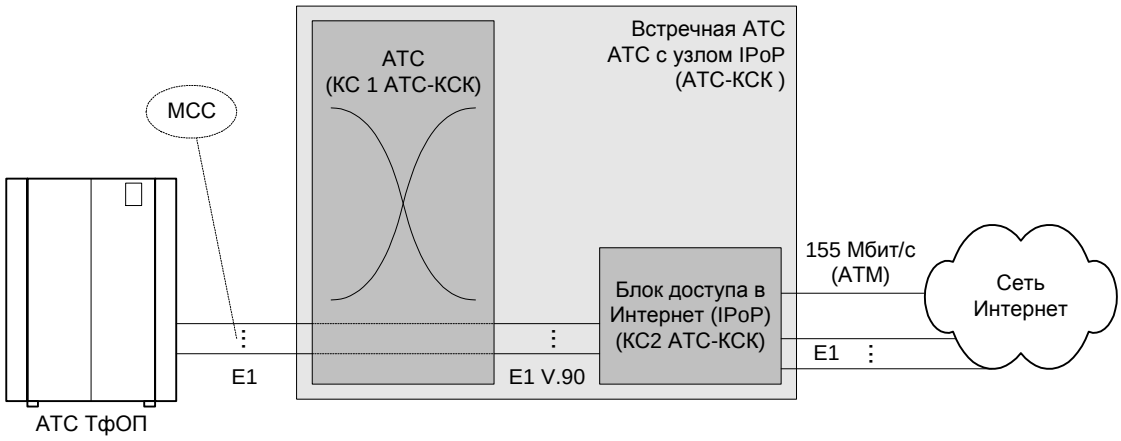


Рисунок 33 Первый вариант конфигурации АТС

В данном случае АТС-ТфОП отводится роль закрепления одной или нескольких линий ИКМ-30 за пользователями Интернет, а все остальные функции возлагаются на блок IPoP (IAM АТС-КСК).

2. через линии Е1 по модемному протоколу V.90 подключить IPoP (КС2 АТС-КСК), обеспечивающую доступ пользователей данной АТС в Интернет. В этом случае выходы Е1 блока IPoP (КС2 АТС-КСК) АТС ТфОП на встречной стороне отображаются в виде входов Е1 (от IPoP других АТС ТфОП) в блок IPoP данной АТС (КС2 АТС-КСК) и уже отсюда поступают к провайдеру Интернет следующего уровня по линиям 155 Мбит/с или Е1 (рисунок 34).

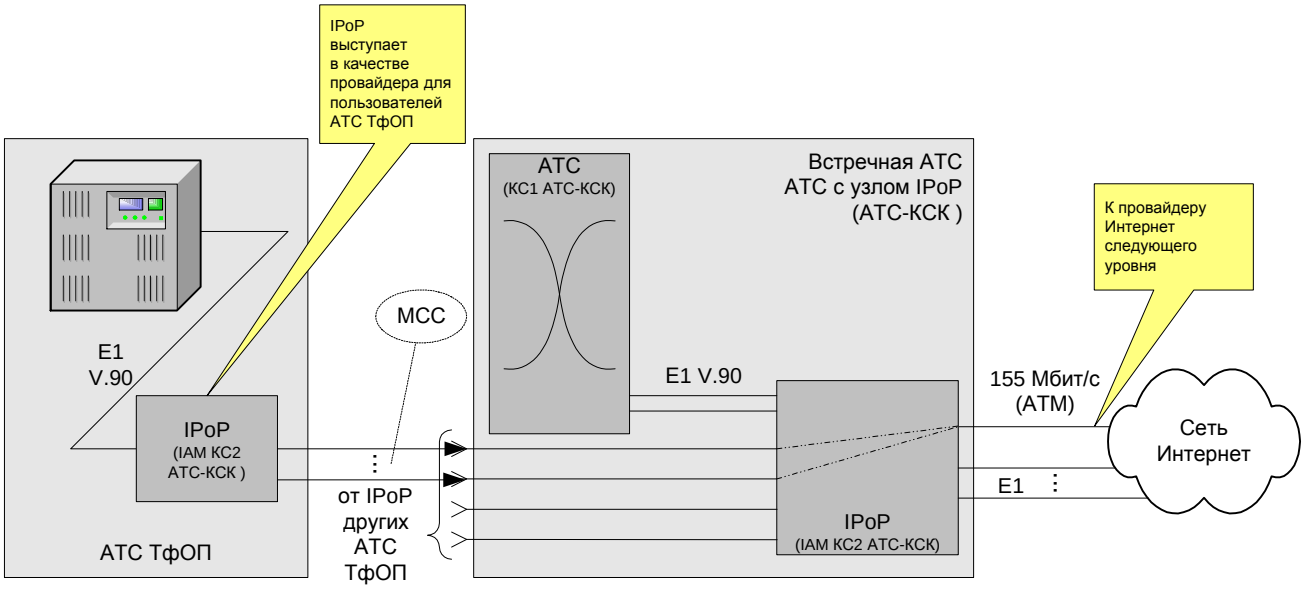


Рисунок 34 Второй вариант конфигурации АТС

Основные функции обеспечения переносятся в существующую АТС ТфОП, а главной функцией блока IPoP (КС2 АТС-КСК) будет подключение входных линий Е1 от АТС ТфОП на соответствующий выход IPoP (КС2 АТС КСК).

АТС-КСК функционально структурирована так, чтобы ее отдельный модуль – блок доступа к сети Интернет – мог самостоятельно использоваться для подключения к АТС ТфОП с целью предоставления абонентам сети общего пользования выхода в сеть Интернет на скорости 155 Мбит/с и Е1. Таким образом, в рассматриваемом случае КС2 АТС-КСК выступает в качестве провайдера для пользователей существующей АТС ТфОП.

3.2.2 Структура сети передачи данных с узлами IPoP

При создании сети передачи данных с узлами IPoP необходимо учитывать, что точку разделения трафика IP на ТфОП/ISDN желательно смещать в сторону оконечного пользователя, если не до уровня сети доступа, то, по крайней мере, до уровня оконечной станции.

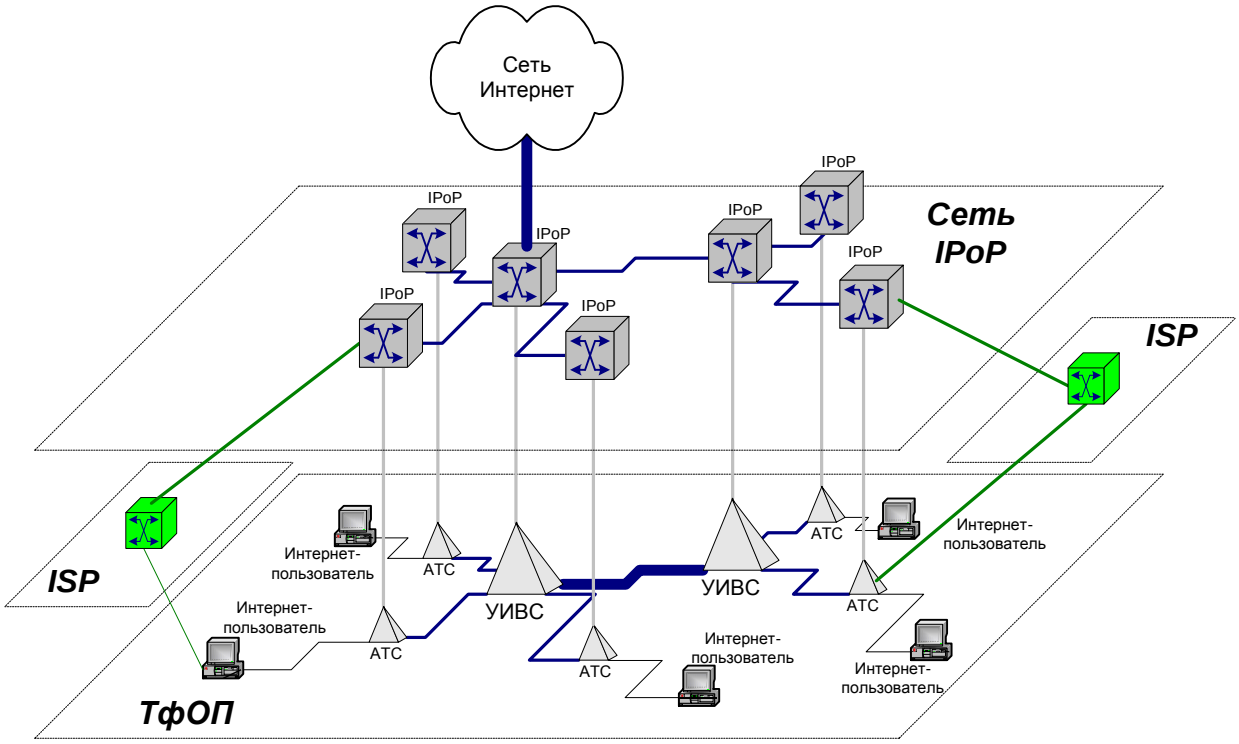


Рисунок 35 Структура наложенной сети IPoP для местной телефонной сети с узлообразованием и повторением структуры ТфОП

Структура наложенной сети IPoP для местной телефонной сети с узлообразованием изображена на рисунке 35. В общем случае она повторяет структуру ТфОП, хотя в зависимости от нагрузки пользователей сети Интернет и развития сети IPoP ее структура может отличаться от структуры ТфОП за счет объединения IPoP для нескольких АТС и/или узлов (рисунок 36). Важно отметить, что наложенная сеть IPoP сможет выполнить не только функцию среды передачи трафика в сеть Интернет, но и позволит операторам осуществлять функции провайдера услуг сети Интернет ISP.

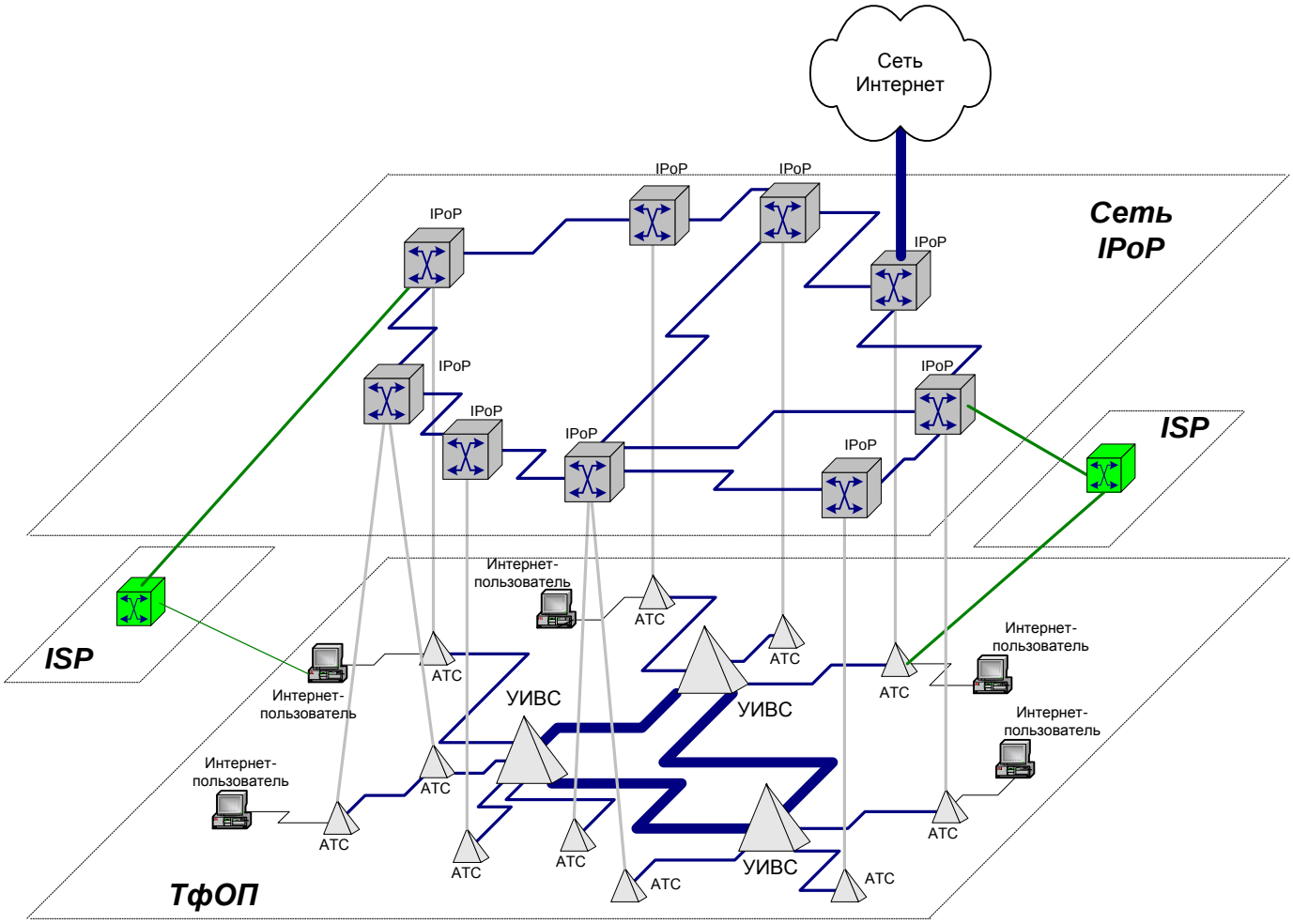


Рисунок 36 Структура наложенной сети IPoP для местной телефонной сети с узлообразованием без повторения структуры ТфОП

Для решения проблемы устранения негативного влияния Интернет-пользователя на работу телефонной сети рекомендуется на каждой узловой телефонной станции устанавливать хотя бы один сервер доступа. Если на конечной АТС пользователей Интернет мало, то их трафик может направляться на узловую АТС по обычным соединительным линиям, а если их много, рекомендуется, чтобы сервер доступа все равно находился на узловой станции, но к нему вел выделенный канал, например, E1, сформированный с помощью системы передачи.

