

Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра сетей и устройств телекоммуникаций

В. Ю. Цветков, Ю. В. Смирнов, А. Н. Кулешевский

***БИЛЛИНГ-УПРАВЛЕНИЕ ТРАФИКОМ
МУЛЬТИСЕРВИСНОЙ СЕТИ***

МЕТОДИЧЕСКОЕ ПОСОБИЕ
по курсу

«Документальные службы и терминальные устройства телекоммуникаций»
для студентов специальности
«Сети телекоммуникаций»
всех форм обучения

Минск БГУИР 2011

УДК [654.01+654.032.94/98]:654.1(076.5)

ББК 32.88я73

Ц27

Рецензент:

доцент кафедры «Защита информации» учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»,
кандидат технических наук И. И. Черная

Цветков, В. Ю.

Ц27

Биллинг-управление трафиком мультисервисной сети : метод. пособие по курсу «Документальные службы и терминальные устройства телекоммуникаций» для студ. спец. «Сети телекоммуникаций» всех форм обуч. / В. Ю. Цветков, Ю. В. Смирнов, А. Н. Кулешевский. – Минск : БГУИР, 2011. – 50 с. : ил.

ISBN 978-985-488-579-7.

Рассмотрены принципы построения биллинговых систем и работа с типовой биллинговой системой на примере CakeBilling в учебной мультисервисной сети. Приведены описание и порядок выполнения лабораторной работы по администрированию биллинговой системы CakeBilling.

УДК [654.01+654.032.94/98]:654.1(076.5)

ББК 32.88я73

ISBN 978-985-488-579-7

© Цветков В. Ю., Смирнов Ю. В., Кулешевский А. Н., 2011

© УО «Белорусский государственный университет информатики и радиоэлектроники», 2011

Содержание

Перечень условных обозначений	4
Основные термины и определения	7
Введение	8
1. Принципы построения биллинговых систем и биллинг-управления трафиком	9
1.1. Задачи биллинговых систем	9
1.2. Структура биллинговой системы	10
1.3. Функции биллинговых систем	12
1.4. Требования к биллинговым системам	14
2. Биллинговые системы мультисервисных сетей	17
2.1. Состав серверной части биллинговой системы	17
2.2. FreeRADIUS-сервер	17
2.3. Протокол PPP	22
2.4. Служба PPTP	23
2.5. СУБД PostgreSQL	23
2.6. Комплект разработчика JDK	23
2.7. Servlet/JSP-контейнер	24
2.8. PostgreSQL JDBC-драйвер	24
3. Лабораторная работа «Администрирование биллинговой системы CakeBilling»	25
3.1. Цель работы	25
3.2. Описание лабораторной работы	25
3.3. Предварительное задание к лабораторной работе	39
3.4. Порядок выполнения и методические указания	39
3.5. Контрольные вопросы	41
Литература	42
Приложение. Порядок установки и конфигурирования операционной системы Debian 4.0-r3	43

Перечень условных обозначений

АСР	– автоматическая система расчёта
БД	– база данных
ОС	– операционная система
ПО	– программное обеспечение
AAA	– Authentication, Authorization, Accounting – протокол, разработанный для передачи сведений между программами-сервисами (NAS, Network Access Server) и системой биллинга
IAB	– Internet Architecture Board – группа технических советников ISOC, осуществляющих надзор за архитектурой Интернета (включая его протоколы и связанные с ними процедуры), созданием новых стандартов Интернета, редактирование и публикацию серии документов RFC, консультации руководства ISOC по техническим, архитектурным и процедурным вопросам, связанным с Интернетом и его технологиями
CSD	– Circuit Switched Data – технология передачи данных, разработанная для мобильных телефонов стандарта GSM
Dial-up	– коммутируемый удалённый доступ – сервис, позволяющий компьютеру подключаться к другому компьютеру (серверу доступа) с использованием модема через телефонную сеть общего пользования для передачи данных
EAP-TLS	– Extensible Authentication Protocol – Transport Layer Security – расширяемый протокол аутентификации и метод защиты транспортного уровня протокола EAP
EDGE	– Enhanced Data rates for GSM Evolution – технология мобильной связи, функционирующая поверх 2G и 2.5G (GPRS)
GRE	– Generic Routing Encapsulation – общая инкапсуляция маршрутов – протокол Cisco туннелирования сетевых пакетов
GPRS	– General Packet Radio Service – пакетная радиосвязь общего пользования – надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных
IETF	– Internet Engineering Task Force – открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров, созданное IAB в 1986 г., которое занимается развитием протоколов и архитектуры Интернета
ISOC	– Internet Society – общество Интернета – международная профессиональная организация
IP	– Internet Protocol – маршрутизируемый протокол сетевого уровня
IPsec	– IP Security – набор протоколов для обеспечения защиты данных, передаваемых по протоколу IP, позволяющий осуществлять подтверждение подлинности и/или шифрование IP-пакетов

- ISP – Internet Service Provider – Интернет-провайдер – организация, предоставляющая услуги доступа к Интернету и иные связанные с Интернетом услуги
- JDBC – Java DataBase Connectivity – соединение с базами данных на Java – платформенно-независимый промышленный стандарт взаимодействия Java-приложений с различными СУБД, реализованный в виде пакета java.sql, входящего в состав Java Standard Edition
- JDK – Java Development Kit – комплект Java-разработчика
- JRE – Java Runtime Environment – среда исполнения Java – ПО, необходимое для запуска приложений, созданных с помощью Java
- JSP – JavaServer Pages – технология, позволяющая Web-разработчикам динамически генерировать HTML, XML и другие Web-страницы
- J2EE – Java Platform To Enterprise Edition – набор спецификаций и соответствующей документации для языка Java, описывающей архитектуру серверной платформы для задач средних и крупных предприятий
- LDAP – Lightweight Directory Access Protocol – «облегченный протокол доступа к каталогам» – сетевой протокол доступа к службе каталогов X.500
- Linux – GNU/Linux – общее название UNIX-подобных операционных систем на основе открытого ядра Linux и собранных для него библиотек и системных программ, разработанных в рамках проекта GNU. Часто такие операционные системы называют просто «Linux», так как первой, наиболее популярной и единственной тогда системной библиотекой, использовавшейся в системах на базе Linux, была GNU C Library (glibc)
- MPPE – Microsoft Point-to-Point Encryption – протокол шифрования данных, используемый поверх соединений PPP. Использует алгоритм RSA RC4. Поддерживает 40-, 56- и 128-битные ключи, которые меняются в течение сессии (частота смены ключей устанавливается в процессе хэндшейка соединения PPP. Существует возможность генерировать новый ключ на каждый пакет. Часто используется совместно с Microsoft Point-to-Point Compression для сжатия данных. MPPE поддерживается не всеми маршрутизаторами и является причиной несовместимости оборудования при работе в локальных сетях
- MS-CHAP – Microsoft Challenge Handshake Authentication Protocol – протокол Microsoft для выполнения процедур проверки подлинности удаленных рабочих станций Windows
- Nix – Linux, Unix дистрибутив
- Netflow – протокол Cisco, предназначенный для сбора информации об IP-трафике внутри сети
- PPP – Point-to-Point Protocol – протокол точка-точка
- PPTP – Point-to-point tunneling protocol – туннельный протокол типа точка-точка,

- позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в незащищённой сети
- RADIUS – Remote Authentication in Dial-In User Service – протокол
- RFC – Request for Comments – запрос комментариев – документ из серии пронумерованных информационных документов Internet, содержащих технические спецификации и стандарты, широко применяемые в Internet
- RSA – криптографический алгоритм с открытым ключом
- SNMP – Simple Network Management Protocol – простой протокол управления сетью – это протокол управления сетями связи на основе архитектуры TCP/IP
- TCP/IP – Transmission Control Protocol/Internet Protocol – стек протоколов TCP/IP – собирательное название для сетевых протоколов разных уровней, используемых в сетях
- URL – Uniform Resource Locator – единый указатель ресурсов (определитель местонахождения ресурсов)
- VPN – Virtual Private Network – виртуальная частная сеть – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети
- X.500 – серия стандартов ITU-T (1993 г.) для службы распределенного каталога сети

Основные термины и определения

Биллинг (англ. billing – составление счёта) – в некоторых видах бизнеса и телекоммуникациях – автоматизированная система учёта предоставленных услуг, тарификации услуг и выставления счетов для оплаты.

Инкапсуляция – метод согласования сетей, применимый только для согласования транспортных протоколов. Инкапсуляция (тоннель) может быть использована, когда две сети с одной транспортной технологией необходимо соединить через сеть, использующую другую транспортную технологию.

Authentication – процесс, позволяющий идентифицировать субъекта по его данным, например по имени и паролю.

Authorization – процесс, определяющий полномочия идентифицированного субъекта на доступ к определенным объектам или сервисам.

Accounting – процесс, позволяющий вести учет доступа к услугам.

Open source – открытое программное обеспечение, то есть программное обеспечение с «открытым» исходным кодом. Способ разработки ПО, при котором исходный код создаваемых программ открыт (общедоступен для просмотра и изменения). Это позволяет пользователям использовать уже созданный код для своих нужд и, возможно, помочь в разработке открытой программы.

Введение

Управление трафиком является одной из важнейших задач, решаемых системой управления сетью (NMS – Network Management System). Общие принципы управления сетями телекоммуникаций изложены в рекомендациях ИТУ-Т серии 3000. Согласно этим рекомендациям управление трафиком реализуется посредством четырехуровневой системы управления, включающей уровни управления элементами сети, сетью в целом, сервисами и предприятием [1].

Одной из важных составляющих системы управления трафиком является биллинговая подсистема управления [2]. Она располагается на уровне управления услугами и обеспечивает регулирование клиентского трафика в зависимости от состояния его счета и тарифной политики. В простейшем случае биллинг-управление трафиком сводится к отказу в обслуживании клиента при обнулении его счета.

В рамках мультисервисных сетей телекоммуникаций биллинговая система (или автоматизированная система расчетов) представляет собой программный комплекс, обеспечивающий учет доступа пользователей к услугам, расчет и списание денежных средств с клиентских счетов в соответствии с применяемыми тарифными планами. Автоматизированные системы расчетов могут входить составной частью в платёжные системы. Платёжная система представляет собой совокупность процедур и связанных с ними технических средств (телекоммуникационного и компьютерного оборудования, систем передачи и каналов связи), используемых для проведения финансовых транзакций на финансовом рынке.

Телекоммуникационные операторы широко используют специализированные биллинговые системы, организованные по клиент-серверной технологии и обеспечивающие автоматическое выполнение всех операций и процедур, связанных с учётом предоставляемых клиентам услуг, тарификации услуг и выставления счетов для оплаты клиентам.

В настоящем методическом пособии изложены базовые принципы построения биллинговых систем, подробно рассмотрена биллинговая система CakeBilling и предложена для выполнения лабораторная работа, ориентированная на приобретение практических навыков по работе с биллинговой системой в мультисервисной сети.

1. Принципы построения биллинговых систем и биллинг-управления трафиком

1.1. Задачи биллинговых систем

Системы, вычисляющие стоимость услуг, предоставляемых клиентам, хранящие информацию о тарифах и прочих стоимостных характеристиках и использующиеся телекоммуникационными операторами для выставления счетов абонентам и взаиморасчетов с другими поставщиками услуг, носят название биллинговых, а цикл выполняемых операций сокращенно именуется биллингом. Существует ряд международных документов ИТУ-Т, регламентирующих основные функции биллинговых систем и способы реализации этих функций. Например, документы серий E230, E260 и E1001 посвящены техническим аспектам расчета длительности соединения, регистрации вызовов при различных типах связи и определению оплачиваемой длительности сеансов связи. Описания основных принципов тарификации услуг мобильной связи и сценариев соединений приведены в рекомендациях серий D103, D110 и D93.

Требования международных стандартов учитываются при сертификации биллинговых систем. Во всем остальном (в выборе СУБД, приложений и способов организации информационных хранилищ) разработчики биллинговых систем имеют полную свободу действий. Несмотря на множество различных СУБД и систем хранения данных, значительная часть промышленных биллинговых систем (примерно 9 из 10 продуктов) создана на основе СУБД Oracle. У большинства крупнейших операторов сотовой и проводной связи установлены биллинговые системы на базе именно этой СУБД.

Биллинговая система решает следующие задачи [3]:

- сбор информации о предоставляемых услугах – аккаунтинг;
- аутентификация и авторизация клиентов;
- контроль денежных средств на счетах клиентов и списание средств в соответствии с действующим тарифным планом;
- пополнение счетов клиентов;
- внесение изменений в тарифы;
- предоставление статистики по операциям для клиентов и оператора.

Для биллинговой системы существенны два процесса: аутентификация и авторизация. *Аутентификация* – процедура идентификации пользователя, состоящая в проверке указываемых пользователем данных на совпадение с хранящимися данными в системе. *Авторизация* – процесс принятия решения о правомерности доступа пользователя к некоторому ресурсу (например, правомерность доступа к файлу на жёстком диске или правомерность доступа к услуге).

