УДК 004.738

ОРГАНИЗАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ ТРАФИКОМ И РАСЧЕТА ТЕЛЕКОММУНИКАЦИОННЫХ УСЛУГ В РАСПРЕДЕЛЕННОЙ СЕТИ ОПЕРАТОРА СВЯЗИ

В. В. Кузьмин, аспирант Нижегородского государственного технического университета (НГТУ) им. Р. Е. Алекесеева; vvk1987@yandex.ru
А. В. Семашко, доцент НГТУ им. Р. Е. Алекесеева, к.т.н.
Ю. В. Белова, инженер-конструктор II категории ЗАО «НПП «Салют-25», к.т.н.

***Ключевые слова**: распределенная сеть, телематические услуги, биллинговая система, маршрутизатор, узел агрегации, архитектура клиент-сервер.*

Введение. Стремительное развитие мультимедийных услуг (Интернет, кабельное телевидение, телевидение по запросу, телефония и др.) способствует переходу качества обслуживания (QoS) абонентов на новый уровень. В настоящее время в России услуги доступа в сеть Интернет, интерактивного кабельного телевидения, телефонии все больше проникают в удаленные районы. Первоначально центры развития телематических услуг находились в крупных населенных пунктах — городах и мегаполисах с многомиллионным населением.

Уровни QoS в центре какой-либо области и на ее окраинах всего несколько лет назад разделяла целая пропасть. Пока в городе строились мультисервисные оптоволоконные сети со скоростями доступа порядка гигабит, QoS в удаленных районах оставляло желать лучшего. Нередко единственной возможностью доступа к услугам Интернета оставался беспроводной доступ через мобильного оператора связи (2G, 3G), при этом скорость доступа не превышала несколько мегабит. Альтернативным вариантом доступа в сеть Интернет в таких районах могла быть ADSL-технология: телематические услуги оказывались по телефонной линии, построенной много лет назад. Качество услуг, оказываемых по таким каналам связи, было несколько лучше, чем по беспроводной сети.

Старые проводные сети связи находятся в удручающем состоянии, и, как следствие, по ним не могут предоставляться стабильные и надежные телематические услуги. Более того, такие сети не удовлетворяют требованиям, предъявляемым к современным каналам передачи данных. Они не являются мультисервисными (нет возможности передавать различные типы трафика — Интернет, телефония, интерактивное телевидение), а максимальная скорость передачи информации не превышает нескольких мегабит, что, в свою очередь, не может обеспечить абоненту приемлемое QoS [1]. С ростом числа всевозможных сервисов и услуг в сети Интернет, к параметрам канала связи предъявляются определенные требования (задержка, скорость передачи, процент потери пакетов). Старая проводная сеть не гарантирует работу таких приложений, и принципы управления трафиком в подобных случаях будут кардинально отличаться от их современных аналогов.

Особенности организации телематических услуг в распределенных сетях связи. Развитие периферийных районов мегаполисов и необходимость оказывать услуги Интернет приводят к тому, что один оператор обслуживает несколько географически разнесенных на значительные расстояния кампусных сетей. Возникает потребность управлять услугами (блокировать и разрешать доступ, списывать средства с лицевых счетов и т.д.) в распределенной сети из центра (например, центрального офиса). В данной статье понятие распределенная сеть является ключевым, в отличие от локальных кампусных сетей с единым центром агрегации. В такой сети отсутствует единый центр обработки трафика. Рост популярности телематических услуг заставляет операторов заново продумывать способы организации мультисервисных услуг в новых условиях [1].

В крупных компаниях решение этой задачи сводится к построению физических каналов связи между подсетями. Объединение их в общую инфраструктуру позволяет организовать единый центр управления трафиком. Обычно в таких центрах устанавливается дорогостоящее оборудование, предназначенное для маршрутизации трафика всех узлов сети [2].