Обоснование для такой конфигурации следующее.

1. Когда серверы доступа размещены только на узловых телефонных станциях, имеется небольшое число точек присутствия Интернет (IPoP), что облегчает управление и развертывание новых услуг. Между тем с появлением таких технологий, как DWDM, пропускная способность линий связи уже не является узким местом, и стоимость организации дополнительных каналов значительно уменьшается.
2. Если серверы доступа располагать на конечных АТС, то для унификации управления придется соединять конечную АТС с узловой полноценной сетью передачи данных, а это потребует дополнительных затрат на развертывание дополнительного сетевого оборудования, например, маршрутизаторов.

3.2.3 Взаимодействие с ОКС №7

Поддержка системы телефонной сигнализации – важнейшее условие для взаимодействие сервера Интернет-доступа с ТфОП. Причем основное внимание следует уделить общеканальной системе сигнализации ОКС №7, которая благодаря своим многочисленным достоинствам заняла в последнее время главенствующее положение в ТфОП. Так, согласно концепции, предложенной ЛОНИИС (рисунок 37), на базе интеллектуальной платформы «ПРОТЕЙ», могут создаваться узлы услуг для конвергированных сетей. Такие узлы позволят операторам в рамках одной системы предоставлять услуги, характерные для технологий:

- классической интеллектуальной сети (по стандартам ITU);
- компьютерной телефонии (по стандартам ECTF);
- IP-телефонии.

Разумеется, при реализации такой платформы активно используются ресурсы сети ОКС №7.

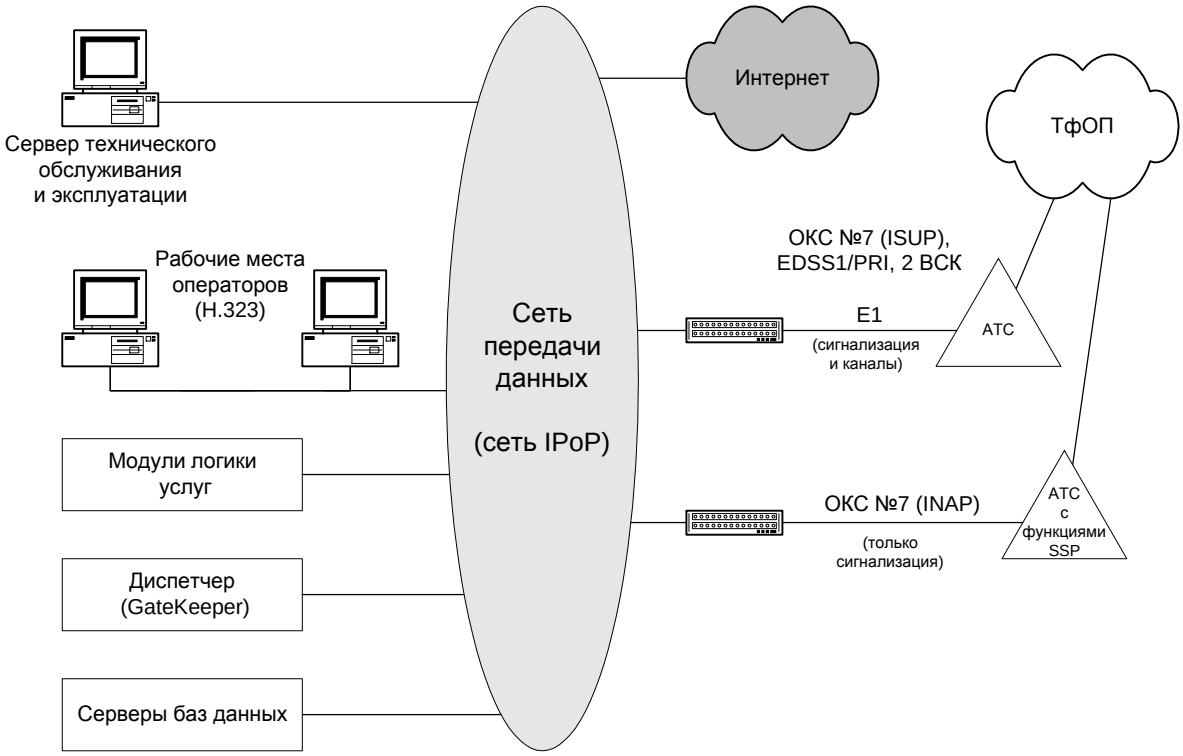


Рисунок 37 Интеграция трех технологий – IN, CT и IP (по концепции ЛОНИИС)

В качестве примера можно взять услугу интеллектуальной сети, основой которой является сеть ОКС № 7, «Internet Call Waiting» (ICW). Услуга ICW позволяет известить пользователя во время сеанса связи с Интернет о поступившем телефонном вызове. Оповещенный пользователь имеет на выбор несколько опций: ответить на вызов, приостановив сеанс с Интернет, перенаправить вызов в почтовый ящик речевых сообщений, послать сигнал ожидания или игнорировать вызов. Если пользователь решил ответить на вызов, то он маршрутизируется по телефонной сети, а сеанс с Интернет прекращается или приостанавливается с отключением модема. Схема предоставления услуги ICW показана на рисунке 38.

Кроме того, как уже отмечалось ранее, с помощью ОКС №7 организуются субтранки в пучках СЛ, позволяя разделить трафик данных («модемные» вызовы Интернет-доступа) и голосовой трафик.

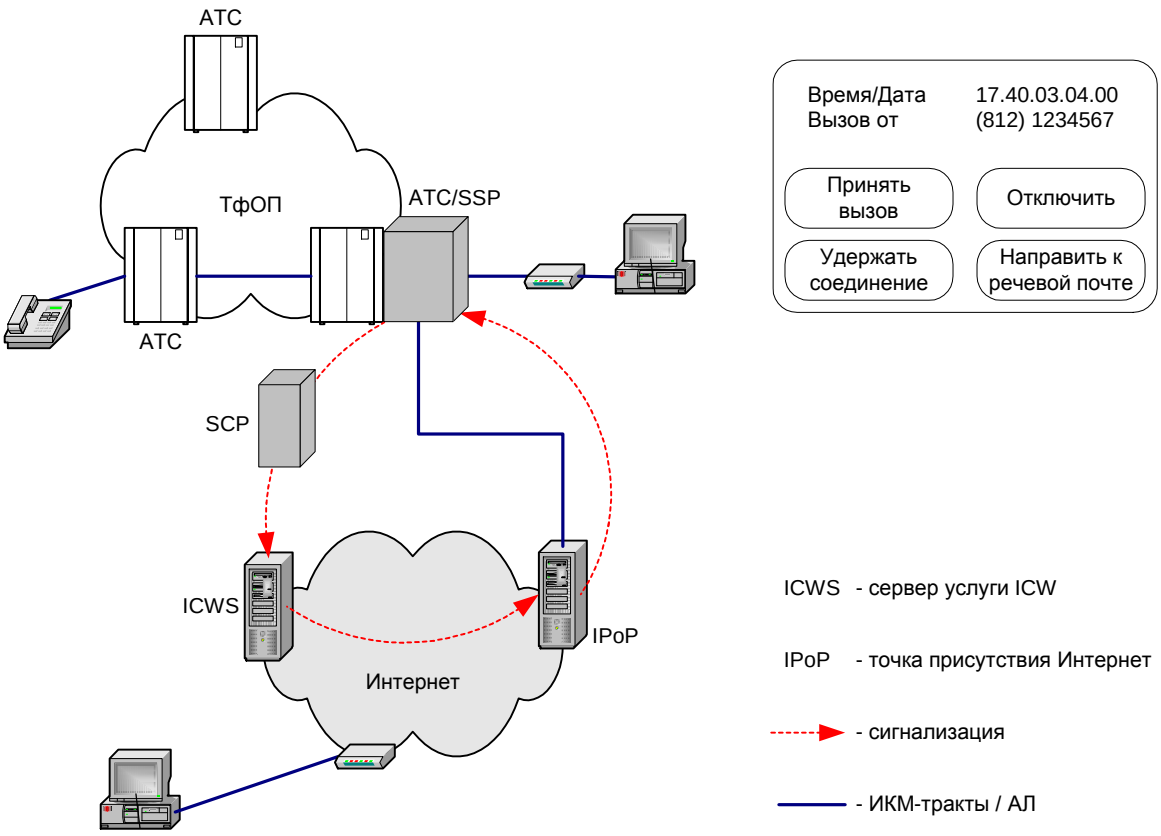


Рисунок 38 Схема предоставления услуги ICW

Следует учитывать, что когда разворачивается большая сеть коммутируемого Интернет-доступа, устанавливается не один, а множество серверов, и сопряжение каждого из них с сетью сигнализации ОКС №7 может оказаться весьма дорогим решением, так как для каждого сервера потребуются выделение своего кода сигнального пункта, подключение двумя каналами сигнализации с целью повышения отказоустойчивости и т.д. Для решения этой проблемы один сервер (или несколько серверов – все зависит от размеров инфраструктуры) взаимодействует с сетью ОКС №7 напрямую и передает сигнальную информацию по IP-сети остальным серверам, выполняя, таким образом, функцию шлюза ОКС №7: принимает сигнализацию ОКС №7, выделяет высокоуровневые сообщения (TUP/ISUP) и упаковывает их для передачи по IP-сети. Один и тот же сервер доступа может одновременно выполнять функции и шлюза сигнализации ОКС №7, и сервера доступа. Однако, в целях устойчивости работы системы, производителями рекомендуется функции сервера доступа и шлюза сигнализации ОКС №7 возлагать на различные серверы (рисунок 39).

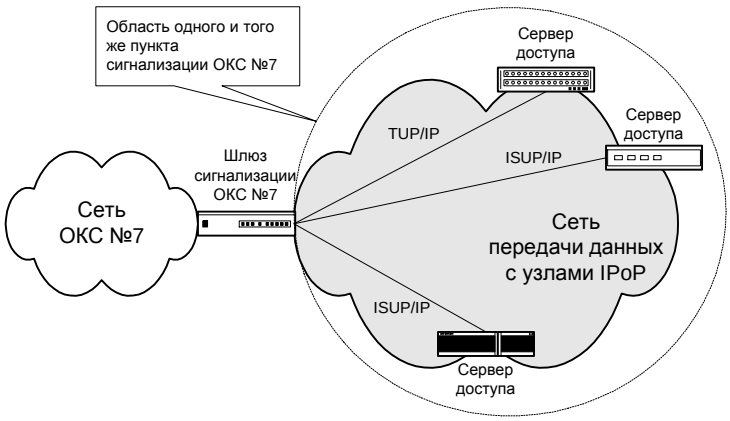


Рисунок 39 Сеть передачи данных с узлами IPoP при разделении пункта сигнализации

Возможный вид гипотетической сети передачи данных с узлами IPoP представлен на рисунке 40. Предполагалось, где что пункты сигнализации оконечно-транзитные STP располагаются на транзитных узлах ТфОП, куда также включается оборудование ISP.