По функциональным возможностям автоматизированные системы расчётов можно разделить на три класса: предназначенные для транснациональных операторов связи, заказные национального масштаба и системы среднего класса для региональных сетей.

Автоматизированные системы расчётов, относящиеся к первому классу, должны обеспечивать взаимодействие сетей на международном уровне, в различных временных зонах и должны быть мультивалютными и многоязыковыми.

Заказные системы национального масштаба создаются под определенного оператора. Оператору может понадобиться новая автоматизированная система расчётов, совместимая с уже существующей автоматизированной системой расчётов. Стоимость таких единичных систем значительно выше.

В масштабе региона достаточно стандартной автоматизированной системы расчётов. Такая система должна обладать гибкостью, масштабируемостью и надежностью.

1.2. Структура биллинговой системы

В мультисервисной сети биллинговая система включается между уровнем доступа и уровнем услуг для учета и управления трафиком клиента и контроля доступа к услугам (рис. 1.1).



Рис. 1.1. Место биллинговой системы в мультисервисной сети

В общем случае в состав биллинговой системы оператора входят следующие компоненты (рис. 1.2):

- коллекторы информации о потребленных услугах;
- система аутентификации абонентов;
- ядро (бизнес-логика);
- многоуровневая база данных;
- модуль авторизации;
- модуль анализа типов трафика (локальный, пиринговый и т. д.);
- модуль разграничения доступа;
- модуль статистики;
- административный интерфейс для управления клиентской информацией;
- интерфейс управления счетами клиентов и тарифными планами.

Многоуровневая база данных требуется для исключения постоянной работы с массивами максимально детальной информации. Работа с массивами максимально детальной информации может значительно снизить быстродействие биллинговой системы.



Рис. 1.2. Общая структура биллинговых систем предприятий связи

Существует три уровня базы данных:

- максимально детализированная информация без обработки;
- классифицированная и первично агрегированная информация;
- оперативная информация.

База данных первого уровня необходима для разрешения спорных вопросов с клиентами. Она должна хранить информацию в исходном виде для возможности перерасчета выставленных к оплате счетов с учетом скорректированных тарифов, например, уточненных границ сетей, по которым делится трафик. Получение детализированной информации о соединениях возможно не для каждого сервиса. Например, при подсчете трафика через Web Proxy использование NetFlows позволяет полную детализацию, но требует значительного объема памяти для хранения данных.

База данных второго уровня занимает меньший объем дискового пространства, чем база данных первого уровня, поэтому возможно хранение информации в ней за более продолжительный период времени. Например, после классификации трафика можно не хранить информацию о локальном трафике, если за него не взимается плата. С большой долей достоверности за одно соединение может учитываться несколько соединений клиента с одним и тем же узлом, произошедших приблизительно в одно время. Такая ситуация типична для многопоточных сетевых клиентов.

Третий уровень базы данных – оперативная информация. Это наименее детализированный уровень базы данных по отношению к остальным уровням, однако операции в нём совершаются быстро, что позволяет сократить время реакции автоматизированной системы расчётов. На основе базы данных третьего уровня осуществляется принятие решений о предоставлении или прекращении предоставления услуг конкретному клиенту.

Основной принцип построения биллинговой системы – это строгая модульность, позволяющая модернизировать отдельные компоненты системы

в зависимости от меняющихся бизнес-задач. Провайдер может предоставлять различные услуги (например, VPN-доступ, dial-up, обычный неинкапсулированный трафик, Proxy, VoIP). Требуется обеспечить доставку ядру системы в единообразном виде информации о том, какой тип услуги запрошен конкретным клиентом, в каком объеме и в какое время. В общем случае для каждого типа услуг необходим уникальный коллектор. При создании коллекторов используются технологии SNMP, RADIUS, NetFlow.

1.3. Функции биллинговых систем

Автоматизированная система расчётов создается и настраивается на бизнес-процесс определенного оператора, имеет собственный набор функций, соответствующий технологическому циклу предоставления услуг, и может работать с конкретным сетевым оборудованием, поставляющим информацию о предоставляемых клиентам услугах. Однако существует стандартный набор функций, поддерживаемых практически всеми автоматизированными системами расчётов. В него входят:

- операции, выполняемые на этапе предварительной обработки и анализа исходной информации, например, функция получения данных о соединениях и услугах (запросы к коммутатору);

- операции управления сетевым оборудованием: функции активации/деактивации (блокировки/разблокировки) абонентов и команды изменения условий подписки абонентов, передаваемые непосредственно в коммутатор;

- операции управления базами данных, включающие тарификацию записей коммутатора о вызовах и услугах, формирование и редактирование таблиц базы данных расчетной системы, выставление счетов и их печать, кредитный контроль счетов, составление отчетов, архивация.

При оценке системы биллинга важным критерием является число контролируемых услуг. Предоставляемый типовой набор услуг Интернет-провайдера включает:

- коммутируемый доступ;
- выделенный доступ;
- WWW/FTP-хостинг;
- почтовые услуги;
- доступ к телеконференциям.

Организация предоставления любой услуги включает авторизацию доступа к услуге, сбор различных статистических данных, непосредственную тарификацию услуги и ограничение доступа.

Автоматизированные системы расчётов позволяют контролировать доступ к телеконференциям. Однако эту услуги предоставляют немногие Интернет-провайдеры. Некоторые автоматизированные системы расчётов поддерживают сбор статистики почтового трафика. Постоянный рост почтового трафика в скором времени заставит Интернет-провайдеров пойти на тарификацию исходящего почтового трафика. Причем эта операция будет осуществляться не на

участке между клиентом-отправителем и сервером, а при отправке сообщений во внешнюю сеть. Это учитывает уже назревшую проблему «спама», связанную с несанкционированной рассылкой по множеству адресов. Само письмо может быть небольшим, поэтому для его пересылки на сервер провайдера потребуется всего несколько секунд. Однако широковещательная рассылка по «бесконечному» количеству адресов способна вызвать перегрузку серверов и каналов провайдера.

Возможности сбора и хранения статистических данных очень важны при выборе автоматизированной системы расчётов, поскольку именно от них зависит вероятность реализации того или иного тарифного плана. Организовать сбор статистики можно различными способами, в частности, с помощью механизмов RADIUS, TACACS+, SNMP.

Статистику по услугам передачи данных можно разделить на две категории: относящаяся к сессиям и трафику. Статистика о сессиях используется для тарификации услуг коммутируемого доступа. Сессия определяется как промежуток времени между установлением соединения и разъединением. Данные о трафике должны собираться отдельно для входящего и исходящего трафика и индивидуально для каждого внешнего канала к первичному провайдеру. Только в этом случае можно раздельно тарифицировать, например, национальный и международный трафик.

Статистика телематических услуг определяется на основе расчета размеров дискового пространства, занимаемого файлами и сообщениями абонента за единицу времени, и трафика, создаваемого каждой службой. Поскольку размер дискового пространства, занимаемого файлами абонента, есть функция времени, наиболее приемлемым статистическим параметром представляется интеграл этой функции по времени, а точнее – его дискретная аппроксимация. Сбор статистических сведений о трафике, создаваемом каждой телематической службой, может осуществляться аналогично услугам передачи данных.

Системы расчётов поддерживают следующие основные функции.

1. Клиентский учет, в том числе:

- ведение справочника клиентов;
- поддержка корпоративных клиентов (возможность древовидной структуры счетов для одного клиента);
- учет персональной информации и реквизитов для юридических лиц;
- различные способы оплаты (предоплата, кредит, ограниченный кредит);
- автоматическая генерация Voip и DialUp карт;
- возможность идентификации клиента по номеру телефона или адресу;
- управление счетами клиента (блокировка и разблокировка, ведение истории состояния счета).

2. Тарификация услуг, в том числе:

- ведение справочника кодов доступа (например междугородных и международных);
- ведение справочника тарифных зон провайдеров;
- ведение справочника тарифных зон трафика;

- поддержка сетей Private Network при учете трафика;
- гибкая система настройки тарифных планов;
- возможность перерасчета стоимости предоставленных услуг.

3. Расчеты с клиентами, в том числе:

- формирование счета для клиентов, работающих в кредит;
- счет-фактура с возможностью настройки печатной формы;
- ввод и учет платежей абонента;
- поддержка нескольких валют.

4. Расчеты с партнерами, в том числе:

- ведение справочника провайдеров;
- учет объема услуг, предоставленных провайдером;
- учет объема услуг, предоставленных провайдеру;
- подсчет себестоимости услуг.

5. Формирование аналитической и статистической отчетности, в том числе:

- отчет о запрашиваемых клиентом услугах за период (детализация счета);
- распределение запросов по тарифным зонам;
- распределение запросов по времени суток, дням недели, месяцам;
- распределение запросов по провайдерам;
- распределение запросов по серверам доступа (NAS);
- распределение DialUp сессий по времени суток, дням недели, месяцам;
- отчет о DialUp сессиях клиента за период;
- отчет об объеме трафика пользователя за период;
- распределение объема трафика по тарифным зонам.

6. Администрирование системы, в том числе:

- ведение справочника клиентов;
- разграничение прав пользователей в системе;
- импорт кодов доступа, платежей, VoIP и DialUp карт из текстового файла;
- экспорт любой выборки в текстовый файл или файл Microsoft Excel.

1.4. Требования к биллинговым системам

Общими техническими требованиями к биллинговым системам являются гибкость, точность расчетов и устойчивость к сбоям. Ниже представлена детализация данных требований.

1. Гибкость. В процессе использования нежелательно подвергать биллинговую систему серьезной модификации. Поэтому следует сразу заложить возможность контроля услуг, которые могут потребоваться в будущем. Как правило, биллинговые системы учитывают входящий и исходящий трафик. В перспективе может возникнуть потребность в контроле новых услуг, таких как платный контент, VoIP, веб-хостинг. Вполне вероятно, что может возникнуть необходимость работать с платежами по временным картам доступа.

2. Точность расчетов. Практика использования автоматизированных систем расчетов показывает, что учёт трафика может производиться хотя и весьма малой, но ненулевой погрешностью. При больших объемах трафика погрешности

в доли процента соответствуют значительные деньги. Чтобы застраховаться от подобных особенностей следует учитывать погрешность в тарифах.

В практике использования автоматизированных систем расчётов существует такое явление, как паразитный трафик, который невозможно исключить из учёта положительного трафика. Его необходимо учитывать, если у провайдера много реальных IP-адресов.

При перепродаже трафика следует учитывать, что головной провайдер под мегабайтом может понимать вовсе не 1 048 576 байт, а, например, 1 000 000, что в результате дает почти 5 % расхождения.

Дополнительные проблемы могут составлять направления трафика. Некоторые головные провайдеры выставляют счета за входящий трафик, некоторые – за исходящий трафик, а некоторые учитывают превышающее направление.

Принятие решения о блокировке абонента при окончании средств на его счете на практике происходит не мгновенно, что также необходимо учитывать. Например, если блокировка срабатывает раз в минуту – при скорости соединения 1 Мбит/с, пользователь может скачать 7,5 Мбайт в убыток провайдеру.

3. Устойчивость к сбоям. При сбоях автоматизированная система расчётов по отношению к клиентам должна использовать политику «запрещено по умолчанию», чтобы провайдер не понёс больших убытков. Необходима надежная система резервного копирования данных, в том числе тарифов и счетов клиентов. Стоимость дополнительного дискового пространства намного меньше финансовых потерь, связанных с потерей информации.

Дополнительными требованиями к биллинговым системам являются следующие.

1. Поддержка актуальной карты границ сетей. По отношению к тарификации важно, чтобы биллинговая система производила расчеты, основанные на актуальных тарифах. Для этого необходимо поддерживать актуальной карту границ сетей. Один из способов решения данной проблемы состоит в периодическом скачивании у головного провайдера актуальной копии статических списков сетей, с которыми у головного провайдера заключены пиринговые соглашения. Альтернативой может быть использование протоколов динамической маршрутизации, с помощью которых можно получать границы пиринговой сети, если головной интернет-провайдер предоставляет такую услугу. Для этого может быть использован протокол RIP.

2. Оперативная связь с клиентом. Кроме классического веб-интерфейса, используемого для доступа к статистической информации и состоянию счета, существует необходимость предоставлять услугу рассылки наиболее важной для клиента информации на его электронный почтовый адрес или посредством услуги рассылки текстовых сообщений через операторов мобильной связи.

3. Кредитование клиентов. Если для организации, использующей автоматизированную систему расчётов, является приемлемым предоставление услуг в кредит, желательно предоставить каждому клиенту возможность лично принять решение, будет ли он немедленно отключен при исчерпании средств

на счете или продолжит работать в кредит. В последнем случае необходимо оговорить размер кредита для отдельных групп клиентов.

4. Гибкость тарифных планов. Перед пуском автоматизированной системы расчётов в рабочий цикл требуется спроектировать систему тарифных планов. В случае продажи трафика по одной фиксированной цене тарифы могут рассчитываться в кусочно-линейной зависимости от некоторого параметра – времени суток и дня недели либо объёма потребленных клиентом услуг.

5. Простота использования. Автоматизированная система расчётов должна позволять техническому персоналу без специальной подготовки управлять тарифными планами.