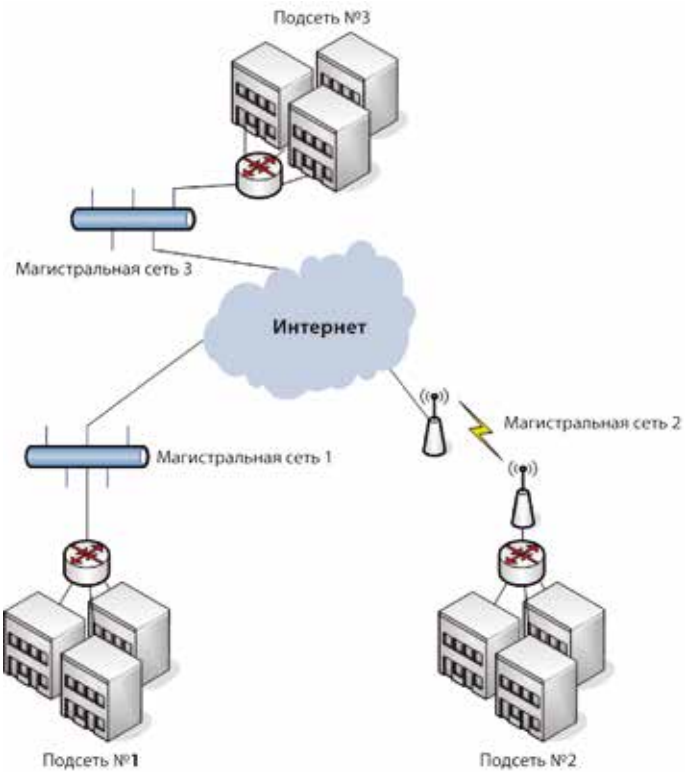

Рис. 1

В удаленных от крупных центров районах доступ к мультисервисным услугам (в первую очередь к Интернету) осуществляется по принципу суб-провайдинга, когда компанией-оператором организуется сетевая инфраструктура только в пределах данного населенного пункта: строится междомовая сеть, разводится кабель внутри подъездов и т.д. Общий канал связи, по которому организуется коллективный доступ к телематическим услугам принадлежит компании, предоставляющей магистральный канал связи. Причем в географически разнесенных районах области, компания-провайдер в большинстве случаев пользуется услугами разных магистральных операторов. В районах области, где поблизости не проходят какие-либо магистральные каналы, используется беспроводной доступ (по радиоканалу) (рис. 1).

Компании-операторы, строящие мультисервисные сети в городе, также сталкиваются с проблемой объединения нескольких разнесенных подсетей (например, в разных микрорайонах города) в единую. В большинстве случаях строятся выделенные высокоскоростные каналы связи, соединяющих подсети. Для надежной устойчивой связи при повреждении основного канала параллельно вводят резервные каналы связи. Объединение сетей необходимо для управления трафиком всех абонентов из единого центра — например, в головном офисе компании, где установлено высокопроизводительное дорогостоящее оборудование.

Решение объединить несколько подсетей находит применения и у компаний, не связанных с предоставлением телекоммуникационных услуг. Такая задача часто связана с соединением разнесенных офисов в одну логическую инфраструктуру. Причем в большинстве случаев подобные решения реализуются с помощью технологии виртуальных частных сетей (Virtual Private Network –VPN), поддерживающей одно или несколько сетевых соединений (логическая сеть) поверх другой сети (например, Интернет) с созданием защищенного соединения [3]. Безопасность передачи данных обеспечивается благодаря использованию математических и программных средств (шифрование, аутентификация, защита от повторов и изменений передаваемых по логической сети сообщений). Технология VPN предусматривает прозрачный доступ к ресурсам сети и инкапсулирует IP-трафик после создания соединения (VPN-туннеля) к удаленному узлу [3].

Актуальность организации управления трафиком в распределенных сетях связи. В случае логического объединения разнесенных подсетей, необходимо организовывать общие каналы доступа таким образом, чтобы их пропускная способность отвечала всем требованиям, предъявляемых абонентами к качеству связи в сети.