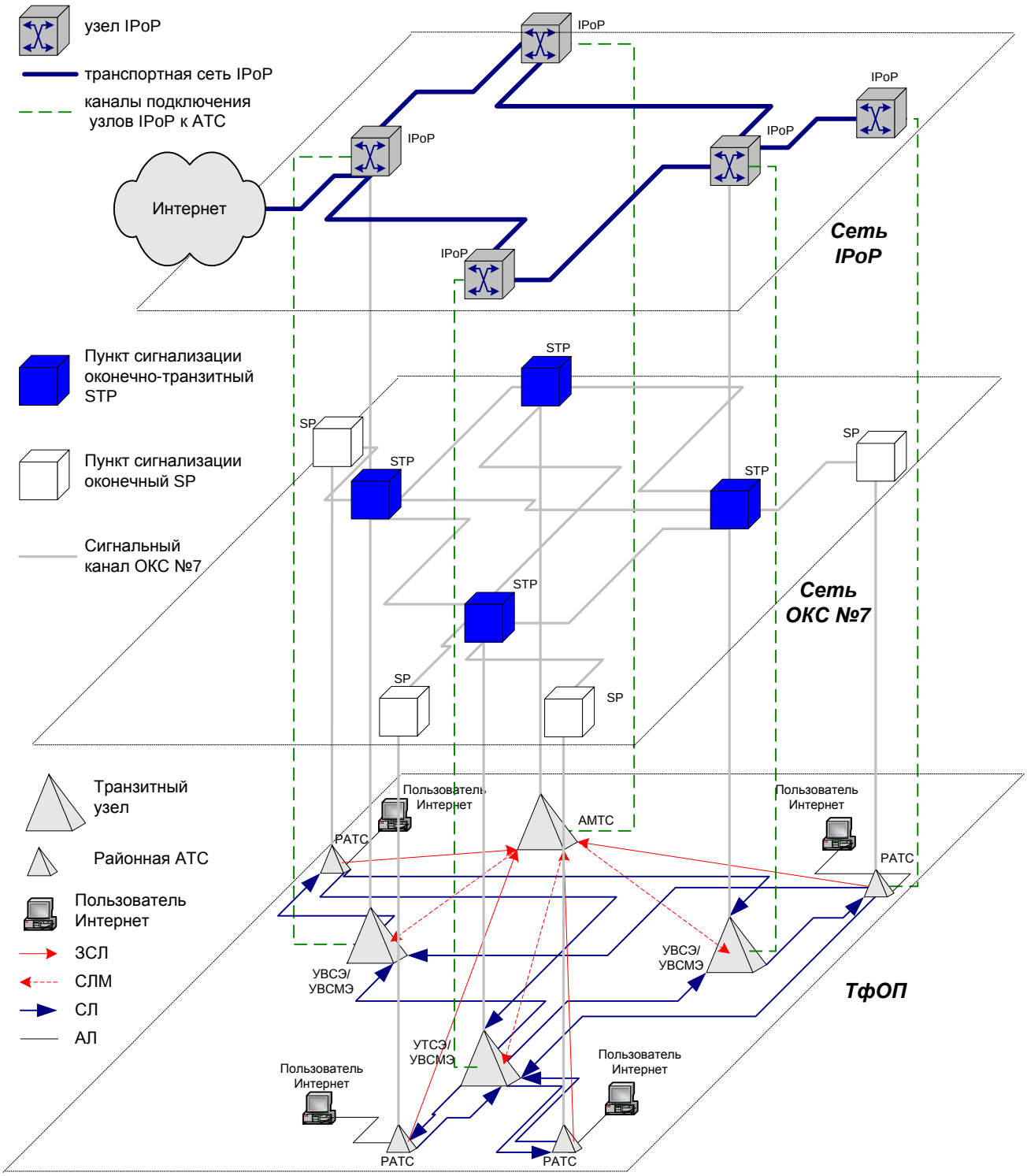


Рисунок 40 Взаимодействие сети с узлами IPoP с сетью сигнализации ОКС №7

«Общие технические требования к городским цифровым АТС» и «Общие технические требования к сельским цифровым АТС» использование на межстанционных СЛ сигнализации ОКС №7 предусматривают для ГАТС/САТС с функциями ISDN.

«Общие технические требования к городским цифровым АТС» формирование сети ОКС №7 определяют следующим образом:

- ГАТС с функциями ISDN должна обеспечивать реализацию функций пункта сигнализации (SP) сети ОКС №7.
- Возможность реализации транзитных пунктов сигнализации (STR) и пунктов трансляции сигнализации с переприемом (SPR) может быть регламентирован ТУ на ГАТС с функциями ISDN.
- ГАТС с функциями ISDN должна обеспечивать обслуживание соединений подсистем:
  - передачи сообщений (MTP);
  - управления соединениями сигнализации (SCCP);
  - пользователя ISDN (ISUP);
  - возможностей транзакции (TC).

«Общие технические требования к сельским цифровым АТС» содержат следующие требования к сети и системе общеканальной сигнализации:

1. Центральная и узловая АТС с функциями ISDN должна обеспечивать реализацию функций пункта сигнализации (SP) сети ОКС №7. Оконечная САТС должна обеспечивать реализацию функций SP в случае применения на участке между оконечной станцией (ОС) и узловой (УС) или центральной (ЦС) станциями системы сигнализации ОКС №7. Возможность реализации функций транзитных пунктов сигнализации (STP) и пунктов обработки соединений подсистемы SCCP (SPR) на ЦС или УС САТС должна быть согласована с изготовителем конкретной САТС с функциями ISDN.
2. САТС с функциями ISDN на уровне ОС должна обеспечивать, как минимум, функционирование подсистем MTP и ISUP, а также может обеспечивать функционирование подсистем SCCP и TC.
3. Для связи на уровнях узла сельско-пригородной связи (УСП), ЦС и УС применение ОКС №7 рекомендуется вне зависимости от количества используемых в данном направлении первичных групп Е1.
4. Систему сигнализации ОКС №7 рекомендуется применять также для связи между ЦС (УС) и ОС в случае, если количество первичных групп больше одной. В случае использования одной первичной группы Е1 рекомендуется применять систему сигнализации EDSS1.

Техническими условиями на конкретную ГАТС, САТС с функциями ISDN могут нормироваться также спецификации других подсистем ОКС №7 в случае необходимости и возможности их реализации.

3.2.4 Состав оборудования узлов IPoP

Состав оборудования на узлах IPoP определяется следующими факторами:

- количество абонентов коммутируемого доступа;
- количество абонентов xDSL доступа;
- количество выделенных абонентов;
- тип оборудования АТС;
- расположение точки подключения к глобальному поставщику услуг Интернет.

На рисунке 41 представлена конфигурация некоторой наложенной сети передачи данных с узлами IPoP. Как видно из представленного рисунка, отдельные узлы могут оснащаться только серверами доступа (IPoP 1), в то время как другие оснащаются не только серверами доступа, но средствами централизованных служб аутентификации и авторизации (IPoP 2, IPoP 3), серверами приложений (IPoP 3).

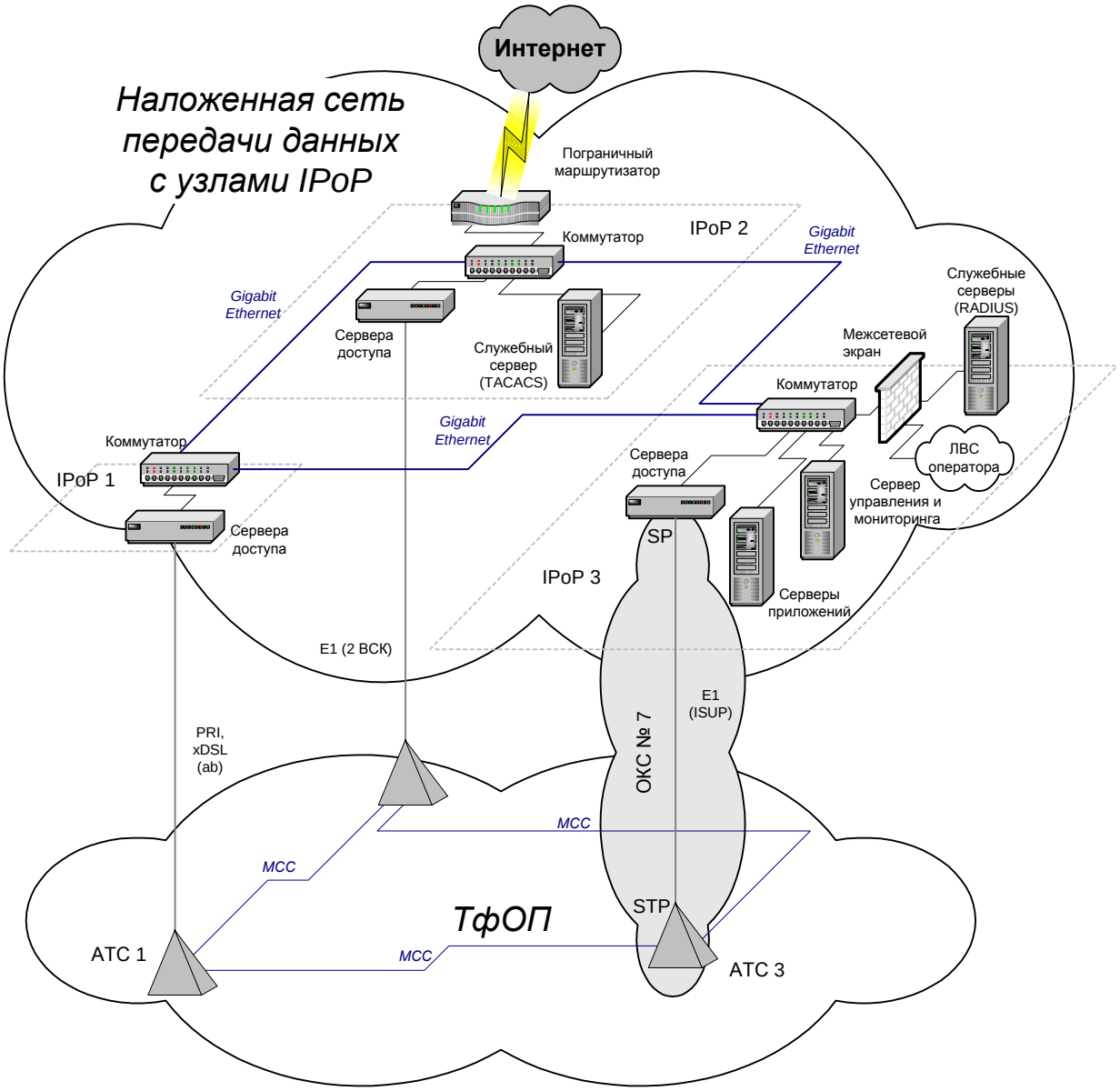


Рисунок 41 Состав оборудования различных IPoP

3.2.5 Подключение поставщиков услуг Интернет

Важным вопросом, связанным с качеством предоставляемых услуг и с нагрузкой на местные телефонные сети, является организация пропуска внутрисетевого и межсетевого, в том числе, междугородного и международного трафика сети Интернет. Существует потенциальная угроза, что эти каналы могут стать узким местом в сети Интернет, существенно снижающим эффективную скорость передачи данных и создающим тем самым дополнительную нагрузку на местных участках телефонной сети. Это возможно в том случае, если Интернет-провайдеры самостоятельно организуют выделенные междугородные и международные каналы для пропуска своего трафика с низкой пропускной способностью в целях экономии средств.

Таким образом, при создании сети передачи данных с узлами IPoP все соответствующие сетевые средства провайдеров сети Интернет целесообразно включить в нее, что позволит белорусским Интернет-провайдерам с минимальными затратами обеспечивать для своих пользователей качественный доступ как зарубежным, так и к белорусским ресурсам сети Интернет. Однако такое решение предъявляет повышенные требования к пропускной способности магистральных и международных участков сети передачи данных с узлами IPoP.

При подключение поставщиков услуг Интернет к наложенной сети доступа с узлами IPoP могут иметь место следующие варианты:

1. традиционное подключение по выделенным линиям или цифровым каналам в пограничный маршрутизатор;
2. оптовая продажа портов поставщикам услуг Интернет.

Во втором случае возможны следующие варианты:

- аутентификация, биллинг и обработка трафика выполняются каждым узлом IPoP
- аутентификация и биллинг выполняются каждым узлом IPoP самостоятельно, а узлы по обработке исходящих данных унифицированы.

3.2.5.1 Аутентификация, биллинг и обработка трафика выполняются каждым узлом ISP

Преимущества данного варианта в том, что не требуется никакой дополнительной модификации существующего оборудования поставщиков услуг Интернет (рисунок 42).

Недостатки – сложность сети, большие инвестиции, сложное управление и плохая масштабируемость. Для решения обозначенных проблем производители оборудования передачи данных разработали свои решения.

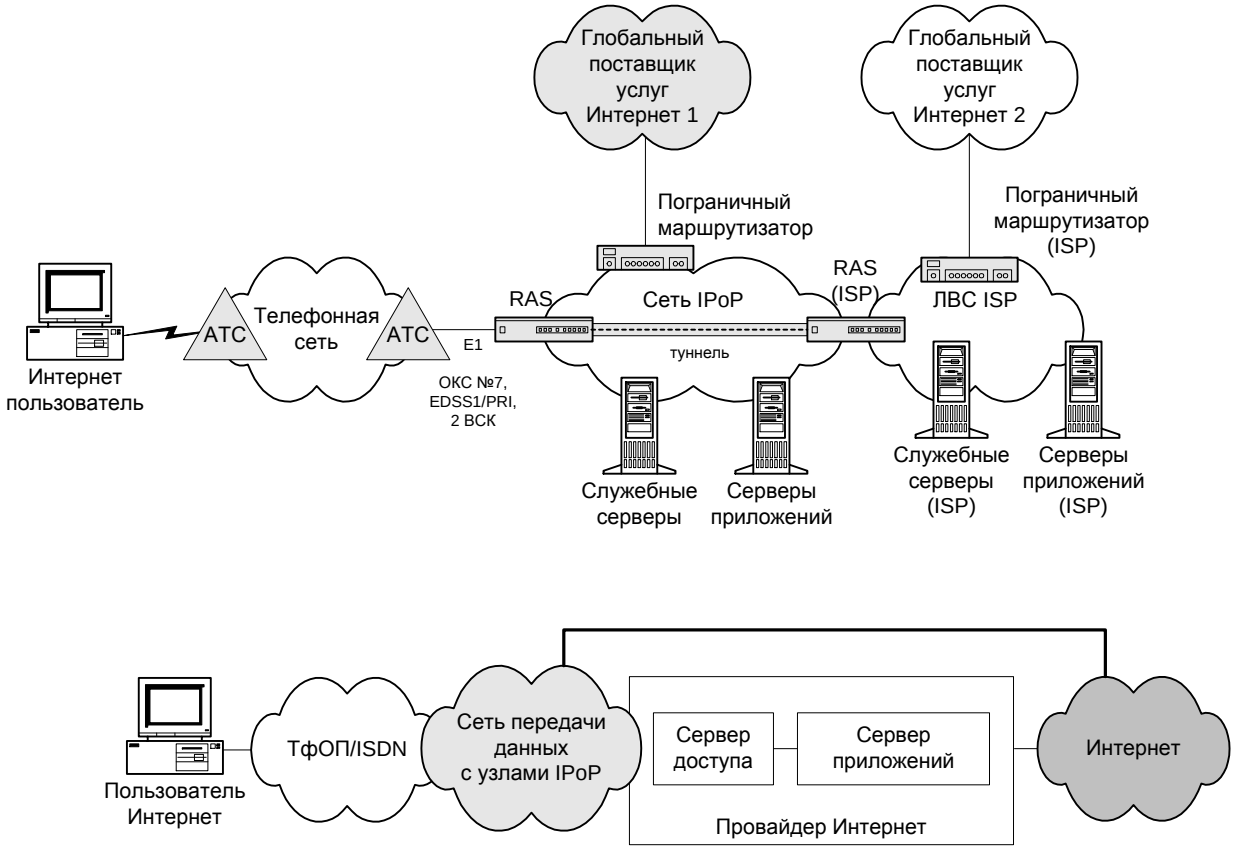


Рисунок 42 Аутентификация, биллинг и обработка трафика выполняются каждым узлом ISP

Для реализации такого способа подключения ISP может использоваться строительство виртуальной частной сети (Virtual Private Network, VPN). При таком подходе звонок удаленного Интернет-пользователя попадает в сеть передачи данных с узлами IPoP. Затем посредством протоколов туннелирования между сервером доступа узла IPoP и сервером доступа узла ISP устанавливается туннель второго уровня, который обеспечивает передачу трафика без маршрутизации (на третьем уровне). VPN может быть легко внедрена, и при ее использовании ресурсы IP-адресов будут находиться в ведении самих ISP (что поможет избежать конфликта между владельцем платформы доступа и ISP по поводу

управления ресурсами). Однако необходимо иметь в виду, что подсистемы VPN сервера доступа и узлов ISP должны выполнять инкапсуляцию и деинкапсуляцию для каждого пакета пользовательских данных.