6. Комплексирование. Актуальной является задача интеграции автоматизированной системы расчётов в общую бухгалтерию провайдера, например, в 1С-бухгалтерию.

7. Поддержка операций со счетами клиента. При планировании структуры базы данных необходимо учитывать, что один клиент может иметь несколько различных счетов, которые могут быть объединены впоследствии либо наоборот. Довольно часто встречается ситуация, когда несколько клиентов работают с одним счётом.

2. Биллинговые системы мультисервисных сетей

2.1. Состав серверной части биллинговой системы

Серверная часть типовой биллинговой системы (например cakebilling) включает в свой состав следующие компоненты [4]:

- FreeRADIUS-сервер (версия 0.9.3 или выше);
- PPP версия 2.4.2.b3 и выше;
- Pptpd версия 1.1.3 и выше;
- PostgreSQL версия 7.4.x;
- JDK 1.3 и выше;
- Servlet/JSP контейнер;
- PostgreSQL JDBC Driver версии 3x.

Для развертывания такой биллинговой системы необходим сервер с установленной операционной системой Debian 4.0-r3 [5]. Порядок установки и конфигурирования ОС Debian 4.0-r3 приведен в приложении.

2.2. FreeRADIUS-сервер

Функции тарификации трафика, аккаунтинга, авторизации и аутентификации в биллинговой системе выполняет RADIUS-сервер (рис. 2.1).

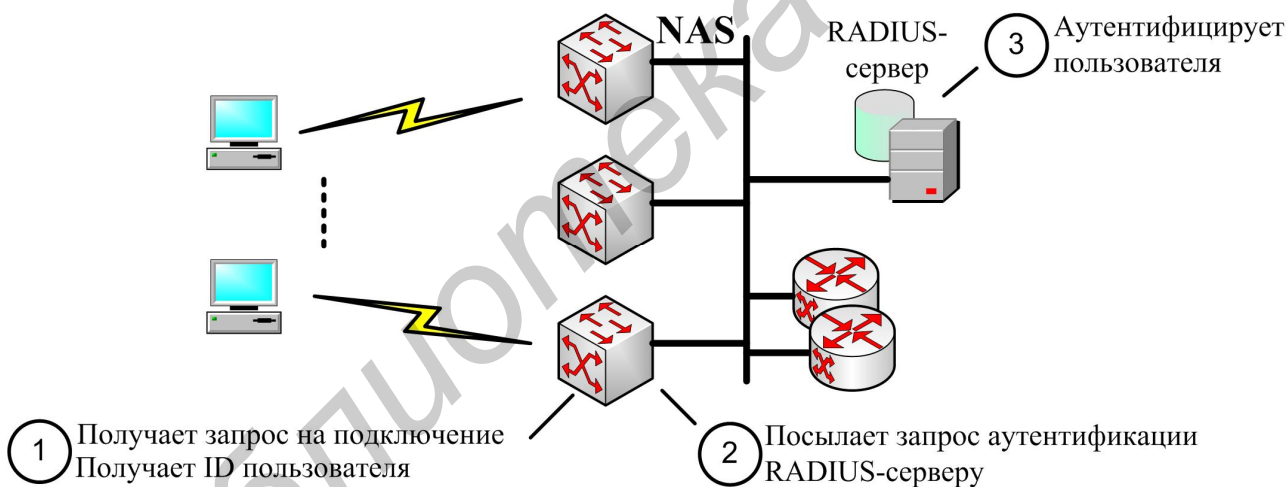


Рис. 2.1. RADIUS-модель контроля доступа

FreeRadius – один из популярных RADIUS-серверов (Remote Authentication Dial-In User Service), разработанный Livingston Enterprises для серии серверов доступа к корпоративной сети. В 1997 г. представлен в качестве стандарта в RFC 2058 и RFC 2059 (в 2008 г. выпущены стандарты RFC 2865 и RFC 2866). Существует несколько коммерческих и open-source RADIUS-серверов. Они несколько отличаются друг от друга по своим возможностям, но большинство поддерживает списки пользователей в текстовых файлах, LDAP и различных базах данных для записи учетных записей пользователей. Для удаленного мониторинга используется SNMP. Существуют прокси-серверы для RADIUS, упрощающие централизованное администрирование. В настоящее время разраба-

тывается протокол DIAMETER (в 2008 г. выпущены стандарты RFC 3588 и RFC 3589), который должен заменить RADIUS.

Протокол авторизации RADIUS является ключевой частью большинства биллинговых систем. Составные части службы идентификации удаленных пользователей описываются двумя стандартами RFC от IETF: RFC 2865 под названием Remote Authentication Dial-In User Service (RADIUS) в форме проекта стандарта и RFC 2866 под названием RADIUS Accounting в виде «информационного RFC».

Первоначально концепция RADIUS состояла в обеспечении удаленного доступа через коммутируемое телефонное соединение. Со временем определились дополнительные области применения этой технологии. К ним относятся серверы виртуальных частных сетей (Virtual Private Network, VPN) и точки доступа беспроводных локальных сетей (Wireless LAN, WLAN).

Концепция службы идентификации удаленных пользователей подразумевает, что клиент RADIUS – обычно сервер доступа, сервер VPN или точка доступа беспроводной локальной сети – отправляет серверу RADIUS параметры доступа пользователя (в англоязычной документации – Credentials, мандат, включающий настройки безопасности и права доступа), а также параметры соединения. Для этого клиент использует специальное сообщение RADIUS-Message. В ответ сервер начинает проверку, в ходе которой он аутентифицирует и авторизует запрос клиента RADIUS, а затем пересылает ему в качестве ответа сообщение RADIUS-Message-response. После этого клиент передает на сервер RADIUS учетную информацию (рис. 2.2).

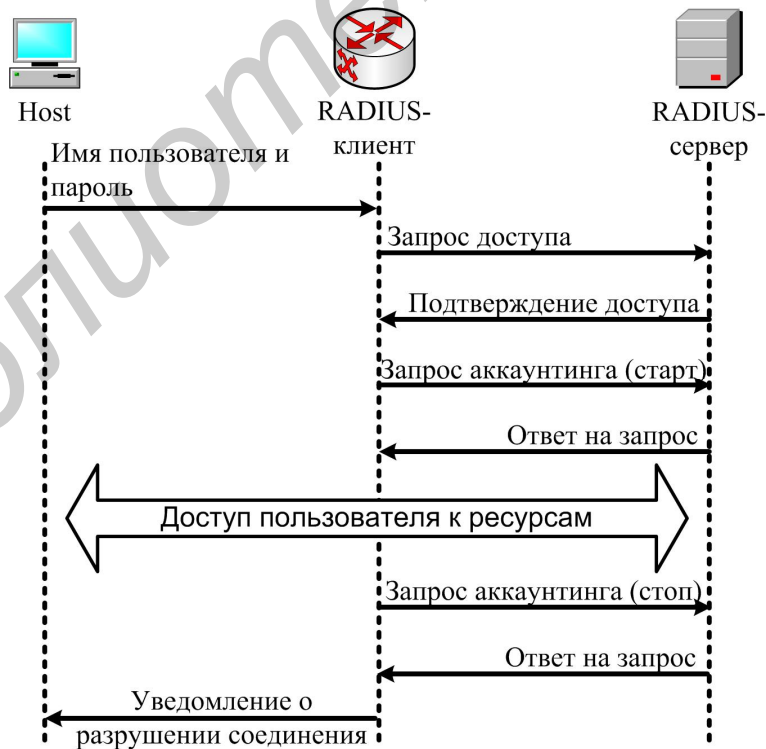


Рис. 2.2. Структура протокола обращения RADIUS-клиента к RADIUS-серверу

Сообщения RADIUS передаются в форме пакетов UDP. Информация об аутентификации направляется на порт UDP с номером 1812. Некоторые серверы доступа используют порты 1645 (для сообщений об аутентификации) или 1646 (для учета). Выбор порта должен определять администратор. В поле данных пакета UDP (в поле полезной нагрузки) всегда помещается только одно сообщение RADIUS. В соответствии с RFC 2865 и RFC 2866 определены следующие типы сообщений:

- Access-Request – «запрос доступа». Запрос клиента RADIUS, с которого начинается аутентификация и авторизация попытки доступа в сеть;
- Access-Accept – «доступ разрешен». Клиенту RADIUS сообщается, что попытка соединения была успешно аутентифицирована и авторизована;
- Access-Reject – «доступ не разрешен». Означает, что попытка доступа к сети не удалась. Такое возможно в том случае, если пользовательских данных недостаточно для успешной аутентификации или доступ для пользователя не авторизован;
- Access-Challenge – «вызов запроса». Сервер RADIUS передает его в ответ на запрос доступа;
- Accounting-Request – «запрос учета», который клиент RADIUS отсылает для ввода учетной информации после получения разрешения на доступ.

Сообщение RADIUS состоит из заголовка и атрибутов, каждый из которых содержит информацию о попытке доступа: например, имя и пароль пользователя, запрашиваемые услуги и IP-адрес сервера доступа. Главной задачей атрибутов RADIUS является транспортировка информации между клиентами и серверами RADIUS. Атрибуты RADIUS определены в RFC 2865, RFC 2866, RFC 2867, RFC 2868, RFC 2869 и RFC 3162.

RADIUS может работать совместно с различными протоколами аутентификации. Наиболее часто используются протокол аутентификации пароля (Password Authentication Protocol, PAP), протокол аутентификации с предварительным согласованием (Challenge Handshake Authentication Protocol, CHAP), а также MS-CHAP (CHAP от Microsoft в первой версии или MS-CHAPv2 – во второй).

Протокол CHAP – это протокол проверки подлинности типа «запрос-ответ», использующий стандартную схему хеширования Message Digest 5 (MD5) для шифрования ответа. Протокол CHAP используется множеством поставщиков серверов и клиентов доступа к сети. Сервер, использующий маршрутизацию и удаленный доступ, поддерживает CHAP таким образом, что выполняется проверка подлинности клиента удаленного доступа, требующего данный протокол. Так как CHAP требует использования обратимо зашифрованного пароля, рекомендуется использовать другой протокол проверки подлинности, например MS-CHAP версии 2.

Операционные системы семейства Windows Server поддерживают протокол MS-CHAP v2, обеспечивающий взаимную проверку подлинности, создание более надежных начальных ключей шифрования данных для MPPE (Microsoft Point-to-Point Encryption) и разные ключи шифрования для отправки и приема данных. Чтобы свести к минимуму риск раскрытия пароля во время обмена

паролями, из протокола исключена поддержка старых методов обмена паролями MS-CHAP. Поскольку версия MS-CHAP v2 обеспечивает более надежную защиту, чем MS-CHAP, при подключении сначала предлагается использовать именно ее (если она доступна), а затем уже MS-CHAP.

Протокол MS-CHAP v2 поддерживается на компьютерах, работающих под управлением Windows. Кроме того, возможно применение RADIUS вместе с PPP, протоколом передачи «точка – точка» (Point-to-Point Protocol). Результаты сеанса аутентификации между сервером доступа и действующим клиентом передаются на сервер RADIUS, который их потом удостоверяет.

Для защиты сообщений клиент и сервер RADIUS обладают «общим секретом» (ключом). При этом речь, как правило, идет о цепочке символов, имеющейся как на серверах, так и на клиенте RADIUS.

Еще одним недостатком RADIUS является «общий секрет» (Shared Secret). Это связано с тем, что очень часто один и тот же «общий секрет» служит для поддержки максимального количества пар «клиент-сервер» в службе RADIUS. К тому же в большинстве случаев криптологически он недостаточно устойчив против атаки с перебором слов по словарю в автономном режиме. Значение поля Response Authenticator и содержимое атрибута Message Authenticator легко вычисляются. Потом эти данные сравниваются с перехваченным сообщением Access-Accept, Access-Reject или Access-Challenge. Таким образом, легко разгадываемый «общий секрет» может быть быстро скомпрометирован.

Данная ситуация усугубляется вариантами реализации RADIUS – часто длина «общего секрета» не может превышать определенной величины или набор символов, из которых образуется ключевое слово, ограничен. В качестве примера можно привести распространенную установку на использование только тех символов из набора ASCII, которые находятся непосредственно на клавиатуре – то есть лишь 94 из 256 символов ASCII. Если выбор ограничен только возможностями клавиатуры, последовательность символов должна состоять минимум из 22 знаков и содержать примерно в одинаковой пропорции строчные и прописные буквы, цифры и специальные символы. Если же «общий секрет» может быть задан в виде строки из шестнадцатеричных чисел, следует задавать не менее 32 цифр.

RFC 2865 предписывает использование 16 символов в «общем ключе». Однако для достижения энтропии (в теории информации энтропия отражает количество информации в последовательности символов), равной 128 бит, каждый отдельный символ должен иметь энтропию 8 бит. Если выбор символов ограничен имеющимися на клавиатуре, энтропия 8-битного символа уменьшается до 5,8 бит. Поэтому, чтобы добиться уровня энтропии в 128 бит, необходимо 22 символа. В среде Windows 2000 максимально возможная длина «общего секрета» может быть равна 64 символам (из имеющихся на клавиатуре). Качественно улучшить результаты позволяет использование программ для генерирования «общего секрета», поскольку при этом обычно получаются лучшие, по сравнению с ручным вводом, значения энтропии. Кроме того, пара «клиент-сервер»,

использующая RADIUS, всегда должна быть защищена одним и тем же «общим секретом».