Объединение подсетей не всегда физически реализуемо или финансово целесообразно, особенно для небольших телекоммуникационных компаний. Если провайдер предоставляет услуги коллективного доступа к телематическим услугам в территориально удаленных друг от друга районах, то объединение в единую сеть практически не возможно. Организация логических VPN-туннелей потребует значительных затрат, связанных с увеличением пропускной способности общих магистральных каналов связи. Поэтому в такой распределенной сети устанавливается несколько центров агрегации, находящихся на границе подсети и канала доступа магистрального оператора связи. Маршрутизация и управление абонентским трафиком осуществляется с помощью оборудования, установленного в таких точках. Таким образом, вместо единого центра обработки трафика создается несколько агрегационных несвязанных друг с другом узлов связи.

Задача управления распределенными узлами связи, особенно для небольших операторов связи с ограниченным бюджетом, усложняется и ее следует решать на начальном этапе проектирования сети. От того, каким образом будет организовано управление распределенными ресурсами, зависит успех компании на рынке услуг. На прибыль оператора связи влияет способ организации системы по расчету телематических услуг и эффективность ее работы.

Коллективный доступ к телематическим услугам в распределенной сети можно организовать одним из следующих способов: строительство объединенных высокоскоростных линий связи с единым центром управления или организация отдельных независимых друг от друга узлов агрегации в каждой подсети оператора связи. Очевидно, что каждый из них имеет недостатки. Первый метод в виду значительных финансовых затрат, практически недоступен небольшим операторам связи или не всегда целесообразен; второй — трудно масштабируется в условиях расширения сети (подсетей) и требует значительных затрат при создании и обслуживании такой инфраструктуры. Затраты могут быть не только финансовые: каждый раз при строительстве новой подсети возникает необходимость создавать отдельную базу данных и средства блокировки абонентов.

Существующие решения. Они ориентированы на небольших операторов связи или сети предприятий и уступают (по функциональным возможностям) биллинговым системам, устанавленным в узлах крупных операторов связи, например LANBilling, АСР «Гидра», UTM 6 и т.д. [4]. Зачастую, биллинговая система разрабатывается самим оператором для решения собственных задач и является интеллектуальной собственностью компании. Дорогостоящие биллинговые системы имеют модульную архитектуру. При этом самый доступный — базовый модуль (ядро будущей системы) содержит минимальный функционал. Остальные модули и решения при внедрении биллинга реализуются в соответствии с требованиями заказчика, что сказывается на конечной цене продукта, однако даже в этом случае существующие решения не всегда могут функционировать в распределенных сетях.

Решения для небольших операторов связи представлены на рынке биллинговых систем свободно распространяемыми, бесплатными и полукоммерческими программными продуктами. Однако функциональные возможности таких систем ограничены и предназначены в основном для управления телематическими услугами в кампусных сетях с единым центром и сетях крупных предприятий [5]. Биллинговая система устанавливается на маршрутизаторе и не предназначена для управления трафиком в распределенных узлах связи, поэтому администраторы вынуждены устанавливать эти системы на каждом узле распределенной сети, при этом их синхронизация в едином центре не возможна. Управление трафиком и расчет потребления телематических услуг выполняется для каждой подсети отдельно. Такой подход предполагает ведение базы абонентов подсети на каждом маршрутизаторе, что не гарантирует целостности и конфиденциальности данных, представляющих коммерческую тайну компании (при выходе из строя какого-либо узла агрегации).