Организация туннелей в сети IPoP может быть реализовано с помощью протоколов туннелирования PPTP, L2F, L2TP (приложение Г). Использование фирменных протоколов туннелирования определяется типом используемого оборудования, и в данной работе не рассматриваются.

Режимы VPN доступа обладают различными свойствами, однако, имеют и общие характеристики. В целом, при подключении Интернет-пользователей к провайдерам посредством VPN, организованной на базе сети передачи данных с узлами IPoP, присутствуют следующие этапы:

1. Пользователи дозваниваются по сети с коммутацией каналов до узла IPoP.
2. Сервер узла IPoP использует IP-адрес VPN-сервера провайдера в соответствии с дозвоночным номером ISP, специализированной учетной записью VPN, пользовательским доменным именем.
3. Сервер узла IPoP устанавливает туннельное соединение с VPN сервером провайдера. Соответствующая аутентификация туннеля может осуществляться способом, определяемым опционально.
4. Интернет-пользователи проходят PPP-аутентификацию на VPN сервере провайдера и устанавливают PPP соединение с VPN сервером провайдера (RAS провайдера).

В режиме **дозвоночного номера ISP**, каждому провайдеру ставится в соответствие уникальный дозвоночный номер. Когда клиент такого провайдера звонит по этому номеру на узел IPoP, в соответствии с этим номером устанавливается туннельное соединение с соответствующим VPN сервером провайдера. После того, как клиент проходит процедуру аутентификации на сервере провайдера, он получает доступ к его ресурсам.

Приведенный ниже пример показывает использование данного метода. Предполагается, что клиент поставщика услуг Интернет имеет учетное имя PPP “ispuser” и пароль “hello”, сервер доступа узла IPoP сконфигурирован таким образом, что телефонный номер 16333 соответствует VPN серверу ISP. Когда клиент звонит по номеру 16333 для регистрации на узле IPoP с учетным именем “ispuser” и паролем “hello”, между узлом IPoP и VPN сервером ISP устанавливается соединение, как показано на рисунке 43.

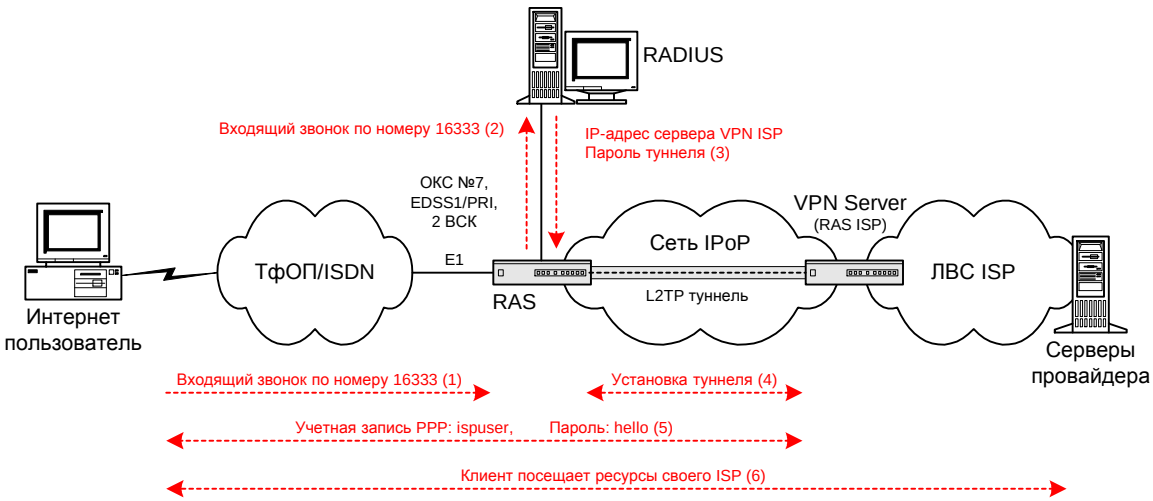


Рисунок 43 Процесс доступа по дозвоночному номеру ISP[17]

[17] Появление дозвоночного номера VPN 16333 в шагах (1) и (2) подчеркивает, что RAS узла IPoP не имеет отношения к учетной регистрации пользователя, дозвоночный номер используется для установления туннельного соединения с соответствующим VPN сервером ISP.

В режиме **специализированной учетной записи VPN**, пользователю присваивается специализированная учетная запись. Когда пользователь дозванивается до узла IPoP, сначала появляется диалоговый интерфейс. После ввода в него специализированной учетной записи, узел IPoP проведет аутентификацию пользователя в соответствии номером учетной записи, и установит туннельное соединение в соответствующим VPN сервером провайдера. PPP-аутентификация пользователя осуществляется на VPN-сервере провайдера.

Таким образом, пользователь должен сначала пройти аутентификацию на узле IPoP, прежде чем будет установлен туннель между с VPN сервером провайдера, осуществляющим PPP-аутентификацию. Этот режим позволяет избежать необходимость установки туннельного соединения между нелегальным пользователем и VPN сервером провайдера.

Ниже приведен пример использования специализированной учетной записи VPN. Предполагается, что VPN сервер провайдера содержит учетную запись PPP протокола с именем “ispuser” и паролем “hello”. Сервер узла IPoP сконфигурирован на идентификационную запись пользователя с именем “iac” и паролем “8010” в качестве специализированной учетной записи в отношении VPN сервера; в компьютере пользователя Интернет (клиента провайдера) установлены соответствующие настройки установки связи таким образом, чтобы после дозвона появлялось диалоговое окно. Когда пользователь набирает номер, например, 163, для ввода своей учетной записи “ispuser” с паролем “hello”, после дозвона на узел IPoP, появляется окно ввода информации. После ввода в него учетной записи “iac” и пароля “8010”, будет установлено виртуальное соединение с VPN-сервером провайдера, как показано на рисунке 44.

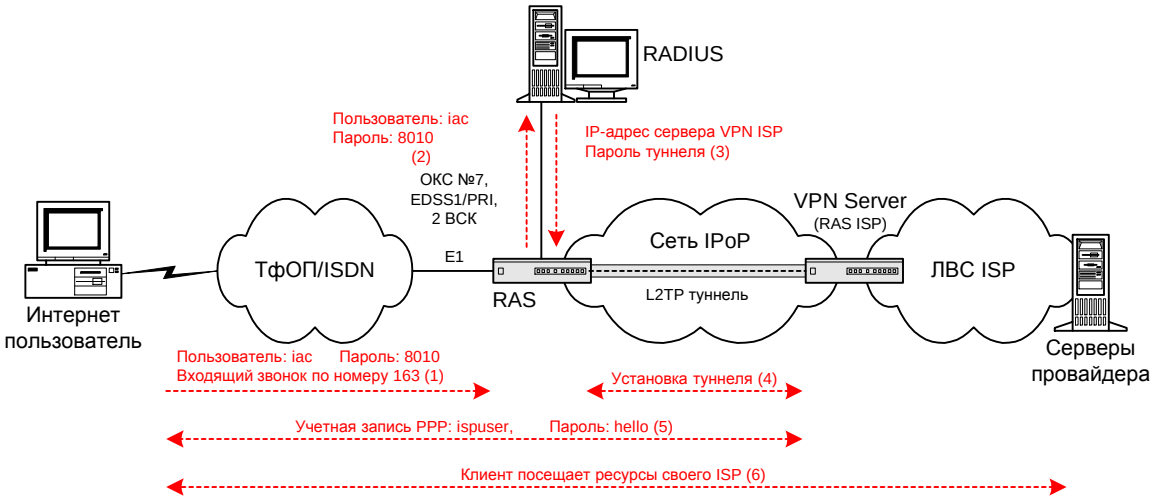


Рисунок 44 Процесс доступа по специализированной учетной записи VPN[18]

В режиме **использования доменного имени**, сервер узла IPoP устанавливает туннель с соответствующим VPN сервером провайдера в соответствии с доменным именем клиента ISP. PPP-аутентификацию пользователь проходит на VPN сервере провайдера.

Этот режим VPN доступа аналогичен доступу режима абонентского номера VPN, однако, при этом не занимается дополнительный ресурс номеров. Каждый провайдер, использующий этот режим VPN, регистрирует свое доменное имя и VPN сервер в сервере узла IPoP для выполнения приложений пользовательского доступа.

Ниже приводится пример доступа с использованием доменного имени пользователя. Предполагается, что VPN сервер провайдера содержит идентификационную PPP-запись своего клиента “ispuser@iac.com” и пароля “hello”. Сервер IPoP сконфигурирован таким образом, что доменное имя “ iac.com ” используется для доступа к соответствующему VPN

[18] Рассмотренный выше процесс содержит две идентификационных записи. Специализированная учетная запись “huawei” вводится в появляющееся диалоговое окно после дозвона до узла IPoP. Учетная запись “ispuser” представляет собой идентификационную запись для протокола PPP, и вводится на VPN сервере провайдера для доступа к его сетевым ресурсам.

серверу провайдера. Когда по коммутируемой сети звонит клиент провайдера, например, по номеру 163, они попадают на узел IPoP. После ввода учетной записи “ispuser@iac.com” и пароля “hello” будет установлено VPN соединение с сервером VPN провайдера, как показано на рисунке 45.

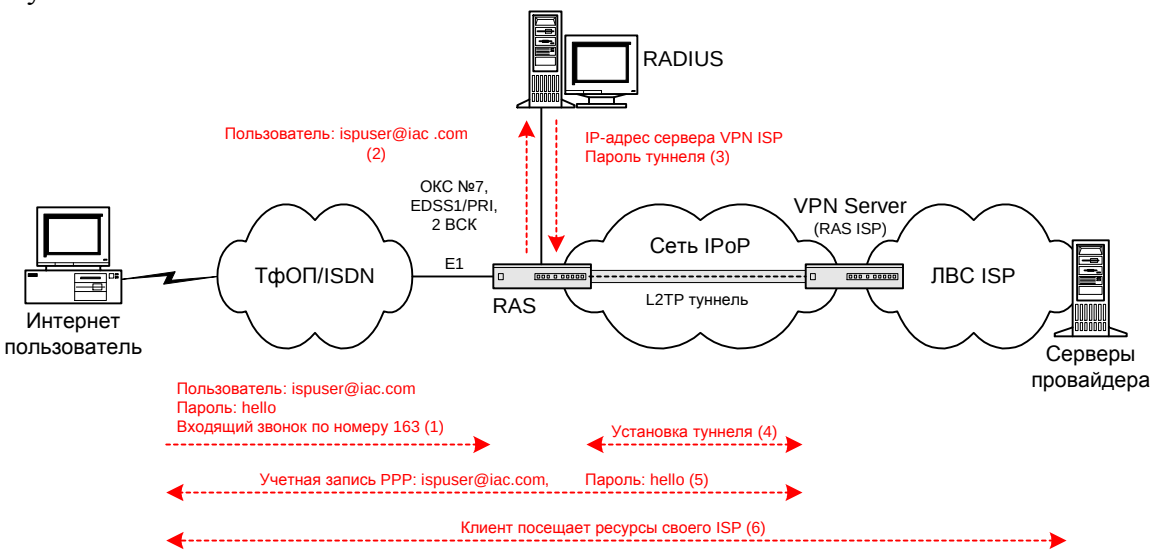


Рисунок 45 Процесс VPN доступа с использованием доменного имени

3.2.5.2 Аутентификация и биллинг выполняются каждым узлом IPoP самостоятельно, а узлы по обработке исходящих данных унифицированы

В этом случае структура сети гораздо проще (рисунок 46). IP-адреса могут выделяться сервером доступа и отсутствует необходимость в сложном управлении маршрутами между сервером доступа и узлами ISP. Развертывание этого решения позволит оптимизировать структуру сети с Интернет-провайдеров. Облегчается решение задач управления, увеличиваются возможности по развертыванию новых служб, а расширения сети не будут оказывать серьезного влияния на ее сложность.