Соблюдение некоторых принципов при вводе RADIUS в эксплуатацию поможет свести различные риски к минимуму. При этом следует использовать алгоритм шифрования Triple DES (метод описан также в документе RFC 3162). Путем шифрования всего сообщения RADIUS защищаются особо чувствительные его части: поле удостоверения запроса в сообщении запроса доступа, атрибуты RADIUS (пароль пользователя или атрибуты ключа MPPE). При попытке проникновения в систему понадобится сначала расшифровать защищенное с помощью ESP сообщение RADIUS, а затем появится возможность анализировать его содержимое. Чтобы предотвратить атаки на сервер RADIUS извне, рекомендуется установить программное обеспечение для аутентификации с использованием сертификатов. Кроме того, возможны и другие варианты защиты, приводимые ниже.

1. Используемый «общий секрет» должен иметь длину не менее 32 шестнадцатеричных символов или 22 символов клавиатуры соответственно.

2. Для всех сообщений с запросом доступа обязательны атрибуты удостоверения сообщения. Для клиента RADIUS это означает, что атрибут удостоверения сообщения нужен и для всех сообщений запроса доступа. Это правило требуется соблюдать также в случае сервера RADIUS.

3. С криптографической точки зрения неизменным условием является качественное удостоверение запроса.

Нижеперечисленные требования помогут в реализации дополнительной защиты аутентификации.

1. Следует пользоваться EAP или схемами типа EAP с поддержкой сильных методов аутентификации, например метод EAP-TLS. Он требует обмена сертификатами между клиентом, пытающимся получить доступ, и сервером RADIUS. Все сообщения EAP должны иметь атрибуты удостоверения сообщения для защиты сообщений запроса доступа.

2. Необходимо выбирать методы аутентификации, рассчитанные на двустороннюю аутентификацию. При таком подходе противоположные конечные точки соединения аутентифицируют свои системы. Если с какой-либо стороны аутентификация пройдет неудачно, то в установлении соединения будет отказано. Примерами подобных методов служат EAP-TLS и MS-CHAPv2. В случае EAP-TLS сервер RADIUS проводит проверку пользовательского сертификата клиента, пытающегося получить доступ, а клиент в свою очередь – сертификата сервера RADIUS.

3. Если аутентификация производится посредством PAP, то эту опцию следует отключить. При аутентификации с помощью однократных паролей или токенов происходит откат к PAP. Но поскольку IEEE 802.1x не поддерживает PAP, в подобных случаях чаще всего пользуются соединениями PPP.

Расширенный протокол аутентификации (Extensible Authentication Protocol, EAP) изначально задумывался как дополнение к PPP для поддержки различных механизмов аутентификации доступа к сети. Протоколы аутентификации для PPP,

например CHAP, MS-CHAP и MS-CHAPv2, определяют механизм аутентификации во время фазы установления соединения. На этом этапе необходимо применять согласованный протокол аутентификации для верификации соединения.

При использовании EAP в процессе установления соединения в рамках PPP специальный механизм аутентификации не определяется. Лишь на этапе аутентификации участники взаимодействуют по специальной схеме аутентификации EAP. EAP позволяет осуществлять обмен сообщениями между клиентом, запрашивающим доступ, и аутентифицирующим сервером (в его роли часто выступает сервер RADIUS). При этом обмен сообщениями может варьироваться с учетом особенностей различных соединений. Он состоит из запросов, в которых требуется предоставление информации об аутентификации, и ответов. Длительность и конкретные детали сеанса аутентификации зависят от заданной схемы EAP.

В архитектурном плане EAP задумывался таким образом, чтобы аутентификацию можно было выполнять с помощью подключенных модулей с обеих сторон соединения: от клиента и от сервера. EAP предоставляет гибкую среду для внедрения безопасных методов аутентификации – если библиотечный файл EAP установить на обоих концах, то в любой момент можно применить новую схему аутентификации. EAP удобен при таких видах аутентификации, как токены (Generic Token Card), однократные пароли (One Time Password), запрос/ответ (MD5-Challenge) или защита на транспортном уровне (Transport Level Security). EAP используется не только с PPP. Он поддерживается на канальном уровне стандарта IEEE 802.

Например, службу RRAS операционной системы Windows можно настроить таким образом, что система с каждым сообщением запроса доступа станет отправлять атрибут удостоверения сообщения (Message-Authenticator). При этом в соответствующем диалоговом окне необходимо выбрать в свойствах опцию always use digital signatures («всегда использовать цифровую подпись»). Служба аутентификации в Интернет (Internet Authentication Service, IAS) настраивается со стороны Windows так, чтобы при получении любого сообщения запроса доступа проверялось наличие атрибута Message-Authenticator. Администратор должен установить соответствующий флажок в свойствах клиента RADIUS, чтобы клиент постоянно пересылал в запросе атрибут подписи. Если по каким-либо причинам такой вариант невозможен, Windows обладает механизмом учета и блокировки аутентификации. Благодаря этому механизму клиент не может превысить заданное количество попыток аутентификации за установленное время. Если же это происходит, система прервет с ним связь.

2.3. Протокол PPP

PPP – протокол канального уровня (Data Link) сетевой модели OSI. Это также механизм для создания и запуска IP и других сетевых протоколов на линиях связи (нуль-модемный кабель, Ethernet, модемная связь по телефонным линиям, мобильная связь по технологиям CSD, GPRS или EDGE). Используя PPP,

можно подключить компьютер к PPP-серверу и получить доступ к ресурсам сети, к которой подключён сервер.

2.4. Служба PPTP

Служба PPTP используется в биллинговой системе для создания VPN-подключения.

PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например Интернет. PPTP может использоваться для организации туннеля между двумя локальными сетями. Для обслуживания туннеля PPTP использует дополнительное TCP-соединение.

Спецификация протокола опубликована как информационный RFC 2637 в 1999 г. и не была ратифицирована IETF. Протокол считается менее безопасным, чем другие VPN-протоколы (например IPSec). PPTP работает, устанавливая обычную PPP-сессию с противоположной стороной с помощью протокола GRE. Второе соединение через TCP-порт 1723 используется для инициации и управления GRE-соединением. PPTP сложно перенаправить за сетевой экран, так как он требует одновременного установления двух сетевых сессий.

PPTP-трафик может быть зашифрован с помощью MPPE. Для аутентификации клиентов могут использоваться различные механизмы, наиболее безопасные из них MSCHAP-v2 и EAP-TLS.

2.5. СУБД PostgreSQL

PostgreSQL – свободная объектно-реляционная система управления базами данных (СУБД). Она используется в биллинговой системе для хранения данных о пользователях и контролируемом трафике. Вместе с другими свободными СУБД (такими, как MySQL и Firebird) PostgreSQL является альтернативой коммерческим СУБД (таким, как Oracle Database, Microsoft SQL Server, IBM DB2, Informix и СУБД производства Sybase).

2.6. Комплект разработчика JDK

Для инициализации JSP в биллинговой системе используется комплект разработчика JDK.

Sun JDK Blackdown JDK BEA Jrockit JDK – бесплатно распространяемый фирмой Sun комплект разработчика приложений на языке Java, включающий компилятор Java (javac), стандартные библиотеки классов Java, примеры, документацию, различные утилиты и исполнительную систему Java (JRE). В состав JDK не входит интегрированная среда разработки на Java (IDE), поэтому разработчик, использующий только JDK, вынужден применять внешний текстовый редактор и компилировать свои программы, используя утилиты командной строки.

Все современные интегрированные среды разработки на Java, такие, как NetBeans, Sun Java Studio Creator, IntelliJ IDEA, Borland JBuilder, Eclipse, опираются на сервисы, предоставляемые JDK, и вызывают для компиляции Java-программ компилятор командной строки из комплекта JDK. Поэтому эти среды разработки, либо

включают в комплект поставки одну из версий JDK, либо требуют для своей работы предварительной инсталляции JDK на машине разработчика.

Фирма Sun предоставляет полные исходные тексты JDK, включая исходные тексты самого Java-компилятора.

2.7. Servlet/JSP-контейнер

Для построения Web-интерфейса биллинговой системы используется Java servlets/JSP (сервлеты).

Сервлет является Java-программой, выполняющейся на стороне сервера и расширяющей функциональные возможности сервера. Сервлет взаимодействует с клиентами посредством принципа запрос – ответ. Сервлеты должны реализовывать Servlet-интерфейс, который определяет методы жизненного цикла.

Хотя сервлеты могут обслуживать любые запросы, они обычно используются для расширения Web-серверов. Для таких приложений технология Java Servlet определяет HTTP-специфичные Servlet-классы. Пакеты javax.servlet и javax.servlet.http обеспечивают интерфейсы и классы для создания сервлетов.

JSP является составной частью единой технологии создания бизнес-приложений J2EE. Технология позволяет внедрять Java-код, а также EL (expression language) в статичное содержимое страницы. Также могут использоваться библиотеки JSP-тегов для внедрения их в JSP-страницы. Страницы компилируются JSP-компилятором в сервлеты, представляющие собой Java-классы, которые выполняются на сервере. Сервлеты также могут быть написаны разработчиком, не используя JSP-страницы. Эти технологии могут дополнять друг друга.

JSP – высокопроизводительная технология – весь код страницы транслируется в java-код сервлета с помощью компилятора JSP-страниц Jasper и компилируется в байт-код виртуальной машины java (JVM). Сервлет-контейнеры (Tomcat), способные исполнять JSP-страницы, написаны на платформе независимом языке Java, который может работать под различными операционными системами и платформами. Сервлет-контейнеры могут работать как полноценные самостоятельные Web-серверы, служить поставщиками страниц для других Web-серверов или интегрироваться в J2EE-серверы приложений. Web-контейнер обеспечивает обмен данными между сервлетом и клиентами, берет на себя выполнение таких функций, как создание программной среды для функционирующего сервлета, идентификацию и авторизацию клиентов, организацию сессии для каждого из них.

2.8. PostgreSQL JDBC-драйвер

JDBC основана на концепции так называемых драйверов, позволяющих получить соединение с базой данных по специально описанному URL. Драйверы могут загружаться динамически (во время работы программы). Загрузившись, драйвер сам регистрирует себя и вызывается автоматически, когда программа требует URL, содержащий протокол, за который драйвер «отвечает».

3. Лабораторная работа

«Администрирование биллинговой системы CakeBilling»

3.1. Цель работы

Ознакомиться с принципами построения и функционирования биллинговой системы CakeBilling, приобрести базовые навыки по администрированию данной биллинговой системы в мультисервисной сети.

3.2. Описание лабораторной работы

3.2.1. Общая характеристика лабораторной базы

Лабораторная работа выполняется на базе учебной мультисервисной сети. На рис. 3.1 представлена общая структура учебной мультисервисной сети, развернутой на кафедре «Сети и устройства телекоммуникаций».