Новый способ организации биллинговой системы. Рассмотрим новый подход организации системы расчета

телематических услуг и управления трафиком в распределенной сети оператора связи. Этот метод ориентирован на небольшие компании-операторы с ограниченным бюджетом, занимающиеся субпровайдингом телематических услуг. Решение было реализовано на сети действующего оператора связи. К разрабатываемой системе управления трафиком и расчета телематических услуг предъявлялся ряд требований:

- модульный принцип построения, т.е. модули работы с клиентом, администратора системы, проводки платежей, управления трафиком клиентов (блокировка, приостановка, возобновление работы услуги и т.д.);
- гибкая структура — возможность расширения с увеличением числа абонентов и распределенных подсетей;
- единая база данных (абонентская база, тарифы, услуги, проводки платежей) на выделенном сервере;
- онлайн платежи (внесенная абонентом сумма в терминале немедленно зачисляется на его лицевой счет и предоставление услуги возобновляется). Система должна поддерживать механизмы восстановления (в случае если какой-либо из узлов временно вышел из строя или потерял связь с выделенным сервером с установленной на нем базой данных);
- функции программных компонент управления трафиком на узловых маршрутизаторах не могут заменяться. Система является только надстройкой, управляющим слоем для работы программных модулей (шейперов).

Рассматриваемое решение внедрено на сети действующего оператора связи и полностью отвечает всем требованиям, выдвинутым заказчиком на этапе проектирования системы.

Ниже описан принцип организации такой системы с точки зрения различных пользователей (администратор, клиент, бухгалтер, инженер технической поддержки), показана диаграмма взаимодействия (рис. 2), а также представлена программная архитектура биллинговой системы и структурная схема ее работы в сети оператора связи.

Рис. 2

Каждый пользователь системы имеет свой интерфейс доступа с соответствующими правами. Как видно из диаграммы, клиент может заходить только в свой личный кабинет для просмотра сведений о состоянии лицевого счета, отправлять заявку на смену тарифа, просматривать движение денежных средств, задавать вопрос по работе телематических услуг. При этом, получив заявку, отправленную из личного кабинета клиента, система переадресует ее администратору (через кабинет администратора), или в сервисную службу (кабинет сервисного инженера). Администратор системы обладает наибольшими привилегиями, и имеет доступ, как в кабинет сервисного инженера, так и бухгалтера. Такой подход выбран с учетом особенностей использования биллинга небольшими операторами связи, когда функции бухгалтера, инженера поддержки и администратора может выполнять один человек. Бухгалтер системы работает с приходящими средствами от платежных систем и с помощью кабинета бухгалтера следит за проводками денежных средств, проходящих через биллинговую систему.

Программную реализацию биллинга можно разделить на несколько частей — модулей, каждый из которых выполняет определенную функцию в системе. Модульный принцип организации системы управления трафика и расчета телематических услуг представлен на рис. 3.

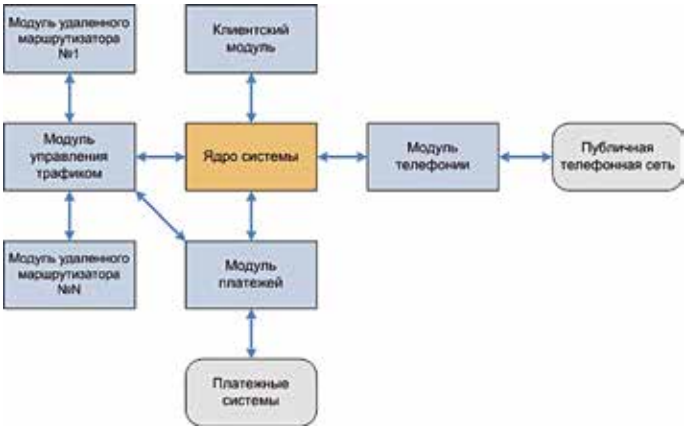

Рис. 3

Ядро системы — реляционная база всех данных, обрабатываемых системой, и средств управления ей. Все остальные модули системы используют данные, обращаясь к ядру системы. Клиентский модуль отвечает за работу с конечным абонентом и представляет собой программную реализацию личного кабинета с функциями смены тарифного плана, обратной связи с технической поддержкой. Модуль управления трафиком используется в системе для выполнения функций блокировки, приостановки и возобновления услуг доступа к телематическим услугам (Интернет, кабельное телевидение). При списании средств с лицевого счета абонента и возникновении отрицательного или равного нулю баланса, система автоматически заблокирует доступ к услуге через этот модуль. Причем, как видно из рис. 3, данный модуль отправляет служебные сообщения на удаленные маршрутизаторы для блокировки услуги. На рисунке изображены только два модуля удаленных маршрутизаторов, хотя их число соответствует общему числу разнесенных подсетей.