Как видно из приведенного, оператор сети общего пользования, располагая развитой сетевой инфраструктурой, посредством строительства сети передачи данных с узлами IPoP мог бы взять на себя функции организации взаимодействия с пользователями (оптовая продажа портов). Провайдеры в этом случае могут сконцентрировать свои усилия на поддержании сети серверов приложений и развитии информационных услуг (приложение Д). Такой подход устраивает обе стороны, расширяет их рыночные возможности, и потому получил применение во многих странах.

Рассматриваемый метод подключения поставщиков услуг Интернет базируется на следующих ключевых технологиях:

- единые соединительные линии;
- аутентификация, основанная на дозвоночном номере или доменном имени пользователя;
- маршрутизация по источнику;
- ISP центр.

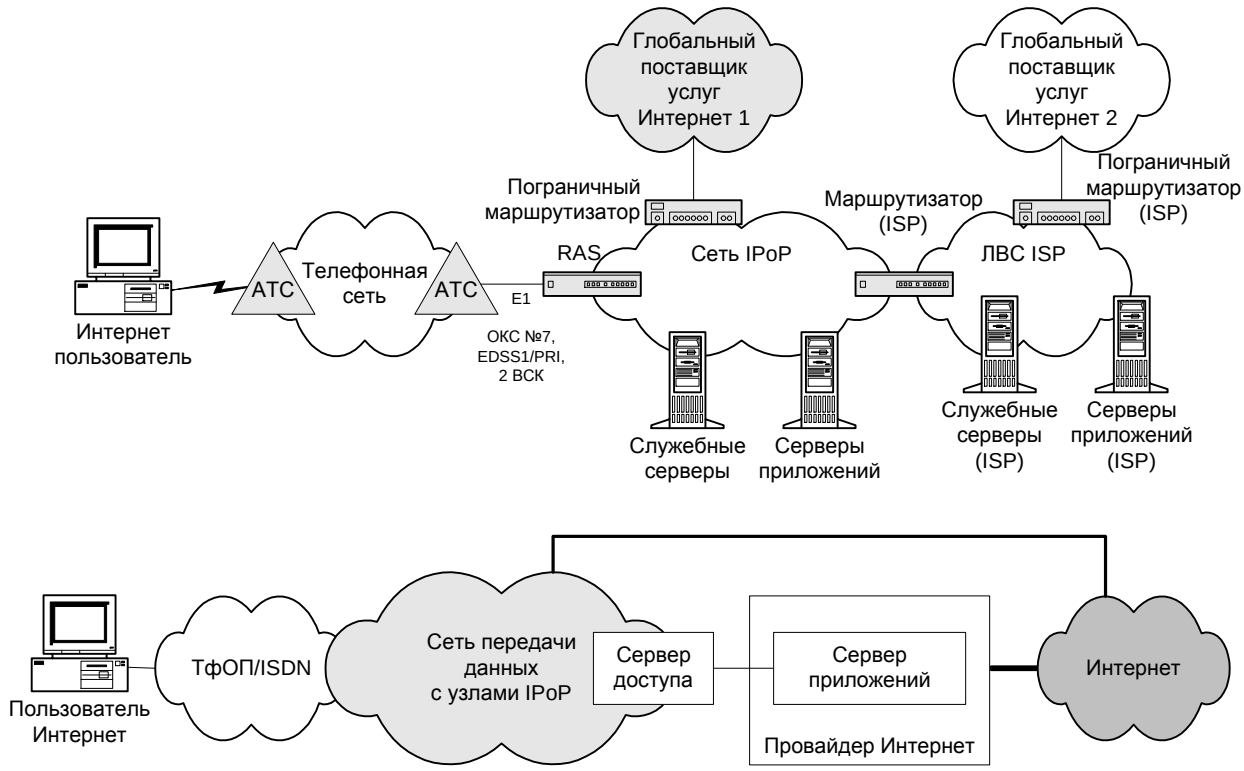


Рисунок 46 Аутентификация и биллинг выполняются каждым узлом IPoP самостоятельно, а узлы по обработке исходящих данных унифицированы

Единые соединительные линии. Сервер доступа узла IPoP может выделить фиксированное количество портов каналов связи. Например, он может выделить 50 портов соединительных линий доступа для ISP_1 и 30 портов соединительных линий доступа для ISP_2. Современные серверы доступа обладают возможностью унифицированного управления портами соединительных линий и соединяются с сетью общего пользования посредством цифровых соединительных линий ИКМ с интерфейсом E1. Эти соединительные линии не различаются по номерам доступа, и каналы подключаются к различным портам. Таким образом, существующие ресурсы соединительных линий используются полностью. Чтобы улучшить их эксплуатацию, сервер доступа узла IPoP может предоставлять уровни приоритета, верхние и нижние пределы для различных кодов доступа, которые значительно улучшают динамическое распределение ресурсов соединительных линий при подключении множества ISP. Например, ISP устанавливает 169 номеров доступа для учтенных пользователей и 96330 номеров доступа для пользователей, не имеющих учетной записи пользователя или пароля и имеющих привилегии гостя. Если имеется в наличии 240 портов доступа, и приоритет доступа отдается зарегистрированным пользователям, ISP может установить 180 портов в качестве минимального количества для 169 зарегистрированных пользователей, 30 портов для 96330 пользователей, и оставшиеся 30 портов разделить между 169 и 96330 пользователями. Таким образом, 169 пользователей распределены максимум на 210 портов и минимум на 180, в то время как 96330 пользователей будут иметь минимум 30 портов и максимум 60.

Для поддержки функции разделения портов, на сервере RAS узла IPoP может быть использована концепция «группы». Каждая «группа» обладает собственными реквизитами данных, включая групповую таблицу дозвоночных номеров, таблицу маршрутизации от источника, таблицу псевдоадресов и таблицу данных сервера RADIUS. RAS обращает внимание только на группы и дозвоночные номера, вместо индивидуальной обработки провайдерами. Каждая группа обладает системой AAA[19], и может иметь один или более

[19] Система AAA (Authentication, Authorization, Accounting) – система аутентификации, авторизации и учета.

номеров дозвона. ISP может использовать различные дозвоночные номера, которые также могут быть в той же группе или других группах. Если дозвоночные номера находятся в различных группах, будут использоваться различные системы аутентификации AAA (рисунок 47).

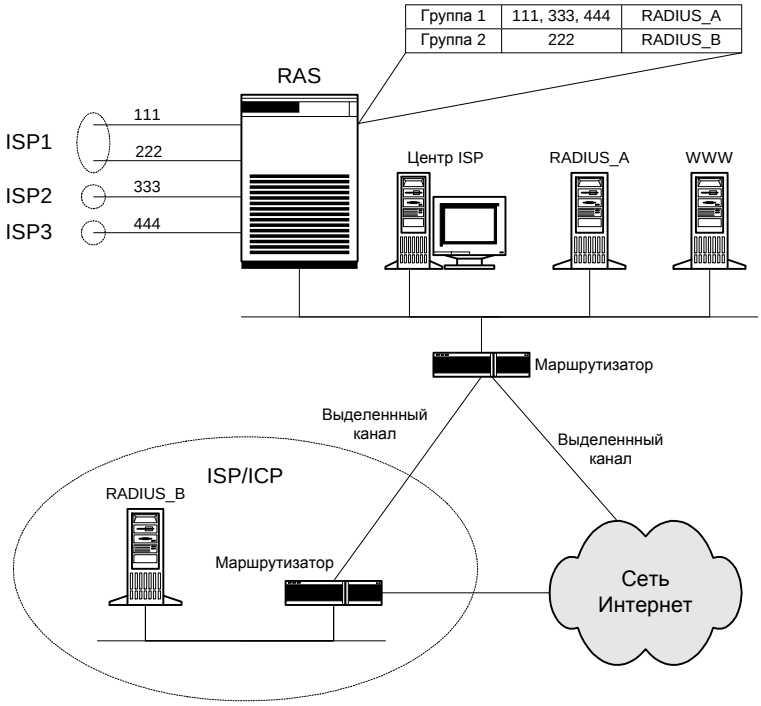


Рисунок 47 Пояснение технологии единых соединительных линий

Поясним вышеизложенное на следующем примере. Предположим, что RAS содержит две группы, группу 1 и группу 2, также как четыре дозвоночных номера, «111», «222», «333», «444». Номера «111», «333», «444» принадлежат группе 1 и используют систему аутентификации и учета RADIUS_A. Номер «222» принадлежит группе 2 и использует систему аутентификации и учета RADIUS_B. За ISP1 закреплены номера «111» и «222», которые находятся в различных группах, таким образом, ISP1 будет использовать две системы аутентификации и учета – RADIUS_A и RADIUS_B. ISP2 использует дозвоночный номер «333» и ISP3 – «444». Так как номера «333» и «444» принадлежат одной и той же группе, ISP2 и ISP3 будут разделять систему аутентификации и учета RADIUS_A.

Группирование полностью отвечает требования провайдеров, в которых дозвоночные номера, серверы аутентификации и учета и IP пулы различных групп независимы друг от друга. Такой подход гарантирует независимость каждой группы в аутентификации, учете, обеспечении безопасности и распределении адресов при использовании единой платформы доступа.

Аутентификация, основанная на дозвоночном номере и доменном имени пользователя. Сервер RAS узла IPoP обращается с ISP1 и ISP2 как к двум независимым группам изменяет для них существующие установки групп, включая IP-адрес сервера RADIUS каждой группы. Когда RAS получает вызов, он анализирует вызываемый номер (дозвоночный номер) и ищет информацию по группе согласно дозвоночному номеру. После получения IP адреса сервера RADIUS группы, RAS передаст запрос на аутентификацию этому серверу RADIUS для завершения процесса аутентификации (рисунок 48).

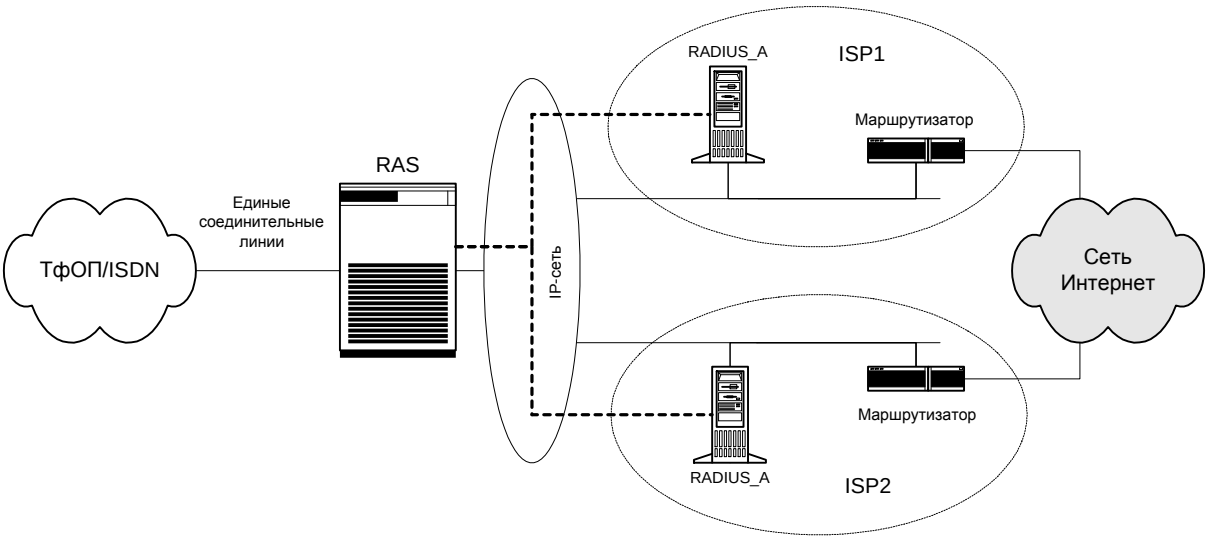


Рисунок 48 Аутентификация по дозвоночному номеру или пользовательскому имени на сервере RADIUS

Поддержку сервером удаленного доступа узла IPoP аутентификации по дозвоночному номеру поясняется на следующем примере. Пусть дозвоночным номером ISP1 будет номер «111», а ISP2 – «222». Звонки по номерам «111» и «222» могут приниматься сервером RAS узла IPoP по одному и тому же интерфейсу E1. RAS будет анализировать дозвоночный номер и посылать запросы на аутентификацию серверу RADIUS_A провайдера ISP1 или RADIUS_A провайдера ISP2 согласно различным дозвоночным номерам.

Поддержка сервером удаленного доступа узла IPoP аутентификации по доменному имени пользователя идентична аутентификации по дозвоночному номеру. Предположим, что пользователи ISP1 и ISP2 используют “xxx@111.net” и “xxx@222.net” соответственно в качестве своих адресных имен. RAS узла IPoP анализирует суффиксы пользовательских имен для получения соответствующей информации по группе и IP адресу сервера RADIUS для аутентификации.

Маршрутизация по источнику. Сервер RAS узла IPoP передает пользовательские данные присоединенному маршрутизатору, который в конечном итоге маршрутизирует данные в пункт назначения. Для использования независимого учета для каждого ISP, RAS должен продвигать пользовательские данные определенного ISP таким образом, чтобы Интернет-соединение было организовано через порт данного ISP. Для обеспечения этой функции, RAS может использовать технологию маршрутизации по источнику.