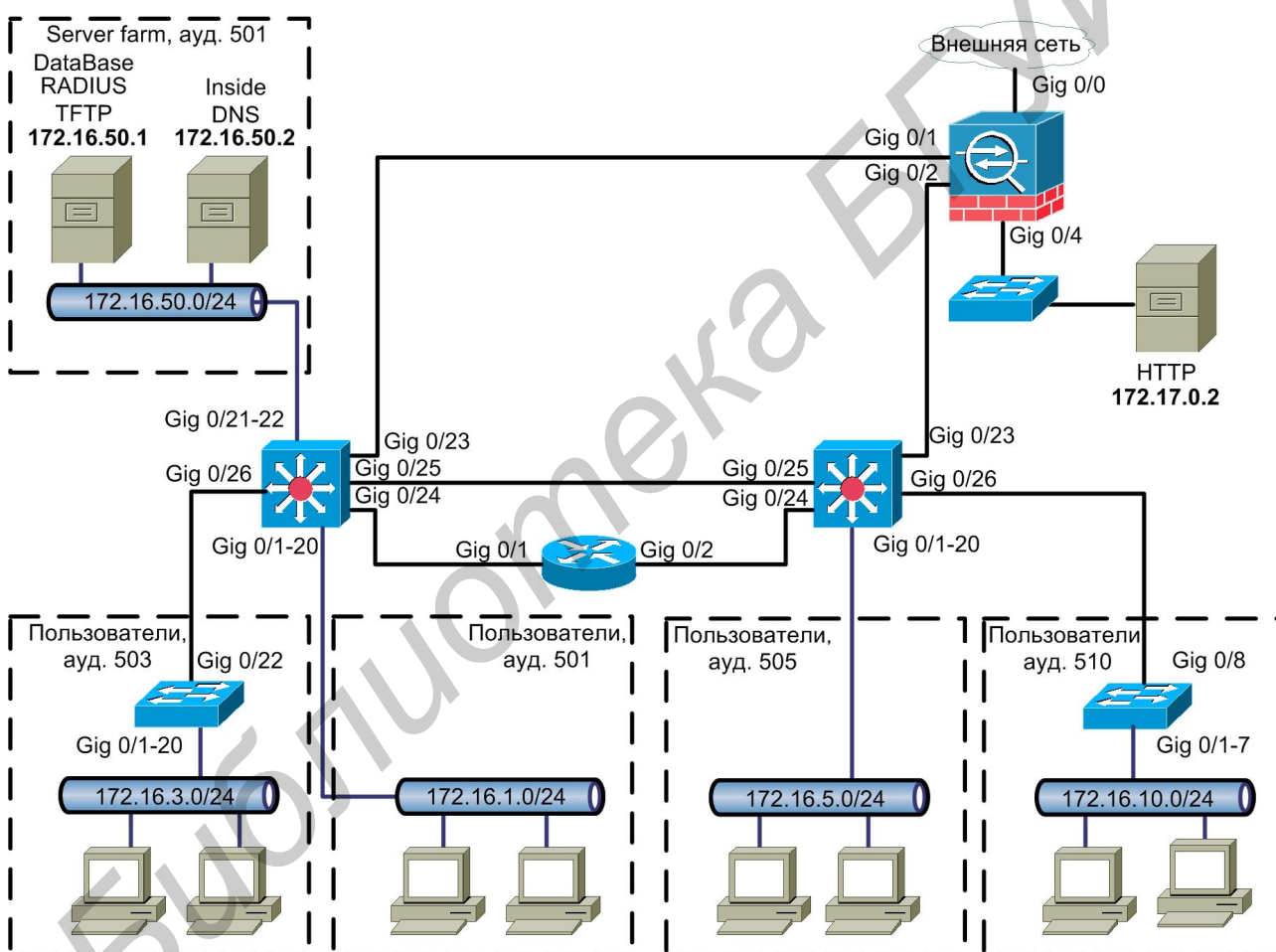


Рис. 3.1. Общая структура учебной мультисервисной сети кафедры СиУТ

Учебная мультисервисная сеть включает кампосный и глобальный сегменты, связанные между собой посредством межсетевых экранов Cisco 5500 ASA. В кампосном сегменте размещен сервер автоматизированных платежей с установленной биллинговой системой CakeBilling. К одному из портов биллинг-сервера через коммутатор Cisco 3560 подключен сегмент виртуальной сети, объединяющий клиентские рабочие станции (рис. 3.2). Другой порт биллинг-сервера через коммутатор

Cisco 3560 и межсетевой экран Cisco 5500 ASA соединен с глобальным сегментом, обеспечивающим доступ к серверам приложений через маршрутизаторы Cisco серий 2500, 2600, 1900, 1600, 1700, 2821 и 4000.

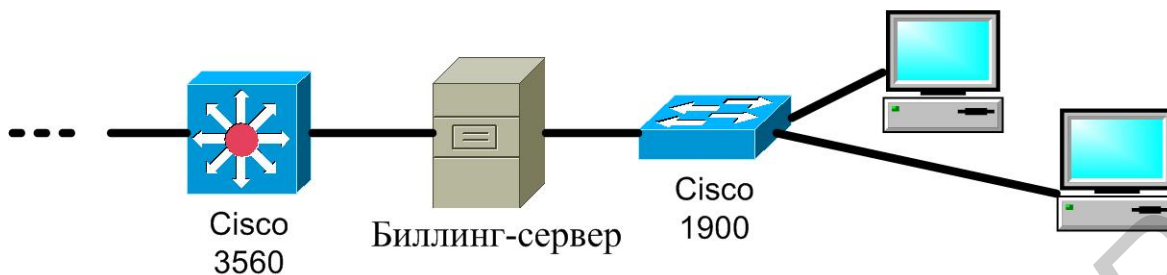


Рис. 3.2. Структурная схема фрагмента учебной мультисервисной сети с размещенным в ней биллинг-сервером

Логика соединений портов биллинг-сервера, коммутаторов и маршрутизаторов задается администратором учебной мультисервисной сети (рис. 3.3).

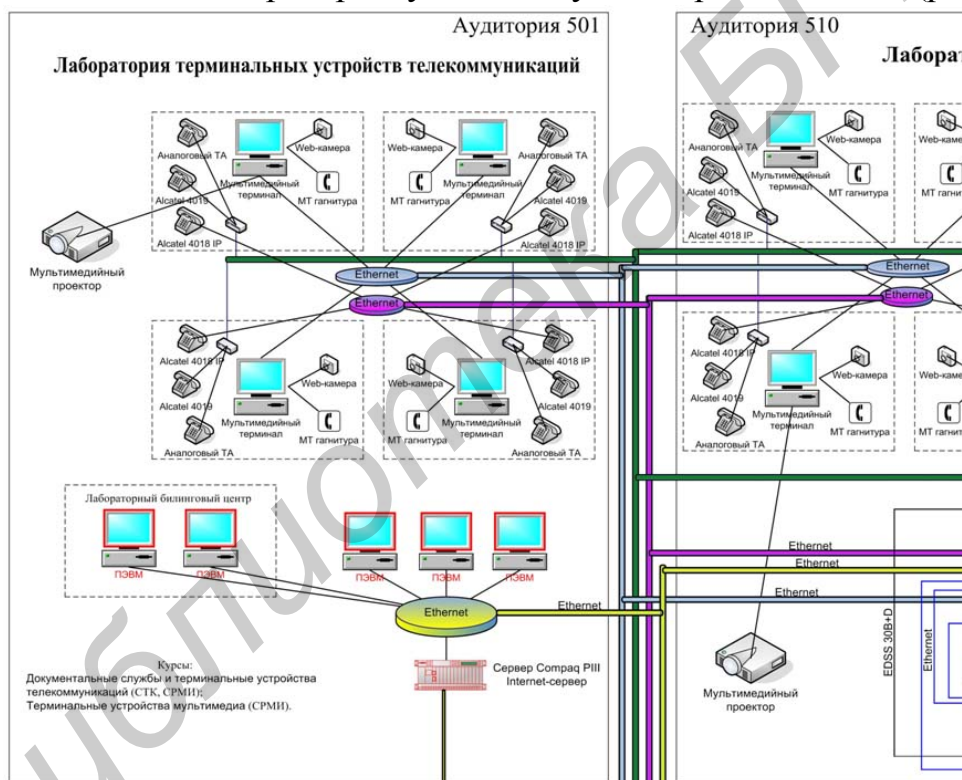


Рис. 3.3. Логика включения биллинг-сервера в мультисервисную сеть

Биллинговая система CakeBilling применяется для контроля доступа в глобальную сеть (например Интернет) из локальных сетей предприятий и домашних локальных сетей.

Возможности биллинговой системы CakeBilling:

- учёт трафика;
- поддержка нескольких тарифов;

– ограничение доступа в Интернет по расходу времени и трафика (концепция лицевого счёта и положительного баланса).

Биллинговая система CakeBilling поддерживает следующие виды отчётности:

– интенсивность расхода трафика в зависимости от часов суток, дней недели, дней месяца;

– объём трафика (суммарный, пользовательский) за календарные периоды (сутки, недели, месяцы);

– объём трафика (суммарный, пользовательский) за произвольный заданный период.

Особенностью биллинговой системы CakeBilling является сборка из стандартных пакетов для *nix-систем. Ядром системы являются конфигурационные файлы структуры базы данных, архив с Web-интерфейсом и изменённые под нужды биллинговой системы конфигурационные файлы стандартных приложений.

Роль стандартных *nix-приложений в биллинговой системе CakeBilling заключается в следующем:

– rrpdpd – менеджер VPN соединений (обеспечивает первоначальное подключение и запуск rpppd);

– rpppd – транспортный инкапсулятор туннелей (обеспечивает инкапсуляцию PPP в IP-протокол);

– FreeRADIUS – RADIUS сервер (обеспечивает AAA-сервисы: Authorization, Authentication, Accounting);

– PostgreSQL – сервер СУБД (обеспечивает хранение аккаунтов, информации о трафике, содержит необходимую бизнес-логику для учёта трафика и ограничения доступа в Интернет).

Биллинговая система CakeBilling состоит из клиентской и серверной части.

Механизм соединения в биллинговой системе CakeBilling заключается в следующем.

1. На стороне клиента необходимо создать VPN-подключение.

2. При попытке подключения клиента к серверу служба rrpdpd создает GRE-туннель и передает поток службе rpppd.

3. Служба rpppd запрашивает авторизацию у RADIUS-сервера.

4. RADIUS-сервер обращается к СУБД и на основе полученных данных формирует ответ.

5. rpppd получает ответ от RADIUS-сервера, разрешающий или запрещающий подключение.

6. При получении разрешающего ответа служба rpppd устанавливает различные лимиты по времени или допустимому объему трафика на сессию, если необходимые атрибуты содержались в ответе.

7. После этого служба rpppd отправляет RADIUS-серверу пакет с уведомлением о запуске сессии.

8. Далее служба pppd может отправлять данные о промежуточном состоянии сессии, если в ответе от RADIUS-сервера был установлен необходимый атрибут.

9. Сессия завершается при разрыве соединения пользователем или службой pppd при превышении установленных лимитов.

10. После закрытия сессии служба pppd отправляет RADIUS-серверу пакет о завершении сессии.

Описание порядка обмена пакетами в терминах RADIUS-протокола представлено в таблице.

Порядок обмена пакетами в терминах RADIUS-протокола

Шаг	Пакет	Цель	-	Цель	Атрибуты	Примечания
<i>Авторизация</i>						
1	auth-request	pppd	>	radius	username, userpassword	Запрос на существование юзера в базе
2	auth-accept/auth-reject	pppd	<	radius	yes or no	Есть/нет
<i>Получение reply пакета</i>						
3	auth-reply	pppd	<	radius	traffic limit, time limit	Ответ
<i>Работа на линии</i>						
5	acct-start	pppd	>	radius	current datetime, username, session id	Старт сессии
6	acct-alive	pppd	>	radius	current datetime, session id, traffic	Обновление данных сессии
...	acct-alive	pppd	>	radius	...	Повторение с заданным периодом
7	acct-stop	pppd	>	radius	current datetime, traffic	Стоп сессии
<i>Ответ</i>						

3.2.2. Описание клиентской части биллинговой системы CakeBilling

3.2.2.1. *Функции клиентской части.* Клиентская часть инициирует VPN-туннель между внешним сетевым интерфейсом машины-сервера и внешним сетевым интерфейсом клиента. Внешний сетевой интерфейс – это интерфейс, через который осуществляется выход в Интернет.

3.2.2.2. *Принципы функционирования клиентской части.* Машина-клиент посылает запрос на аутентификацию службе rprtd машине-сервера. По введённому имени пользователя и паролю клиент проходит авторизацию, если количество условных единиц на его счету больше нуля. В противном случае клиент получает отказ в соединении. В процессе работы клиента с серверной частью ведётся аккаунтинг и, если баланс пользователя станет меньше нуля, происходит автоматическое отключение пользователя. Подключиться к системе пользователь сможет, когда администратор пополнит его счёт.

Клиент имеет доступ к персональной статистике, для входа в которую требуется авторизация (рис. 3.4, 3.5).

Рис. 3.4. Диалоговое окно «Вход в систему статистики»

Персональная статистика

isid: Иван Сидоров

от	День	Расход, мб	Тарифный план	Начисление
01.1.2008	01.01.2008	12.87	Оптим	29.61 руб.
	02.01.2008	28.61	Оптим	65.80 руб.
	03.01.2008	38.15	Оптим	87.74 руб.
	04.01.2008	19.07	Оптим	43.87 руб.
	05.01.2008	13.35	Оптим	30.71 руб.
	06.01.2008	62.94	Оптим	144.77 руб.
	07.01.2008	66.76	Оптим	153.54 руб.
	Всего за период	241.76		556.04 руб.

[Выход »](#)

Рис. 3.5. Диалоговое окно «Персональная статистика пользователя»

3.2.2.3. *Порядок работы клиентской части (создание VPN-подключения).*

Далее изложен порядок работы для ОС Windows XP.

Для создания VPN-подключения необходимо выполнить следующие операции.

1. Следует открыть окно «Мастер новых подключений» (рис. 3.6). Для этого необходимо выбрать последовательно кнопку «Пуск», опцию «Панель управления», опцию «Сеть и подключения к Интернету», опцию «Сетевые подключения» и опцию «Создание нового подключения».