Каждый модуль удаленного маршрутизатора устанавливается непосредственно на удаленном узле связи и ожидает поступления служебных сообщений от модуля управления трафиком на выполнение приостановки — блокировка или возобновление услуги. Модуль платежей используется для работы с платежными системами (онлайн-системы) когда баланс лицевого счета пополняется автоматически (мгновенно) при оплате, например, через терминал за услугу доступа в сеть Интернет. Модуль платежей при поступлении оплаты проверяет состояние клиента и при необходимости отправляет модулю управления трафиком команду на разблокирование абонента. Модуль телефонии

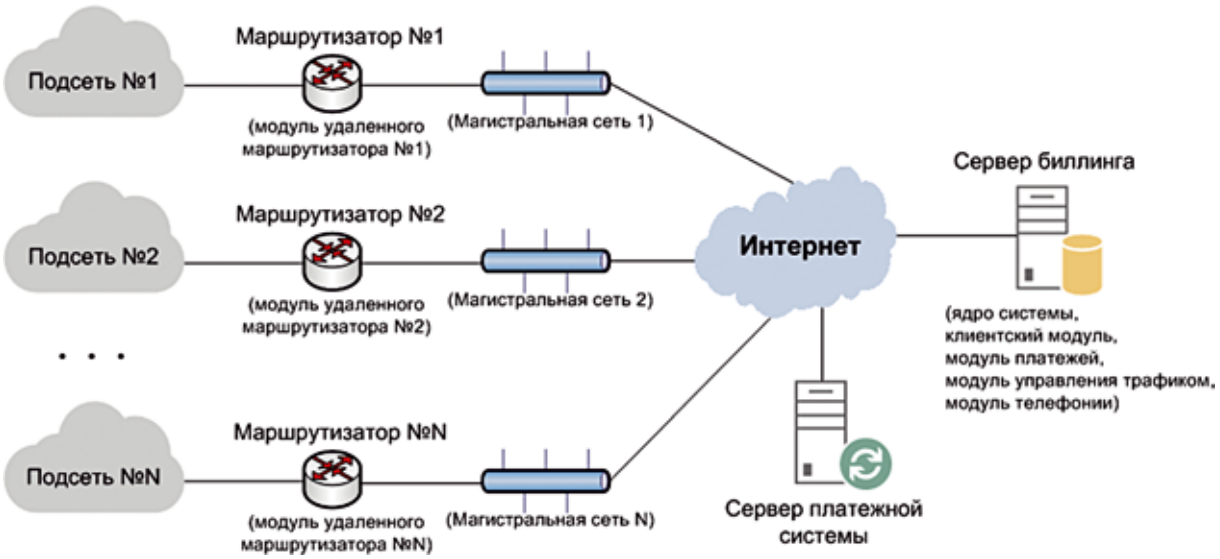

Рис. 4

представляет собой меню IVR (Interactive Voice Response) и предназначен для обработки телефонных звонков клиентов. По телефону абонент может узнать состояние своего лицевого счета, отправить заявку на ремонт [6] и т.д.

На рис. 4. изображена структурная схема сети на основе программного обеспечения реализованной системы. Модули, отвечающие за управления трафиком, устанавливаются на удаленных маршрутизаторах и биллинговом сервере и отвечают за обработку служебных сообщений о блокировке, приостановке и возобновлении действия услуг между управляющим центром (сервер биллинга) и коммутационными узлами удаленных подсетей. Сервер биллинга не выполняет трансляцию трафика абонентов всех подсетей (за это отвечают удаленные маршрутизаторы), а выполняет только контролирующую функцию доступа к таким услугам. В случае выхода из строя биллингового сервера, телематические услуги будут по прежнему доступны клиентам и это никак не скажется на их работе в сети.