RAS узла IPoP может поддерживать два режима маршрутизации: маршрутизацию по назначению и маршрутизацию по источнику. Маршрутизация по назначению заключается в выборе следующего хопа[20] пакета пользовательских данных в соответствии с адресом назначения пакета. Такая маршрутизация основывается на таблице маршрутизации пунктов назначения. Маршрутизация по источнику определяет следующий хоп и передает пакет пользовательских данных в соответствии с адресом источника пакета. В этом случае маршрутизация основывается на таблице маршрутизации источников.

После прохождения аутентификации пользователь получает IP адрес, который может быть назначен:

- сервером RADIUS;
- Центром ISP;
- сервером доступа – RAS запрашивает соответствующий пул адресов по дозвоночному номеру пользователя и назначает свободный IP адрес пользователю (различные дозвоночные номера соответствуют различным пулам IP адресов).

[20] Хоп – транзитная передача между сетями, переход к следующему промежуточному маршрутизатору.

RAS использует режим маршрутизации по источнику для маршрутизации пользовательских данных определенному ISP согласно IP адресу, назначенному пользователю. После соответствующего управления и регистрации со стороны провайдера, пользовательская информация достигнет Интернет через порт, предоставляемый ISP.

Центр ISP. Провайдеры общей платформы доступа динамически делят ресурсы техническое обеспечение и порты оборудования. Так как нет взаимосвязи между портами и IP адресами, IP адреса клиентов ISP назначаются динамически. Центр управления ISP назначает IP адреса в пределах всей сети. Он контролирует порты, арендованные провайдерами. ISP могут запросить временное занятие портов в центре управления ISP через Web-броузер. Центр управления ISP также предоставляет пользовательскую статистику и статистику по сервисным функциям сети.

В целом, процесс входа пользователя в систему состоит из следующих этапов:

1. Клиент провайдера звонит по дозвоночному номеру, после установления соединения вводит имя пользователя и пароль.
2. Сервер удаленного доступа узла IPoP анализирует дозвоночный номер и ищет таблицу группы согласно дозвоночному номеру для того, чтобы получить IP адрес соответствующего сервера RADIUS. Затем он передает информацию аутентификации серверу RADIUS.
3. Сервер RADIUS аутентифицирует имя пользователя и пароль.
4. В случае успешной аутентификации пользователь может получить IP адрес от сервера RADIUS, центра ISP или в зависимости от конфигурации сервера удаленного доступа узла IPoP.
5. Сервер удаленного доступа запрашивает таблицу маршрутизации согласно IP адреса пользователя для маршрутизации данных к следующему маршрутизатору.
6. Пользователь работает в сети Интернет.

Приложение А. Решения оптовой продажи портов

Основными компоненты решения оптовой продажи портов являются (рисунок А.1):

- серверы удаленного доступа в конфигурации с высокой плотностью портов;
- средства аутентификации и биллинга с высокой гибкостью, надежностью и производительностью;
- средства управления услугами с возможностью управления на уровне услуг и устройств.

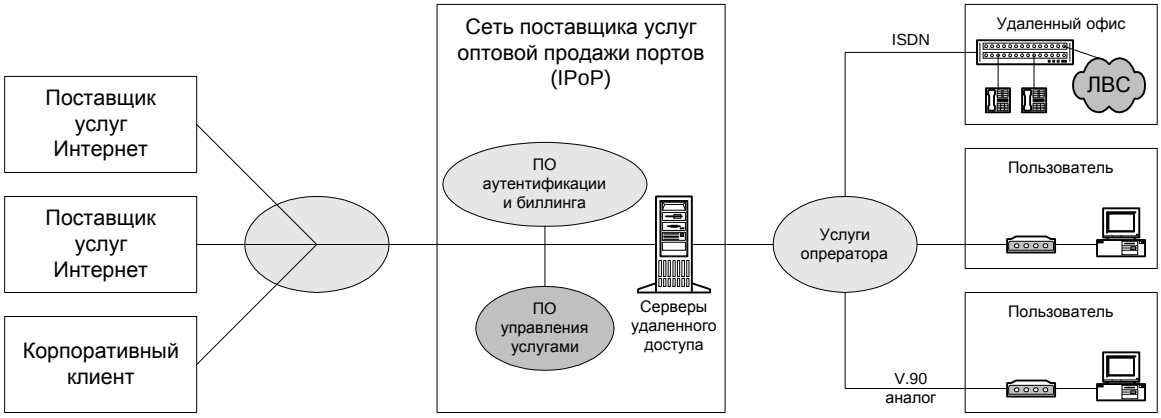


Рисунок А.1 Основные компоненты решения оптовой продажи портов

Поставщик услуг оптовой продажи портов может распределять порты серверов удаленного доступа между поставщиками услуг Интернет (ISP) и корпоративными клиентами в соответствии с потребностями. Обычно пользователь входит в IP сеть через ISP или корпоративную ЛВС, получая доступ через серверы удаленного доступа. Для аутентификации пользователей используется соответствующее программное обеспечение. При входе пользователя в сеть сервер удаленного доступа посылает запрос к серверу аутентификации и биллинга. Затем сервер может отказать в доступе или же направить пользователя к соответствующему ISP или в корпоративную VPN с соответствующими параметрами обслуживания. Управление всем решением оптовой продажи портов осуществляется при помощи средств программного обеспечения управления услугами, которое позволяет получать в реальном времени отчеты для проверки выполнения соглашений об уровне обслуживания.

Приложение Б. Сигнализация поддержки услуг мультимедиа в сетях IP

Для обеспечения функций сигнализации в IP-телефонии существуют два основных стандарта: семейство протоколов H.323, разработанное МСЭ, и протокол SIP (Session initiation protocol), разработанный IETF.

Протоколы семейства H.323 и SIP представляют различные подходы к решению одних и тех же задач. Если первые близки к традиционным системам сигнализации, то второй реализует подход на основе протокола HTTP (Hyper text transfer protocol). В рекомендации H.323 описано большое количество различных вариантов прохождения соединений, что с большой вероятностью гарантирует совместимость разных систем. Протокол SIP с сообщениями, базирующимися на текстовом формате, проще реализации и с точки зрения добавления новых функций. Систему объектов H.323 можно рассматривать как прикладную сеть, наложенную на сеть передачи данных (IP-сеть), тогда как услуги SIP ориентированы на интеграцию с услугами Интернет. Технология H.323 предоставляет больше возможностей управления конкретной услугой связи, как в части аутентификации, так и в части контроля использования сетевых ресурсов.

ТЕХНОЛОГИЯ H.323

Рекомендация МСЭ H.323 определяет основы передачи данных в сетях с коммутацией пакетов, протоколы и процедуры мультимедийной связи, в том числе, и в IP-сетях. В ней описаны компоненты сети и даны комментарии к применению других рекомендаций, в частности H.225 и H.245, а также протоколов, разработанных IETF. Рекомендация H.323 определяет четыре компонента системы:

1. диспетчер шлюзов или привратник (GK – Gatekeeper);
2. шлюз (GW– Gateway);
3. блок управления конференциями (MCU – Multipoint Control Unit);
4. H.323-терминал.

Диспетчер (GK) служит для остальных компонентов управляющим устройством. В его функции входит преобразование адресов плана нумерации телефонных сетей по рекомендации МСЭ E.164 в IP-адреса, управление доступом к сети и обеспечение защиты, управление полосой пропускания, управление связью и маршрутизация.

Шлюз (GW) обеспечивает взаимодействие с другими сетями, в первую очередь, с телефонной сетью, преобразуя способы передачи сигналов, используемые в сетях коммутации каналов, в транспортный протокол RTP (Real time transport protocol) для передачи информации по IP-сети, а также выполняет часть функций управления полосой пропускания.

Блок управления конференциями (MCU) необходим для организации многосторонней связи трех и более конечных точек, соответствующих требованиям рекомендации H.323, например, персональных компьютеров.

H.323-терминал – это конечная точка сети, ориентированная на двунаправленное соединение в реальном времени с другим H.323-терминалом, шлюзом или блоком управления конференциями. Это соединение служит для передачи между двумя точками информации управления и пользовательской информации различных видов – речи, движущихся изображений и/или данных.

В сетях IP-телефонии между вызывающей и вызываемой сторонами существует информационная связь двух типов: двунаправленный поток пользовательских данных и обмен сигнальными сообщениями для управления соединением и характеристиками потока пользовательских данных.

Процедура организации связи между конечными точками проходит в три этапа:

1. регистрация конечной точки и управление доступом;
2. маршрутизация в сети и установление соединения между конечными точками;
3. согласование параметров передачи информации между конечными точками.

После того как соединение установлено, и параметры согласованы, передача мультимедийной информации осуществляются по протоколу RTP.

Поток данных пользователя организован в виде двух отдельных RTP-сеансов, по одному для каждого направления передачи, причем для мультимедийного трафика разных типов используются разные логические каналы RTP. Рекомендуется использовать разные логические каналы и для потоков однотипной информации, если разные потоки одного типа предъявляют разные требования к качеству обслуживания.

В рекомендации H.225, входящей в семейство H.323, описаны механизмы сигнализации, необходимые для регистрации, контроля доступа и индикации состояния (RAS – Registration, admission control and status), для управления связью (на основе протокола Q.931 DSS1) и передачи трафика. В рекомендации H.245 определены типы сигнальных сообщений, которые передаются между конечными точками, и процедуры согласования параметров.

ПРОТОКОЛ SIP (IETF)

SIP – это протокол прикладного уровня, который позволяет организовать и провести сеанс многосторонней мультимедийной связи, обеспечивая его создание, модификацию и завершение. Протокол работает по схеме клиент-сервер, в которой клиент запрашивает сервис определенного типа, а сервер обрабатывает его запрос и обеспечивает предоставление этого сервиса. Согласно протоколу SIP, пользовательская система может не только создавать, но и принимать запросы. Следовательно, она должна иметь и клиентскую, и серверную часть.

Обслуживание вызовов осуществляется сервером SIP, который может работать в режиме непосредственного установления связи или в режиме переадресации. В обоих режимах сервер принимает запрос сведений о местоположении нужного пользователя, но если в первом режиме он сам доводит вызов до адресата, то во втором – возвращает адрес конечного пункта запрашивающему клиенту.

Протоколом SIP определены два типа сигнальных сообщении – запрос и ответ, которые имеют текстовый формат и базируются на протоколе HTTP. В запросе указываются процедуры, вызываемые для выполнения требуемых операций, а в ответе – результаты их выполнения. SIP использует адресацию, основанную на унифицированном указателе ресурсов URL, в котором может быть записано имя домена или IP-адрес.

Предназначенный для инициирования сеансов, протокол SIP, кроме определения адреса пользователя и установления соединения с ним, служит также базой для применения других протоколов, реализующих функции защиты, аутентификации, описания характеристик канала мультимедийной связи и начисления платы.

Приложение В. Характеристики мультисервисных платформ

Характеристика	Alcatel		Cisco	Lucent	Nortel Networks	
	A5424 Softswitch (release 1)	A1000 Softswitch (release 2)	Cisco VSC3000	Lucent SoftSwitch	Succession 2000	Succession 3000
Платформа	Compaq Alpha Server: DS10, DS20, ES39	Compact PCI	Sun Netra t 1100/105, t 1120/1125, t 1400/1405, Solaris 2.6	Sun Netra t 1400, Netra T1	DMS-MMP	Sun Ultra 4500/ Sun Solaris
Число вызовов в ЧНН (BHCA)	до 2 млн.	1,5-4,9 млн.	500 тыс.	2 млн. на одну стойку	6 млн.	150 тыс.
Поддержка IP/ATM	есть/есть	есть/есть	есть/есть	есть/есть	есть/есть	есть/есть
Сигнализации						
– *ОКС №7*	*есть*	*Есть*	*есть*	*есть*	*ETSI ISUP V.2*	*ETSI ISUP V.2*
– *ISDN/CAS*	*с 2002 г.*	*с 2002 г.*	*есть*	*есть*	*EDSS1, V5.2*	*EDSS1*
– *H.323*	*версия 3*	*планируется*	*версия 2*	*версии 1 и 2*	*нет*	*версия 2*
– *SIP*	*RFC2543 bis*	*планируется*	*есть*	*есть*	*есть*	*нет*
– *MGCP*	*версия 1*	*планируется*	*есть*	*есть*	*есть*	*есть*
– *H.248*	*версия 1*	*версия 1*	*планируется*	*есть*	*есть*	*есть*
Управление	Осуществляется с A5735 NMC, поддержка SNMP	Осуществляется с Alcatel 1300 CMC, поддержка SNMP/Q2	SNMP, Telnet/MML. Система управления – Cisco MGC Node Manager	SNMP, Telnet, выделенная рабочая станция	SNMP, Telnet, специализированный протокол	SNMP, Telnet
Поддержка RADIUS	есть	планируется	нет	есть	есть	есть

Приложение Г. Туннелирование в сети с узлами IPoP

При туннелировании пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или того же уровня. Механизм туннелирования можно представить как результат работы протоколов трех типов:

- протокола-пассажира (в нашем случае это протокол PPP);
- несущего протокола (нашем случае это протокол IP);
- протокола туннелирования (PPTP, L2F, L2TP).

Процедура помещения пакетов протокола-пассажира в поле данных пакетов несущего протокола составляет суть протокола туннелирования. Пакеты протокола-пассажира никак не обрабатываются при транспортировке их по транзитной сети (сети IPoP). Туннелирование обычно выполняет пограничное устройство (маршрутизатор или шлюз), которое располагается на границе между исходной и транзитной сетями, но этой работой может заниматься и узел-отправитель. Извлечение пакетов-пассажиров из несущих пакетов выполняет второе пограничное устройство, которое находится на границе между транзитной сетью и сетью-назначением, либо узел-получатель.