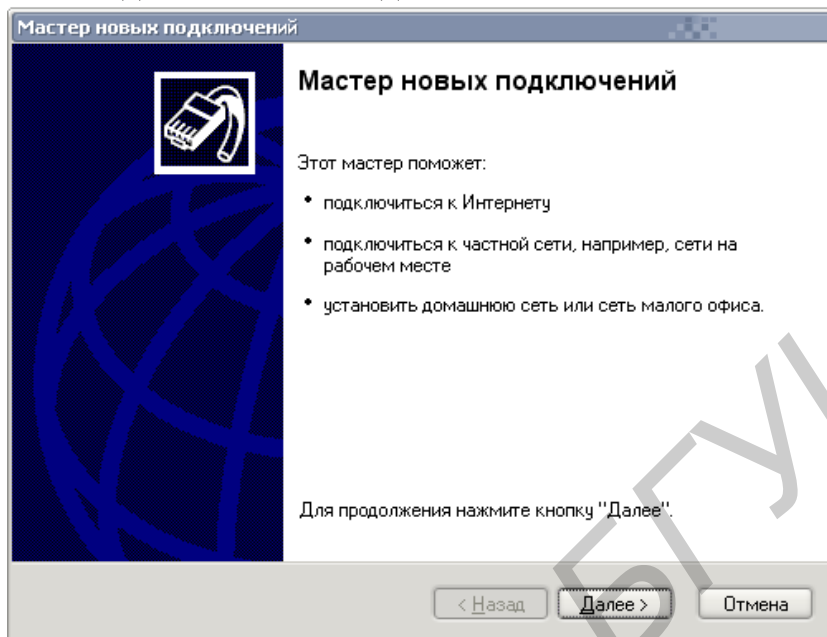


Рис. 3.6. Диалоговое окно «Мастер новых подключений»

2. Нажать кнопку «Далее» диалогового окна «Мастер новых подключений» (см. рис. 3.6).

3. Выбрать опцию «Подключить к сети на рабочем месте» диалогового окна «Тип сетевого подключения» (рис. 3.7).

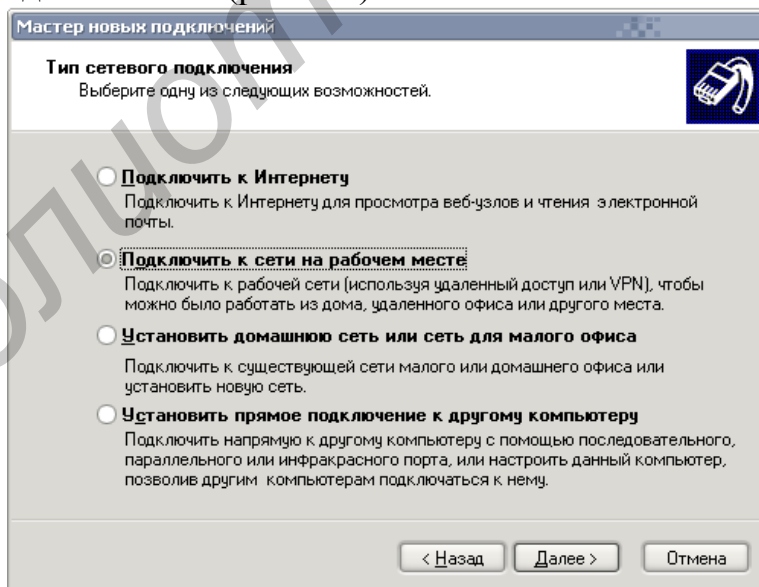


Рис. 3.7. Диалоговое окно «Тип сетевого подключения»

4. Выбрать опцию «Подключение к виртуальной частной сети» диалогового окна «Сетевое подключение» (рис. 3.8).

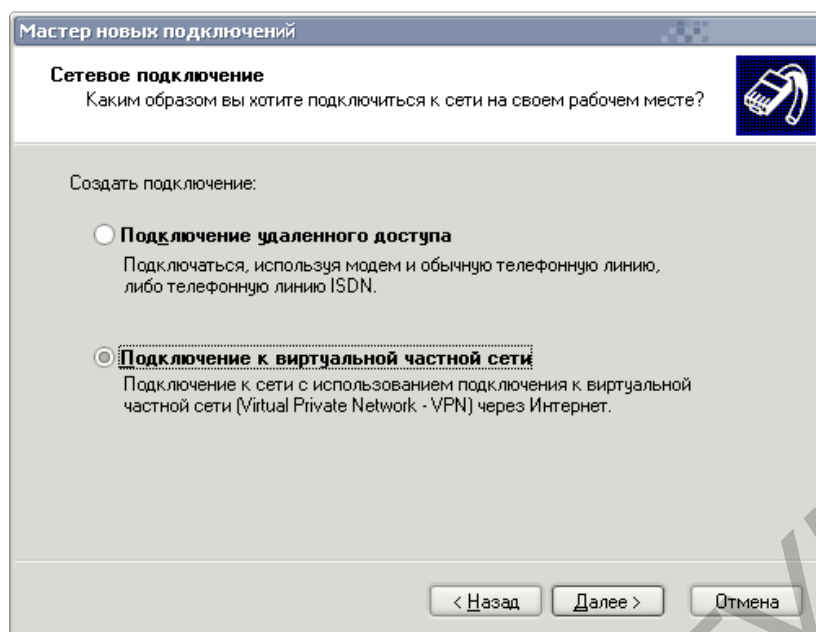


Рис. 3.8. Диалоговое окно «Сетевое подключение»

5. В диалоговом окне «Имя подключения» ввести имя подключения, например «student» (рис. 3.9).

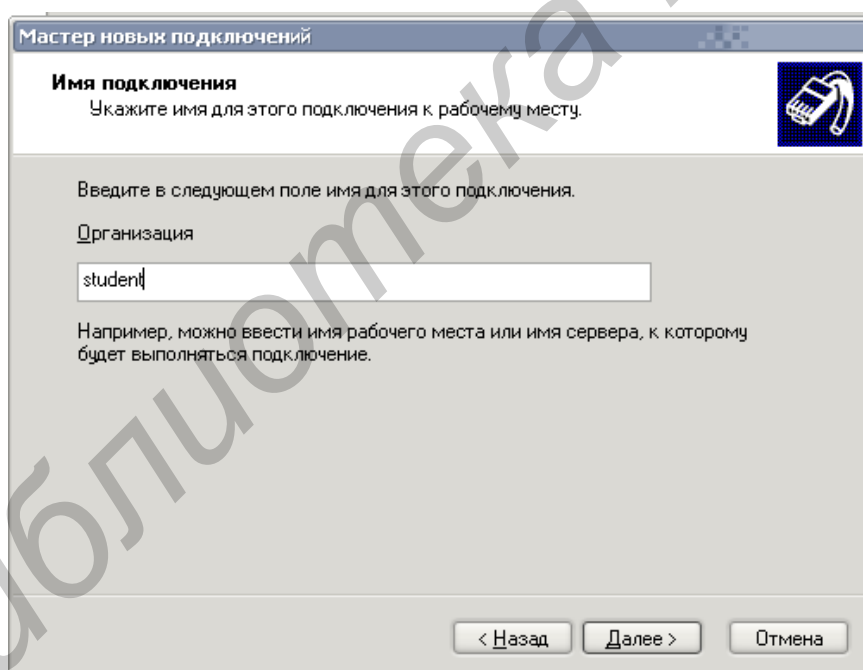


Рис. 3.9. Диалоговое окно «Имя подключения»

6. В диалоговом окне «Публичная сеть» выбрать опцию «Не набирать номер для предварительного подключения» (рис. 3.10).

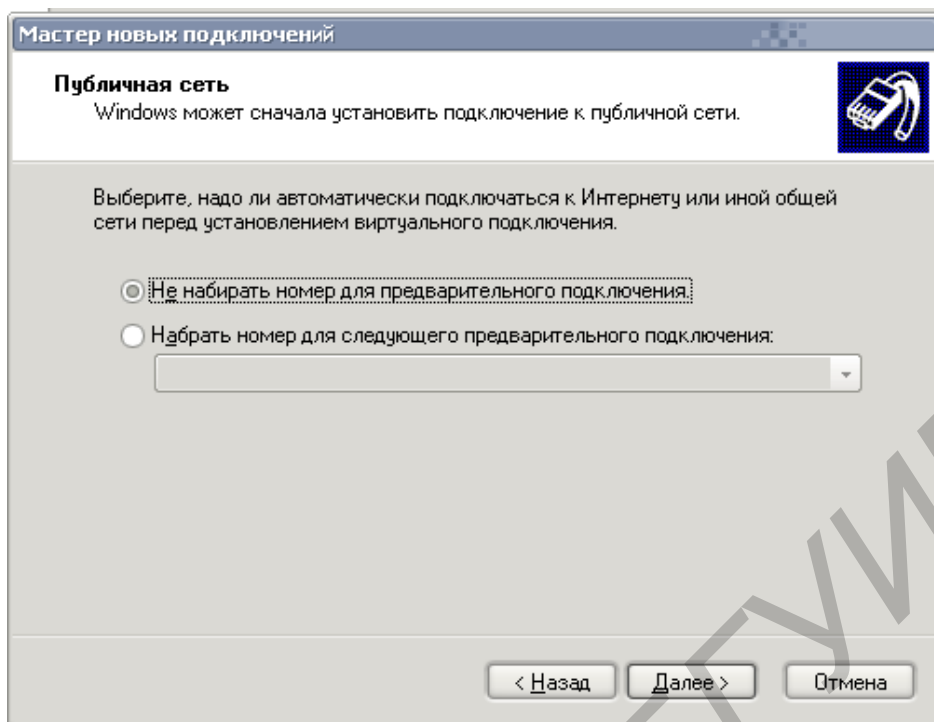


Рис. 3.10. Диалоговое окно «Публичная сеть»

7. В диалоговом окне «Выбор VPN-сервера» ввести IP-адрес сервера, например «192.168.1.1» (рис. 3.11).

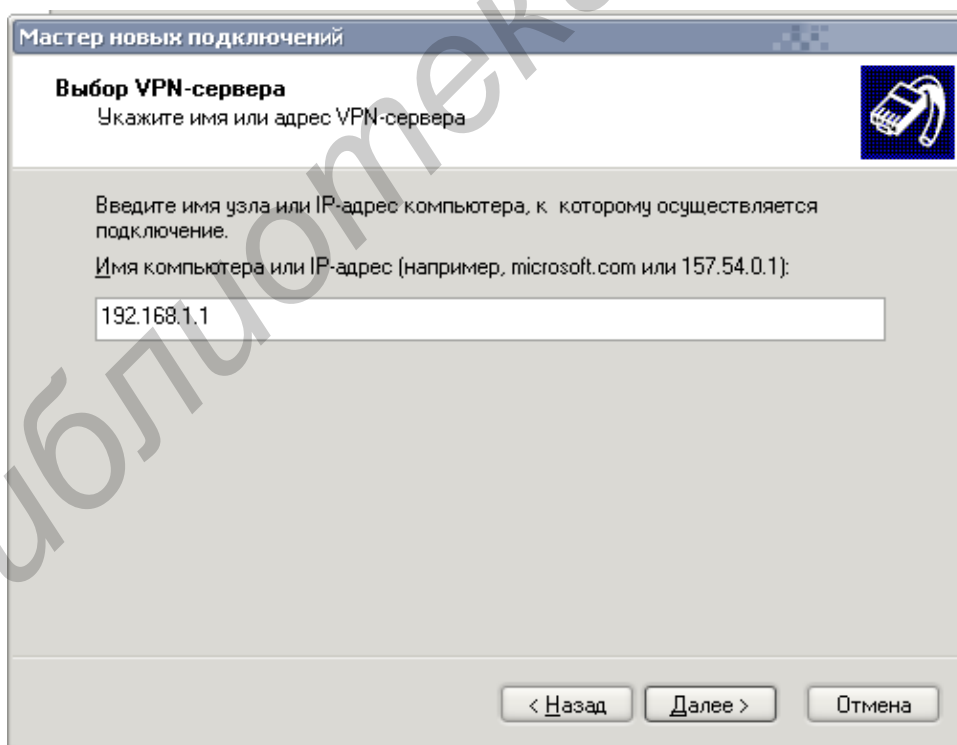


Рис. 3.11. Диалоговое окно «Выбор VPN-сервера»

8. В диалоговом окне «Завершение работы мастера новых подключений» выбрать опцию «Добавить ярлык подключения на рабочий стол» (рис. 3.12).

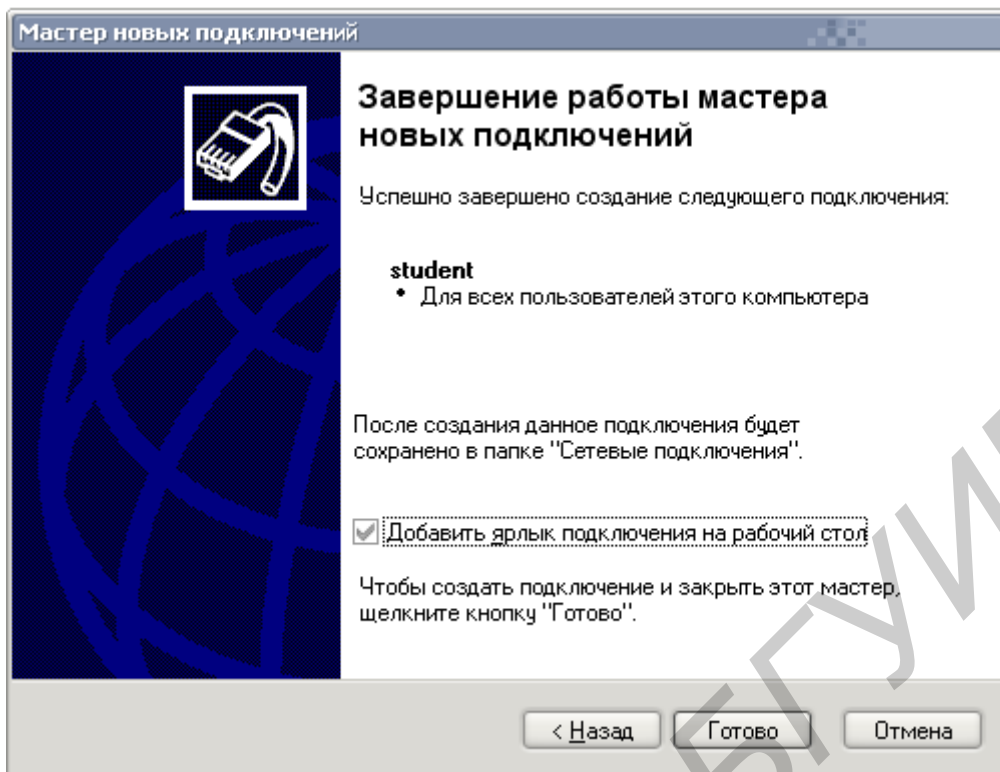


Рис. 3.12. Диалоговое окно «Завершение работы мастера новых подключений»

Для настройки параметров нового подключения необходимо выполнить следующие процедуры.