Модуль управления трафиком имеет клиент-серверную архитектуру, организованную для обмена служебными сообщениями между удаленными маршрутизаторами и сервером биллинга. При этом серверной частью такой системы являются именно удаленные маршрутизаторы, которые «слушают» сеть и ожидают сообщения от биллинговой системы, так как сами маршрутизаторы не могут быть инициаторами служебного диалога. Все команды по блокировке, приостановке, возобновлению поступают именно с сервера биллинга.

Особое внимание стоит обратить на реализацию функции работы с платежными (онлайн) системами, поддерживающими мгновенное пополнение счета при выполнении денежной операции. Механизм поддержки платежных систем (модуль платежей) также реализован с помощью технологии клиент-сервер. Только в данном случае сервер биллинга играет роль сервера, поскольку инициатором соединения уже выступает сервер платежной системы, на который от удаленного платежного терминала поступает информация о выполнении финансовой проводки.

Основная отличительная особенность предлагаемого подхода — тот факт, что полезный трафик всех абонентов во всех подсетях не обрабатывается и не проходит через биллинговую систему. Это позволяет значительно сократить расходы на покупку высокопроизводительного оборудования для сервера биллинга и аренду или покупку дополнительных каналов связи для обработки трафика в едином центре.

Реализованная система предполагает, что служебная информация будет передаваться через открытые сети (Интернет), что не гарантирует защиту данных на пути их следования (рис. 4). Для этого в систему добавлен механизм защищенных соединений (служебные сообщения передаются в зашифрованном виде), структура которых также была разработана в процессе проектирования системы.

Для безопасности передаваемых служебных сообщений между удаленными маршрутизаторами, сервером биллинга и сервером платежной системы применяется протокол HTTP с поддержкой SSL (Secure Sockets Layer — уровень защищенных сокетов). HTTP выполняет только транспортную функцию передачи сообщений между двумя хостами. Шифрование данных происходит с помощью протокола SSL, (поверх HTTP). SSL — криптографический протокол, обеспечивающий безопасность в сети Интернет [7]. Он использует асимметричную криптографию (для аутентификации ключей обмена), симметричное шифрование (для сохранения конфиденциальности) и коды аутентификации сообщений (для целостности сообщений). Несколько версий протоколов широко используются в таких приложениях, как веб-браузер, электронная почта, Интернет-факс, обмен мгновенными сообщениями, передача голоса через IP и др.

При реализации зашифрованного способа передачи служебных сообщений с применением протокола SSL используется двухсторонняя аутентификация клиента и сервера в системе. Перед началом передачи сообщений клиент и сервер обмениваются сертификатами (открытыми ключами). Более подробно об этом методе аутентификации описано в [8].

На рис. 5 представлена часть листинга одного из основных скриптов, входящих в модуль управления трафиком, на сервере биллинга.

Вначале работы скрипта (строки 1—7) проверяется доступность удаленного маршрутизатора перед отправкой ему служебного сообщения. В системе реализован механизм повторной передачи сообщений. Он может понадобиться если удаленный маршрутизатор не доступен по каким-либо причинам: проблемы в канале связи, отсутствие

Рис. 5

электричества на удаленном узле и т.д. В этом случае на сервере в планировщике задач создается задание на повторную отправку сообщения через определенное время (устанавливается администратором системы в файлах конфигурации).

Код программы (строки 9—19) задает параметры будущего SSL-соединения к удаленному узлу. Здесь указываются SSL-сертификаты, ключи и URL-адрес приложения, входящего в состав серверной части модуля управления трафиком на удаленном маршрутизаторе.