Протоколы PPTP, L2F и L2TP объединяет то, что они представляют собой протоколы туннелирования канального уровня (PPP), которые инкапсулируют кадры канального протокола в протокол сетевого уровня (IP, IPX или DECnet). С помощью последнего данные затем передаются по составной сети.

Хотя все три протокола часто относят к протоколам образования защищенного канала, строго говоря, этому определению соответствует только PPTP, обеспечивающий как туннелирование, так шифрование данных. Протоколы L2F и L2TP являются только протоколами туннелирования, а функции защиты данных (шифрование, аутентификация, целостность) в них не поддерживаются. Предполагается, что при их применении защита туннелируемых данных будет выполняться с помощью некоторого третьего протокола, например, IPSec.

ПРОТОКОЛ PPTP

Протокол PPTP (Point-to-Point-Tunneling Protocol) разработан компанией Microsoft совместно с компаниями Ascend Communications, 3Com/Primary Access, ECI-Telematics и US Robotics. Этот протокол был представлен в рабочую группу “PPP Extentions” IETF в качестве претендента на стандартный протокол создания защищенного канала, однако в качестве стандарта так и не был утвержден. Это было связано с тем, что компания Cisco Systems примерно в то же время представила IETF свой протокол L2F (Layer 2 Forwarding), поэтому было решено не отдавать предпочтение ни одному из этих протоколов, а создать некий объединенный вариант, который получил название L2TP (Layer 2 Tunneling Protocol).

Несмотря на отсутствие статуса стандарта Интернет, протокол PPTP получил практическое распространение, в основном, благодаря усилиям компании Microsoft, реализовавшей его в своих операционных системах Windows NT.

Протокол PPTP позволяет создавать защищенные каналы для обмена данными по различным протоколам – IP, IPX или NetBEUI. Данные этих протоколов, поступающие в глобальную сеть (сеть IPoP) упакованными в кадры PPP, инкапсулируются затем с помощью протокола PPTP в пакеты протокола IP, с помощью которого переносятся в зашифрованном виде через любую сеть TCP/IP (сеть IPoP). Принимающий узел извлекает из пакетов IP кадры PPP, а затем обрабатывает их стандартным способом, то есть извлекает из кадра PPP исходный пакет IP, IPX или NetBEUI и отправляет его по локальной сети.

В протокол PPTP определено две схемы его применения. Рассмотрим их применительно к сети IPoP, через которую Интернет-пользователь получает доступ в сеть ISP.

Первая схема рассчитана на то, что протокол PPTP поддерживается сервером удаленного доступа узла IPoP и сервером удаленного доступа (пограничным маршрутизатором) сети ISP.

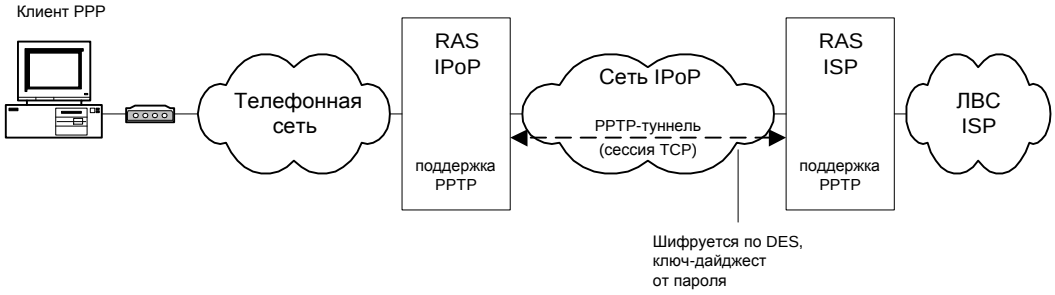


Рисунок Г.1 Защищенный канал «узел IPoP – маршрутизатор ISP» на основе протокола PPTP

Защищенный канал образуется между RAS IPoP и пограничным маршрутизатором ISP (рисунок Г.1). Это варианта защищенного канала типа «шлюз-шлюз», поэтому компьютер удаленного пользователя не должен поддерживать протокол PPTP. Пользователь связывается с сервером удаленного доступа RAS, установленного на узле IPoP, с помощью стандартного протокола PPP, и проходит аутентификацию на данном узле IPoP. По имени пользователя RAS IPoP должен найти в базе учетных данных пользователей IP-адрес пограничного маршрутизатора ISP данного пользователя, поддерживающего протокол PPTP. С этим маршрутизатором RAS IPoP устанавливает сессию через наложенную сеть передачи данных уже по протоколу PPTP. Протокол PPTP определяет некоторое количество служебных сообщений, которыми обмениваются взаимодействующие стороны, причем служебные сообщения передаются по протоколу TCP. RAS IPoP передает пограничному маршрутизатору ISP идентификатор пользователя, по которому маршрутизатор аутентифицирует пользователя по протоколам PAP или CHAP, стандартным протоколам аутентификации протокола PPP. Если пользователь прошел вторичную аутентификацию (она для него прозрачна), то RAS IPoP посылает ему сообщение об этом по протоколу PPP и пользователь начинает отправлять данные в RAS IPoP по протоколу IP, упаковывая их в кадры PPP. RAS IPoP осуществляет инкапсуляцию кадров PPP в пакеты IP, указывая в качестве адреса назначения адрес пограничного маршрутизатора, а в качестве адреса источника – свой собственный IP-адрес. Пакеты PPP шифруются с помощью симметричного секретного ключа, в качестве которого используется дайджест от пароля пользователя, хранящийся в базе учетных данных RAS IPoP для аутентификации по протоколу CHAP. В качестве алгоритмов шифрации используются алгоритмы RC-4 или DES.

Внутренние серверы ЛВС ISP также не должны поддерживать протокол PPTP, так как пограничный маршрутизатор извлекает кадры PPP из пакетов IP и посылает их по сети в необходимом формате – IP.

Эта схема не нашла широкого применения, поскольку протокол PPTP далеко не всегда поддерживается маршрутизаторами и серверами удаленного доступа провайдеров Интернет. Поэтому компания Microsoft предложила также и другую схему использования протокола PPTP, которая не требует поддержки протокола PPTP сервером удаленного доступа узла IPoP. Защищенный канал во второй схеме образуется между пользователем сети Интернет и пограничным маршрутизатором ISP, который, как и в первой схеме, должен поддерживать PPTP. В качестве такого маршрутизатора сегодня может выступать программный маршрутизатор Windows NT 4.0 с установленной службой RAS (без службы RAS протокол PPTP работать не будет), либо другой маршрутизатор с поддержкой PPTP. Если пограничный маршрутизатор ISP не поддерживает PPTP, то туннель может быть

организован между удаленным клиентом и любым внутренним компьютером сети ISP, на котором работает служба RAS и протокол PPTP.

Эта схема приведена на рисунке Г.2. Интернет-пользователь дважды устанавливает удаленное соединение с помощью утилиты Dial-Up Networking, представляющей собой клиентскую часть сервиса удаленного доступа RAS Windows NT.

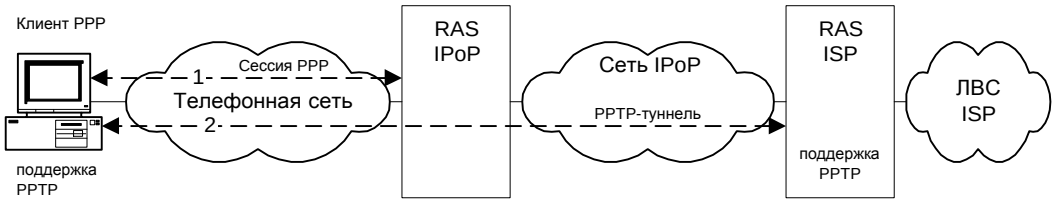


Рисунок Г.2. Защищенный канал «пользователь – маршрутизатор ISP» на основе протокола PPTP

В первый раз он звонит на сервер RAS IPoP и устанавливает с ним связь по протоколу PPP, проходя аутентификацию одним из способов, поддерживаемых узлом IPoP – по протоколам PAP, CHAP или с помощью терминального диалога.

После аутентификации на узле IPoP, пользователь вторично «звонит», на этот раз, на компьютер ISP, где работает PPTP (на рисунке Г.2 этот компьютер выполняет роль пограничного маршрутизатора ISP). Этот «звонок» отличается от обычного тем, что вместо телефонного номера указывается IP-адрес RAS, подключенного к сети IPoP со стороны ISP. При этом устанавливается сессия по протоколу PPTP между клиентским компьютером и компьютером ISP. Клиент еще раз аутентифицируется, теперь уже на сервере RAS ISP, а затем начинается передача данных, как и в первом варианте.

ПРОТОКОЛЫ L2F И L2TP

Протоколы L2F и L2TP выполняют только туннелирование без шифрования данных. Так как протокол L2F, предложенный компанией Cisco Systems, сегодня фактически поглощен протоколом IETF L2TP, имеющим статус проекта стандарта Internet, то далее будут рассматриваться только основные свойства L2TP.

Протокол L2TP обладает следующими свойствами.

- Он прозрачен для конечных систем: ни удаленной конечной системе, ни серверу ISP не требуется дополнительное специальное программное обеспечение, чтобы пользоваться этим сервисом.
- Аутентификация обеспечивается с помощью PPP CHAP/PAP или посредством другого диалога, например текстового обмена, перед стартом сессии PPP. Могут также использоваться такие системы, как TACACS+, RADIUS, токены доступа и одноразовые пароли. Аутентификация выполняется в сети ISP независимо от узла IPoP.
- Адресация конечного узла осуществляется по той же схеме, что и при прямом звонке на сервер удаленного доступа ISP. Адрес назначается не владельцем сети IPoP, а из сети ISP.
- Авторизация, как и при прямом звонке, также управляется из сети ISP.
- Учет выполняется как оператором IPoP (в целях оплаты), так и пользователем (в целях аудита и возврата оплаты).

Протокол L2TP предполагает использование схемы, в которой туннель образуется между сервером удаленного доступа узла IPoP и маршрутизатором сети ISP. В терминах L2TP сервер удаленного доступа узла IPoP, оснащенный протоколом L2TP, называется концентратором доступа LAC (L2TP Access Concentrator), а маршрутизатор ISP, поддерживающий L2TP – сетевым сервером LNS (L2TP Network Server).

LAC является устройством, подключенным к коммутируемой сети и обеспечивает возможность функционирования системы PPP терминалов и обработки протокола L2TP. Как правило, LAC представляет собой NAS и предоставляет пользователям сервисы доступа к сети через ТфОП/ISDN. LNS представляет собой программное обеспечение, обрабатывающее L2TP протоколы со стороны сервера. Существует два типа соединений между LNS и LAC:

- туннельное соединение, которое определяет пару LNS и LAC;
- сеансовое соединение, которое мультиплексируется в туннеле для представления каждой PPP сессии, переносимой по туннелю.

Обслуживание L2TP соединений и передача PPP-данных осуществляется посредством коммутации сообщений L2TP, которые переносятся стеком через UDP порт 1701 из стека TCP/IP. L2TP сообщения содержат управляющие и информационные сообщения. Управляющее сообщение используется для установки и обслуживания туннельного и сеансового соединений. Информационные сообщения используются для передачи пользовательских пакетов данных PPP сессии.

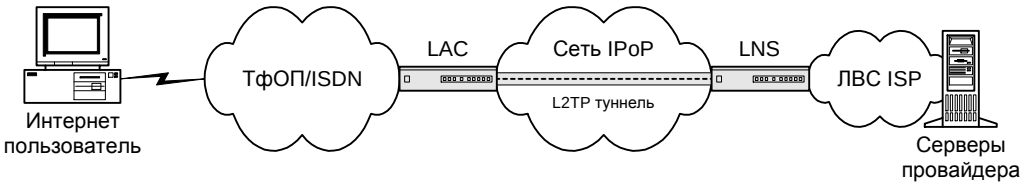


Рисунок Г.3 VPN сервис, созданный посредством L2TP

Удаленный пользователь инициирует PPP-соединение с узлом IPoP через ТфОП или ISDN (рисунок Г.3). Концентратор LAC принимает соединение и устанавливает канал PPP. Протокол L2TP позволяет концентратору свериться с LNS после приема уведомления о звонке, но до приема этого звонка – такая техника полезна в том случае, когда уведомление о звонке содержит информацию о номере вызывающей стороны.

После этого узел IPoP выполняет частичную аутентификацию конечного узла и его пользователя. Для этого используется только имя пользователя, с помощью которого узел IPoP решает, нужен ли пользователю сервис туннелирования L2TP. Если такой сервис нужен, то следующим шагом для LAC будет выяснение адреса сетевого сервера LNS, с которым нужно установить туннельное соединение. Желательно, чтобы имя пользователя указывалось в структурированном виде, например, user@company.com. Это дает возможность простого определения имени сетевого сервера LNS, обслуживающего сеть пользователя, к которой он должен получить доступ. Другим способом определения соответствия между пользователем и его сервером LNS может быть база данных, поддерживаемая оператором IPoP для своих клиентов. Кроме того, оператор IPoP может определить LNS по номеру вызывающего сервис пользователя, если его предоставит телефонная сеть.