1. Нажать кнопку «Свойства» диалогового окна «Подключение» (рис. 3.13).

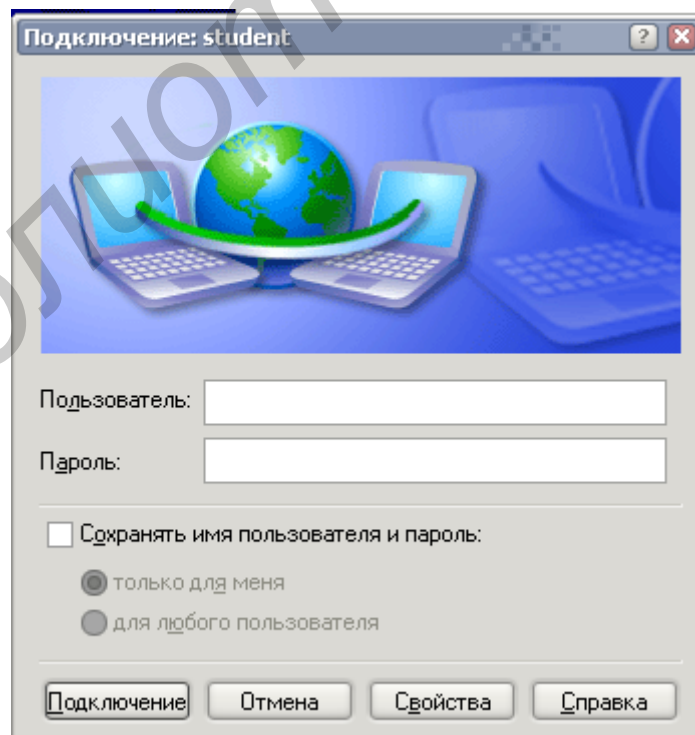


Рис. 3.13. Диалоговое окно «Подключение»

2. В диалоговом окне «Свойства» выбрать вкладку «Безопасность» и деактивировать строку «Требуется шифрование данных (иначе отключаться)» (рис. 3.14).

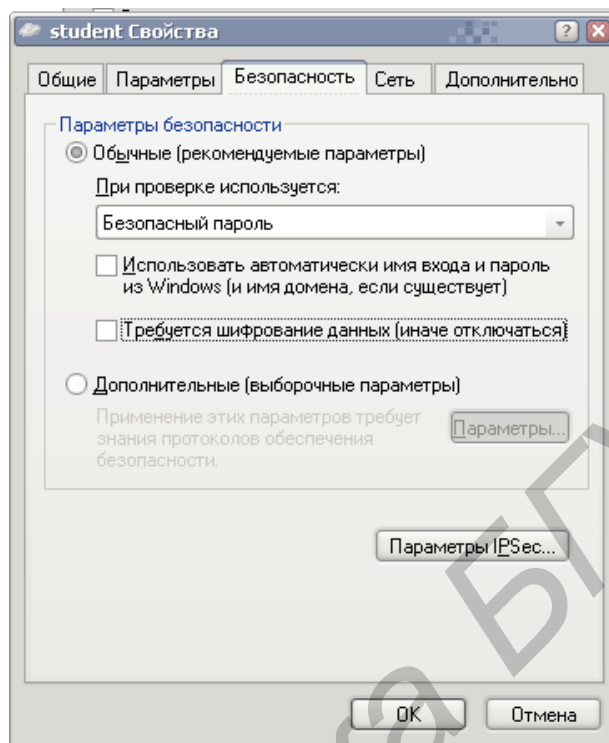


Рис. 3.14. Диалоговое окно «Свойства»

3. В диалоговом окне «Подключение» ввести имя и пароль пользователя и нажать кнопку «Подключение» (рис. 3.15).

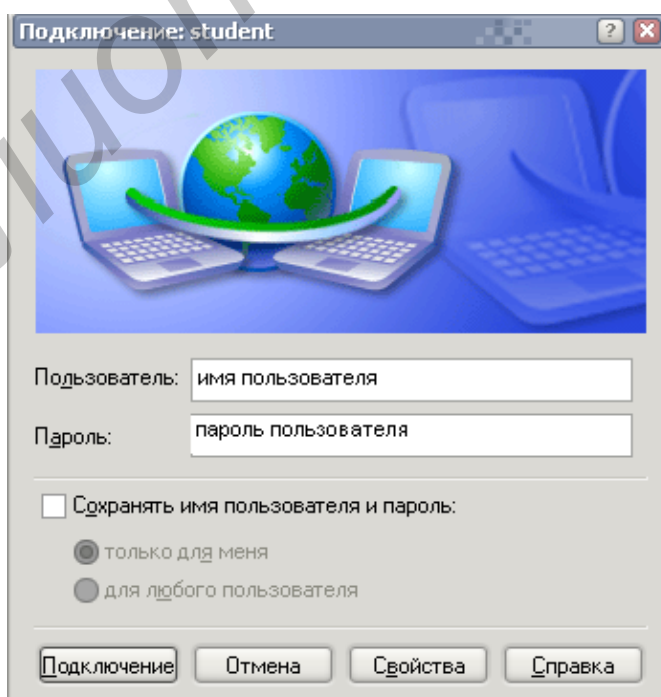


Рис. 3.15. Диалоговое окно «Подключение»

3.2.3. Описание серверной части биллинговой системы CakeBilling

3.2.3.1. *Функции серверной части.* Серверная часть лабораторной установки выполняет процессы аутентификации, авторизации и аккаунтинга пользователей.

3.2.3.2. *Принципы функционирования серверной части.* Аутентификация выполняется за счёт проверки идентичности имени и пароля пользователя между предоставляемыми именем и паролем при подключении и именем и паролем в базе данных серверной части.

Авторизация выполняется за счёт проверки состояния блокировки учётной записи клиента в базе данных на стороне серверной части. Состояние блокировки происходит, когда баланс клиента становится отрицательным.

Аккаунтинг осуществляется за счёт периодического обновления данных сессии. Система произведёт автоматическое отключение клиента, когда баланс клиента станет отрицательным.

3.2.3.3. *Порядок работы серверной части (формирование сводного отчета и текущего статуса).* Для того чтобы получить сводный отчёт и текущий статус, необходимо выполнить следующие операции.

1. Запустить веб-браузер и ввести в адресной строке адрес биллинг-сервера «<http://192.168.1.1:8080/cake>».

2. В диалоговом окне «Вход в систему статистики» необходимо ввести имя администратора, например «studentadmin», и пароль, например «studentadmin», (рис. 3.16).

При этом в диалоговом окне «Сводный отчёт и текущий статус» появится сводный отчет и текущий статус пользователей (рис. 3.17).

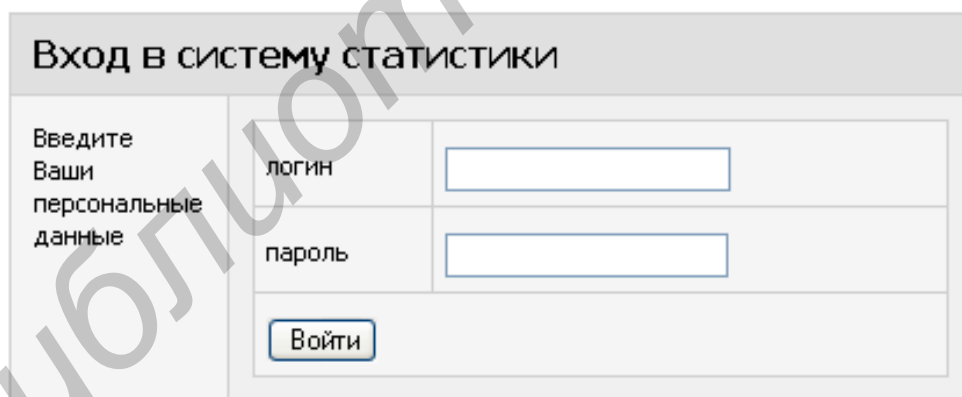


Рис. 3.16. Диалоговое окно «Вход в систему статистики»

3.2.3.4. *Порядок работы серверной части (работа с карточкой пользователя).* Для того чтобы получить доступ к учетной карточке пользователя, необходимо выполнить следующие операции.

1. Выполнить требования подпункта 3.2.3.1.

2. В появившемся диалоговом окне «Сводный отчёт и текущий статус» выбрать вкладку «Пользователи» (рис. 3.18).

Сейчас на линии

№	Пользователь	IP	Время старта	Трафик за сеанс
1	Иван Сидоров	isid	3 07.01, 15:01	66.76 мб.
2	ООО Прогресс	progress	5 07.01, 15:02	31.47 мб.

Расход, баланс, состояние

№	Пользователь		Баланс		Расход за месяц		Внесено за месяц		Подключение	Управление
1	Иван Сидоров	isid	-159.15 мб.	-366.04 руб.	241.76 мб.	556.04 руб.	82.61 мб.	190.00 руб.	Разрешено	Параметры
2	ИП Васильев	ipvas	-11.17 мб.	-44.69 руб.	161.17 мб.	644.68 руб.	150.00 мб.	600.00 руб.	Перерасход	Параметры
3	Сергей Ситников	ssit	253.61 мб.	355.06 руб.	139.24 мб.	194.93 руб.	392.86 мб.	550.00 руб.	Разрешено	Параметры
4	ООО Прогресс	progress	315.33 мб.	1261.30 руб.	109.67 мб.	438.69 руб.	425.00 мб.	1700.00 руб.	Разрешено	Параметры
5	Василий Петров	vpet	326.62 мб.	457.27 руб.	72.48 мб.	101.47 руб.	357.14 мб.	500.00 руб.	Разрешено	Параметры
6	Анна Колотыгина	akol	-6.50 мб.	-12.35 руб.	59.13 мб.	112.34 руб.	52.63 мб.	100.00 руб.	Перерасход	Параметры
7	Денис Чупров	dchepr	123.07 мб.	233.83 руб.	29.56 мб.	56.17 руб.	152.63 мб.	290.00 руб.	Разрешено	Параметры
8	Администратор биллинга	admin	50.00 мб.	100.00 руб.	0.00 мб.	0.00 руб.	50.00 мб.	100.00 руб.	Разрешено	Параметры
[ВСЕ]			891.81 мб.	1984.38 руб.	813.01 мб.	2104.33 руб.	1662.87 мб.	4030.00 руб.	...	

Рис. 3.17. Диалоговое окно «Сводный отчёт и текущий статус»

Статус Пользователи Тарифы Отчёты Настройки Выход »

Управление пользователями

Пользователи

- [Администратор биллинга](#) admin
- [Анна Колотыгина](#) akol
- [Денис Чупров](#) dchepr
- [ИП Васильев](#) ipvas
- **Иван Сидоров** isid
- [ООО Прогресс](#) progress
- [Сергей Ситников](#) ssit
- [Василий Петров](#) vpet

Новый пользователь?

- [Добавить пользователя](#)

Баланс

-366.04 руб.

Новый платёж

0.0 руб.

Платежи

07.01, 14:15:	150.00
03.01, 17:38:	40.00

Данные пользователя Иван Сидоров, isid

Имя, фамилия

Логин

Пароль

Тариф

Группа

Доступ в интернет
 Блокировать

Доступ в интернет при отрицательном балансе
 Блокировать

•

Рис. 3.18. Диалоговое окно «Карточка пользователя»

3.2.3.5. *Порядок работы серверной части (управление тарифами)*. Для того чтобы получить доступ к тарифным планам, необходимо выполнить следующие операции.

1. Выполнить требования подпункта 3.2.3.1.

2. В появившемся диалоговом окне «Сводный отчёт и текущий статус» выбрать вкладку «Тарифы» (рис. 3.19).