При передаче служебного сообщения в системе используется POST-запрос протокола HTTP. Простейший пример запроса с сервера биллинга удаленному маршрутизатору:

```
action=ban
IP=10.10.5.5
```

В 21-й строке выполняется POST-запрос к удаленному узлу, содержащий два параметра: `action` — действие и IP-адрес удаленного компьютера клиента. Действие `ban` информирует серверную часть модуля управления трафиком на удаленном маршрутизаторе о том, что клиент с IP-адресом 10.10.5.5 должен быть заблокирован. Если требуется заблокировать сразу нескольких клиентов на удаленном маршрутизаторе, сервер биллинга отправит массив IP-адресов в POST-запросе.

Модуль управления трафиком на удаленном маршрутизаторе возвращает код завершения операции: `<err>ERROR</err>` — ошибка и `<good>OK</good>` — операция выполнена успешно. В строках 23—39 проверяется полученный результат и при ошибке в планировщике создается новая задача на повторную передачу сообщения через заданное время.

В качестве основного языка программирования созданной биллинговой системы выбран Perl, основанный на многофункциональности, кроссплатформенности и гибкости [9]. С помощью дополнительных программных модулей, поддерживаемых языком Perl, можно создавать гибкие решения для работы с базами данных, вэб-приложениями, электронной почтой, серверными сценариями и т.д. Дополнительные преимущества языка — отсутствие зависимости от коммерческих лицензий, наличие документации, бесплатная поддержка подключаемых при разработке модулей. Все это позволяет значительно снизить затраты конечного заказчика системы, при внедрении ее в инфраструктуру компании. Программные модули разработанной системы не требуют компиляции кода и могут быть установлены на все системы, поддерживаемые языком Perl. Таким образом, предлагаемое решение не требует значительных затрат, связанных с работой высококвалифицированного специалиста при внедрении и дальнейшем обслуживании системы.

Заключение. Предложенный метод позволяет значительно сократить затраты при организации доступа к телематическим услугам. В связи с тем, что сервер биллинговой системы не выполняет трансляцию трафика всех абонентов и работает только со служебными сообщениями, средства, затрачиваемые на оборудование узла агрегации, будут минимальны. Такой подход позволяет обеспечить коллективный доступ в распределенной сети связи без построения коммутирующих (объединяющих) каналов связи с организацией единого центра или без установки независимых отдельных узлов агрегации, тем самым не разбивая распределенную сеть на отдельные независимые подсети.

ЛИТЕРАТУРА

1. **Кузьмин В. В., Семашко А. В**. Методы управления трафиком в кампусных сетях оператора связи // Электросвязь.— 2012.— № 5.— С. 37—40.
2. Маршрутизаторы Cisco Systems [Электронный ресурс].— Режим доступа: http://www.cisco.com/web/RU/products/routers/index.html (дата обращения: 05.03.13).
3. VPN [Электронный ресурс].— Режим доступа: http://ru.wikipedia.org/wiki/VPN (дата обращения: 10.03.13).
4. Сравнительная таблица биллингов для интернет-операторов [Электронный ресурс].— Режим доступа: http://nag.ru/unformat/billing2.php (дата обращения: 20.03.13).
5. Биллинговые системы (billing) [Электронный ресурс].— Режим доступа: http://forum.ru-board.com/topic.cgi?forum=8&topic=1332 (дата обращения: 21.03.13).
6. **Кузьмин В. В., Семашко А. В., Белова Ю. В**. Организация управления VoIP-трафика на голосовых (IVR) платформах // Электросвязь.— 2013.— № 5.— С. 8—11.
7. SSL [Электронный ресурс].— Режим доступа: http://ru.wikipedia.org/wiki/SSL (дата обращения: 07.04.13).
8. An Introduction to Mutual SSL Authentication [Электронный ресурс].— Режим доступа: http://www.codeproject.com/Articles/326574/An-Introduction-to-Mutual-SSL-Authentication (дата обращения: 10.04.13).
9. Преимущества Perl [Электронный ресурс].— Режим доступа: http://www.brainworker.ru/article/preimushchestva-perl (дата обращения: 19.04.13).

Получено 18.07.13