После выяснения адреса сервера LNS проверяется, не существует ли уже туннель L2TP с этим сервером, и если нет, то он устанавливается. Протокол L2TP разработан с максимально возможной степенью изоляции его от деталей транспорта публичной сети, через которую прокладывается туннель. Единственное требование, предъявляемое к транспорту, состоит в том, чтобы он поддерживал пакетный режим взаимодействия «точка-точка». Таким транспортом может быть, например, протокол UDP, постоянные виртуальные соединения frame relay, или коммутируемые виртуальные соединения X.25.

При существовании туннеля между LAC и LNS новому соединению в рамках этого туннеля присваивается идентификатор, называемый идентификатором вызова — Call ID. И LAC посылает LNS пакет с уведомлением о вызове с данным Call ID. Сервер LNS может принять вызов или отклонить его.

Уведомление о вызове может включать информацию для аутентификации пользователя LSN, которую собрал LAC в процессе общения с пользователем. В случае применения CHAP пакет уведомления включает слово-вызов, имя пользователя и его ответ. Для протокола PAP или текстового диалога эта информация состоит из имени пользователя и незашифрованного пароля. Сервер LNS может использовать эту информацию для выполнения аутентификации, чтобы не прибегать к дополнительному циклу аутентификации и не заставлять удаленного пользователя повторно вводить свои данные.

При отправке результата аутентификации сервер LNS может также передать концентратору LAC данные об адресе узла пользователя (например, о его IP-адресе), которые LAC передаст по протоколу PPP этому узлу. В сущности, концентратор LAC работает как посредник между узлом удаленного пользователя и сервером LNS сети ISP. Выделение адреса для удаленного узла из пула адресов сети ISP позволяет избежать многих неудобств, с которыми удаленный пользователь сталкивается при получении адреса из пула узла IPoP. В последнем случае пользователь часто не может получить доступ к ресурсам сети ISP, так как они защищены межсетевым экраном или фильтрующим маршрутизатором, настроенными на пропуск внутрь сети только пакетов со «своими» адресами. Кроме того, сервер LNS может снабдить удаленный узел IP-адресами из частных диапазонов – главное, чтобы эти адреса имели корректное значение для сети ISP, а при передаче через сеть IPoP они не используются.

После приема вызова сервер LNS создает «виртуальный интерфейс» PPP в том же стиле, что и при поддержании обычного PPP-соединения. Теперь по туннелю между LAC и LNS инкапсулированные кадры PPP могут передаваться в обоих направлениях. При поступлении кадра PPP от удаленного пользователя LAC удаляет из него байты обрамления кадра, байты контрольной суммы, инкапсулирует его с помощью L2TP в сетевой протокол и отправляет по туннелю серверу LNS. Сервер LNS после извлечения из прибывшего пакета с помощью протокола L2TP кадра PPP обрабатывает его стандартным образом.

Так как протокол L2TP может работать поверх любого транспорта с коммутацией пакетов, то в общем случае этот транспорт (например, UDP) не обеспечивает гарантированной доставки пакетов. Поэтому протокол L2TP самостоятельно занимается этими вопросами за счет процедуры установления соединения внутри туннеля для каждого удаленного пользователя, а также для нумерации передаваемых пакетов по каждому соединению и восстановления потерянных и искаженных пакетов.

Приложение Д. Виртуальные провайдеры

С развитием Интернет и увеличением количества Интернет-пользователей, появляется все большее количество ISP. Однако сетевая структура малых и средних ISP не удовлетворяет все возрастающим требованиям высокопроизводительного пользовательского доступа, в силу высоких расходов на строительство; сложности в выборе приемлемой производительности, текущем планировании, расходе линий и блокировании; сложности унифицированного управления, гарантирования безопасности сети и единого учета. В настоящее время крупные ISP склоняются к предоставлению оборудования и каналов для сервисной системы доступа, в то время как средние и малые ISP тяготеют к работе в качестве ICP (Internet Content Provider – поставщики контента Интернет). Небольшие ISP/ICP для своей работы могут приобретать только маршрутизаторы, серверы, программное обеспечение приложений и выделенные каналы к крупным провайдерам. Следуя таким путем, средние и малые ISP могут значительно снизить свои инвестиции. Они могут гибким образом арендовать линии в соответствии с текущим спросом, большей частью фокусируясь на предоставлении сервисов Интернет.

Сохраняя независимые системы авторизации, аутентификации и учета, средние и малые ISP/ICP могут делить ресурсы портовой емкости и пропускной способности в рамках одной платформы доступа, обслуживаемой крупными ISP, вместо того, чтобы иметь свои собственные сетевые ресурсы. В этом случае, эти ISP/ICP становятся так называемыми виртуальными ISP, как показано на рисунке Д.1.

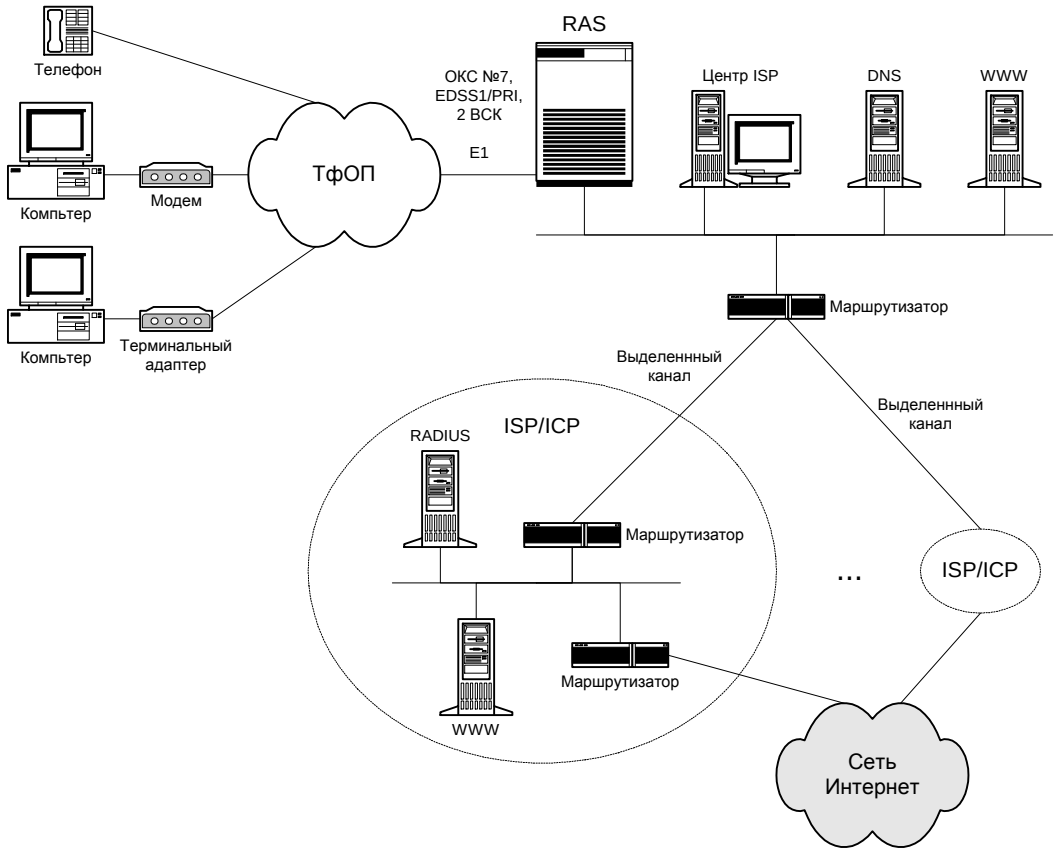


Рисунок Д.1 Сеть виртуальных ISP

Источники информации

1. Общие технические требования к цифровым городским АТС.
2. Общие технические требования к цифровым сельским АТС.
3. Технические спецификации взаимодействия с системами сигнализации национальной сети Республики Беларусь, включая специфические национальные процедуры и сообщения.
4. Технические спецификации на подсистему пользователя (ISUP) для национальной сети Республики Беларусь.
5. Technical Manual Quidway Expert Multiservice Access Switch.
6. **Гольдштейн Б.С.** Сигнализация в сетях связи. Том 1. – М.: Радио и связь, 1998.
7. **Гольдштейн Б.**С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. – М.: Радио и связь, 2000.
8. **Олифер В.Г. Олифер Н.А.** Новые технологии и оборудование IP-сетей. – СПб: БХВ – Санкт-Петербург, 2000.
9. **Олифер В.Г. Олифер Н.А.** Компьютерные сети. Принципы, технологии, протоколы. – СПб: Питер, 2001.
10. **Уолрэнд Д.** Телекоммуникационные и компьютерные сети. Вводный курс. Москва: Постмаркет, 2001.
11. Предложение по построению узла предоставления Интернет-услуг на основе оборудования Lucent Technologies. Lucent Technologies, Inc.
12. **Барсков А.Г.** Softswitch – мягкая посадка в сети нового поколения // Сети и системы связи, №9(73) 15 сентября 2001.
13. **Гильченок Л.З., Кучерявый А.Е.** АТС с комбинированной системой коммутации // Вестник связи, №11’1999.
14. **Голышко А.В.** Интеграция сетей: интеграл от неизвестной функции // Технологии и средства связи, №1’2000.
15. **Голышко А.В., Цыбаков В.И. Ершов В.А.** Метод расчета емкости модемного пула Интернет-провайдера // Вестник связи №8’2001.
16. **Гольдштейн Б.С.** О развитии коммутационной техники связи // Вестник связи, №7’2001.
17. **Гольдштейн Б.С., Рерле Р.Д.** Направления эволюции концепции IN // Вестник связи, №7’2000.
18. **Денисьева О.М., Мирошников Д.Г.** Средства связи для «Последней мили», Эко-Трендз – НТЦ Натекс, 1998.
19. **Доу Даюн.** Новая платформа Интернет-доступа – взаимовыгодное сотрудничество операторов и сервис-провайдеров // Сети и системы связи, №11(75) 22 октября 2001.
20. **Жарков, Кучерявый.** Система общеканальной сигнализации №7 // Вестник связи №1’1997, №4’1997.
21. **Иванов А.Б.** Универсальная платформа FlexGain – концепция построения первичной сети // Электросвязь, №4, 2000.
22. **Иванова Т.И.** Протоколы H.323 и ОКС №7 – фундамент сетей проекта TIPHON // Технологии и средства связи №4’2000
23. **Кучерявый А.Е.** Некоторые аспекты конвергенции сетей ТфОП/ЦСИС и IP // Вестник связи, №4’2000.
24. **Кучерявый А.Е.** Новые технологии телекоммуникаций на сетях связи Российской Федерации // Вестник связи, №4’2000.
25. **Кучерявый А.Е., Гильченок Л.З., Иванов А.Ю., Ревелова З.Б.** Перспективные решения по разделению трафика сети связи общего пользования и Интернет // Электросвязь, №5’2000.

26. **Кучерявый А.Е., Нестеренко В.Д., Парамонов А.И.** Стратегия развития сетей связи на основе новых технологий // Электросвязь, №1’ 2001.
27. **Кюртин П., Уайт Б.** Платформа Tigris – шлюз между сетями с коммутацией каналов и IP-сетями // Электросвязь, №3, 2000.
28. **Кюртин П., Уайт Б.** Платформа Tigris – шлюз между сетями с коммутацией каналов и IP-сетями // Электросвязь, №4, 2000.
29. **Мардер Н.С., Аджемов А.С.** Развитие российской сети ОКС №7 – основа современных услуг связи // Сети и системы связи №9’1997.
30. **Пинчук А.В., Суховицкий А.Л.** Модуль IPU как средство интеграции АТСЦ-90 с IP-сетями // Электросвязь, №5’2001.
31. **Пинчук А.В., Фрейнкман В.А.** Интернет и ТфОП: вопросы подключения маршрутизаторов к городским АТС // Сети и системы связи, №10(32) 1998.
32. **Подпрыгалов Михаил.** Концепция развития мультисервисных сетей связи // Технологии и средства связи №1’2000
33. **Рамнат А. Лакшми-Ротан.** Когда конвергенция становится реальностью // Электросвязь, №5’2001.
34. **Ревелова З.Б., Копытко О.И.** Влияние трафика Internet на телефонную сеть // Вестник связи, №4’1999.
35. **Салосин М.Б., Белов С.А., Лувишис Л.А.** Услуги мультисервисных сетей – стратегия повышения доходности операторов электросвязи // Вестник связи №7’2000, №8’2000.
36. **Самуйлов К., Галентовская М.** Введение в систему сигнализации №7 // Сети май-июнь’99, август-сентябрь’99
37. **Сахаров Михаил.** EWSD InterNode: бизнес становится выгодным // Технологии и средства связи, №1’2000.
38. **Серебрянников А.В., Тулинов В.С.** Доступ в Internet: выбор оборудования // Вестник связи, №4’1999.
39. **Фрейнкман В.А.** Узел услуг на базе интеллектуальной платформы «ПРОТЕЙ» // Электросвязь, №5’2001.
40. **Царева А.В.** Новые перспективы развития мультисервисной сети // Вестник связи, №8’2001
41. **Шаронин С.** Новые решения: Интернет в каждую квартиру // Информ-курьер связь, №10’2000.
42. **Шварцман В.О.** Многофункциональные сети мегаполисов // Век качества, №1’2001.
43. **Шнепс-Шнеппе М.А.** Интеллектуальная сеть – Интернет: оптимистические новости из Ватутинок и Дубно // Информ-курьер связь, №11’2001
44. http://www.alcatel.ru.
45. http://www.ericsson.ru.
46. http://www.lucent.ru.
47. http://novell.ru.
48. http://www.ptti.gov.ru.
49. http://www.uniis.kiev.ua.
50. http://www.xdsl.ru.