Статус	Пользователи	Тарифы	Отчёты	Настройки	Выход »
Управление тарифами					
Наименование	Цена за мегабайт, руб.	Операции			
Оптимизация	2.30	Обновить	Удалить		
Основной	2.00	Обновить	Удалить		
Юридический базовый	4.00	Обновить	Удалить		
Мини	1.90	Обновить	Удалить		
Ультра	1.40	Обновить	Удалить		
Добавление нового тарифа					
Новый тариф	0.00	Добавить			

Рис. 3.19. Диалоговое окно «Управление тарифами»

3.2.3.6. *Порядок работы серверной части (формирование отчета по начислениям и потреблению услуг)*. Для того чтобы сформировать отчет по начислениям и потреблению услуг, необходимо выполнить следующие операции.

1. Выполнить требования подпункта 3.2.3.1.

2. В появившемся диалоговом окне «Сводный отчёт и текущий статус» выбрать вкладку «Отчеты» (рис. 3.20).

3. В поле «Пользователь» выбрать требуемого пользователя или всех пользователей и указать период статистики.

3.2.3.7. *Порядок работы серверной части (технологическая настройка)*. Для общего конфигурирования биллинговой системы необходимо выполнить следующие операции.

1. Выполнить требования подпункта 3.2.3.1.

2. В появившемся диалоговом окне «Сводный отчёт и текущий статус» выбрать вкладку «Настройка» (рис. 3.21).

День	Расход, мб	Тарифный план	Начисление
01.01.2008	75.34	Ультра	105.48 руб.
01.01.2008	12.87	Оптима	29.61 руб.
01.01.2008	49.59	Юридический базовый	198.37 руб.
02.01.2008	20.03	Ультра	28.04 руб.
02.01.2008	28.61	Оптима	65.80 руб.
02.01.2008	11.44	Юридический базовый	45.78 руб.
03.01.2008	38.15	Оптима	87.74 руб.
03.01.2008	38.15	Юридический базовый	152.59 руб.
04.01.2008	56.27	Ультра	78.78 руб.
04.01.2008	19.07	Оптима	43.87 руб.
04.01.2008	73.43	Юридический базовый	293.73 руб.
05.01.2008	3.81	Ультра	5.34 руб.
05.01.2008	32.42	Мини	61.61 руб.
05.01.2008	13.35	Оптима	30.71 руб.
05.01.2008	66.76	Юридический базовый	267.03 руб.
06.01.2008	4.77	Ультра	6.68 руб.
06.01.2008	26.70	Мини	50.74 руб.
06.01.2008	62.94	Оптима	144.77 руб.
07.01.2008	51.50	Ультра	72.10 руб.
07.01.2008	29.56	Мини	56.17 руб.
07.01.2008	66.76	Оптима	153.54 руб.
07.01.2008	31.47	Юридический базовый	125.89 руб.
Всего за период	813.01		2104.37 руб.

Рис. 3.20. Диалоговое окно «Отчёты»

Статус	Пользователи	Тарифы	Отчёты	Настройки	Выход »
--------	--------------	--------	--------	-----------	---------

Системные настройки

Наименование	Значение	Описание	Операции	
clear_keepalive	30	Время ротации статистики (в днях)	Обновить	Удалить
idle_timeout	7200	«Сонный» таймаут (в секундах)	Обновить	Удалить
ipnetmask	255.255.255.0	Маска виртуальной сети	Обновить	Удалить
ipsubnet	192.168.2	Виртуальная подсеть (в формате «x.x.x»)	Обновить	Удалить
max_pool_ip	254	Максимальный ip адрес клиента	Обновить	Удалить
max_timeout	43200	Максимальное время сессии (в секундах)	Обновить	Удалить
max_traffout	1073741824	Максимальный трафик сессии (в байтах)	Обновить	Удалить
min_pool_ip	2	Минимальный ip адрес клиента	Обновить	Удалить
traffinterval	60	Период обновления данных о расходе трафика (в секундах)	Обновить	Удалить

Добавление нового параметра

<input type="text"/>	<input type="text"/>	Новый параметр	Добавить
----------------------	----------------------	----------------	----------

Рис. 3.21. Диалоговое окно «Технологические настройки»

3.3. Предварительное задание к лабораторной работе

3.3.1. Ознакомиться с задачами, общей структурой и функциями биллинговых систем, рассмотренных в разд. 1.

3.3.2. Ознакомиться с составом серверной части типовой биллинговой системы локальной сети на примере CakeBilling, назначением и функциями ее основных компонент, рассмотренных в разд. 2.

3.3.3. Изучить структуру учебной мультисервисной сети, в которую интегрирована биллинговая система CakeBilling по описанию, представленному в п. 3.2.1.

3.3.4. Ознакомиться с назначением и характеристиками телекоммуникационного, серверного и компьютерного оборудования, используемого биллинговой системой CakeBilling.

3.3.5. При необходимости произвести установку на биллинг-сервер и конфигурирование ОС Debian 4.0-r3 (см. приложение), а также необходимых компонент биллинговой системы CakeBilling (см. разд. 2).

3.3.6. Изучить пользовательский интерфейс клиентской части биллинговой системы CakeBilling.

3.3.7. Изучить пользовательский интерфейс серверной части биллинговой системы CakeBilling.

3.4. Порядок выполнения и методические указания

3.4.1. Создание клиентской учетной записи в биллинговой системе CakeBilling.

3.4.1.1. Зайти на биллинг-сервер под администратором. Для этого необходимо запустить веб-браузер, ввести в адресной строке адрес биллинг-сервера «<http://192.168.1.1:8080/cake>», в диалоговом окне «Вход в систему статистики» необходимо ввести имя администратора и пароль «studentadmin» (их конкретные значения следует уточнить у преподавателя, ведущего лабораторные занятия).

3.4.1.2. В диалоговом окне биллинговой системы выбрать вкладку «Пользователи».

3.4.1.3. В диалоговом окне «Карточка пользователя» удалить все лишние учетные записи пользователей, кроме учетной записи администратора.

3.4.1.4. В диалоговом окне «Карточка пользователя» добавить пользователя и ввести персональные данные, пароль доступа к персональному счету, тарифный план и алгоритм биллинг-управления трафиком при отрицательном балансе. В качестве имени пользователя использовать номер зачетной книжки, в качестве пароля – номер по порядку в списке студентов в лабораторном журнале.

3.4.1.5. Ввести новый платеж, зачислив на счет абонента 10 условных рублей.

3.4.1.6. Повторить подпункты 3.4.1.4 и 3.4.1.5 для всех новых пользователей.

3.4.2. Настройка VPN-подключения к биллинговой системе CakeBilling.

3.4.2.1. На клиентском компьютере открыть диалоговое окно «Мастер новых подключений», как описано в подпункте 3.2.2.3.

3.4.2.2. В диалоговом окне «Тип сетевого подключения» выбрать опцию «Подключить к сети на рабочем месте».

3.4.2.3. В диалоговом окне «Сетевое подключение» выбрать опцию «Подключение к виртуальной частной сети».

3.4.2.4. В диалоговом окне «Имя подключения» ввести имя подключения, например «student».

3.4.2.5. В диалоговом окне «Публичная сеть» выбрать опцию «Не набирать номер для предварительного подключения».

3.4.2.6. В диалоговом окне «Выбор VPN-сервера» ввести IP-адрес биллинг-сервера (его конкретное значение следует уточнить у преподавателя, ведущего лабораторные занятия).

3.4.3. Доступ клиента к персональной учетной записи в биллинговой системе CakeBilling.

3.4.3.1. Настроить параметры созданного в п. 3.4.2 VPN-подключения, используя кнопку «Свойства» диалогового окна «Подключение», как описано в подпункте 3.2.2.3.

3.4.3.2. Для доступа к персональной статистике ввести в диалоговом окне «Вход в систему статистики» имя пользователя и пароль, заданные в п. 3.4.1.

3.4.3.3. В диалоговом окне «Персональная статистика пользователя» проверить наличие на счете абонента заданного количества условных рублей.

3.4.4. Создание тарифных планов в биллинговой системе CakeBilling.

3.4.4.1. Используя права администратора, выйти на биллинг-сервер, как описано в подпункте 3.4.1.1.

3.4.4.2. В диалоговом окне биллинговой системы выбрать вкладку «Тарифы».

3.4.4.3. В диалоговом окне «Управление тарифами» назначить тарифы.

3.4.5. Биллинг-управление трафиком мультисервисной сети.

3.4.5.1. Скачать на клиентский компьютер информацию с какого-либо сетевого ресурса, размещенного за пределами локальной сети (за биллинг-сервером). Адрес сетевого ресурса следует уточнить у преподавателя, ведущего лабораторные занятия).

3.4.5.2. Получить доступ к персональной статистике, как описано в п. 3.4.3, и установить причину окончания процесса скачивания информации (окончание файла или обнуление счета).

3.4.5.3. Выполнять подпункт 3.4.5.2 до тех пор, пока не обнулится баланс. При необходимости изменить тарифный план, как описано в п. 3.4.4.

3.4.5.4. Убедиться в блокировке трафика пользователя, предприняв попытку скачивания информации с внешнего сетевого ресурса. Если при регистрации пользователя в биллинговой системе не была активирована опция «Блокировать доступ в Интернет при отрицательном балансе», убедиться в увеличении отрицательного баланса при скачивании информации с внешнего сетевого ресурса.

3.4.5.5. Используя права администратора, пополнить баланс клиента, как описано в п. 3.4.1.

3.4.5.6. Используя доступ к персональной клиентской статистике, как описано в п. 3.4.3, убедиться в пополнении клиентского счета и восстановлении возможности скачивания информации, если она была заблокирована биллинговой системой при обнулении баланса.

3.4.6. Оформить отчет по пп. 3.4.1 – 3.4.5 лабораторной работы, включив в него также структурную схему учебной мультисервисной сети, структуру биллинговой системы CakeBilling и параметры ее настройки.

3.5. Контрольные вопросы

1. Каковы задачи биллинговой системы?
2. Общая структура типовой биллинговой системы.
3. Каковы функции биллинговой системы?
4. Состав биллинговой системы CakeBilling.
5. Функциональное назначение FreeRADIUS-сервера.
6. Функции протокола PPP и службы PPTP в биллинговой системе CakeBilling.
7. Функциональное назначение СУБД PostgreSQL и PostgreSQL JDBC драйвера в биллинговой системе CakeBilling.
8. Задачи, решаемые в биллинговой системе CakeBilling комплектом разработчика JDK и Java servlets/JSP.
9. Каково место биллинговой системы CakeBilling в структуре учебной мультисервисной сети?
10. Каковы функции клиентской части биллинговой системы CakeBilling?
11. Каковы функции серверной части биллинговой системы CakeBilling?
12. Каким образом создается новая учетная запись пользователя в биллинговой системе CakeBilling?
13. Как настраивается VPN-подключение к биллинговой системе CakeBilling?
14. Что обеспечивает функция доступа клиента к персональной учетной записи в биллинговой системе CakeBilling?
15. Каким образом задаются тарифы в биллинговой системе CakeBilling?
16. Что происходит при обнулении счета клиента в биллинговой системе CakeBilling?
17. Каким образом зачисляются денежные средства на персональный счет клиента в биллинговой системе CakeBilling?

Литература

1. Хоменок, М. Ю. Трехмерная модель системы управления сетями телекоммуникаций Республики Беларусь. Структурированный анализ / М. Ю. Хоменок, В. Ю. Цветков // Известия Белорусской инженерной академии. Современные средства связи. – 2001. – №1 (11)/1. – С. 44 – 49.
2. Хоменок, М. Ю. Функциональная структуризация областей управления логической модели TMN / М. Ю. Хоменок, В. Ю. Цветков // Известия Белорусской инженерной академии. Современные средства связи. – 2002. – №2 (14)/1. – С. 34 – 36.
3. Принципы разработки биллинговой системы [Электронный ресурс]. – 2009. – Режим доступа: http://www.citforum.ru/operating_systems/linux/billing. – Дата доступа: 03.02.2009.
4. Информация о проекте бесплатного биллинга для малых сетей [Электронный ресурс]. – 2009. – Режим доступа: <http://code.google.com/p/cakebilling>. – Дата доступа: 03.02.2009.
5. Debian – универсальная операционная система [Электронный ресурс]. – 2009. – Режим доступа: <http://www.debian.org>. – Дата доступа: 03.02.2009.

Порядок установки и конфигурирования операционной системы Debian 4.0-r3

Компоненты биллинговой системы работают поверх операционной системы Debian 4.0-r3. Для ее инсталляции на сервер необходимо выполнить следующие шаги.

1. Подключить в ps/2 разъёмы компьютера (сервера) клавиатуру и мышь. Подключить кабель питания. Включить кабель питания в сеть и нажать кнопку пуск, включающую компьютер. Вставить первый (единственный) установочный диск в CD-ROM. После загрузки BIOS произойдёт запуск компьютера с установочного диска.

2. На экране монитора появится приглашение к установке «Press F1 for help, or enter to boot».

Необходимо нажать кнопку Enter на клавиатуре.

3. На экране монитора появится окно «[!] Choose the language» с текстом: «Please choose the language used for the installation process. This language will be the default language for the final system. This list is restricted to languages that can currently be displayed. Choose a language:»

Из предложенного списка языков следует выбрать English и нажать кнопку Enter на клавиатуре.

4. Текст в окне поменяется на

«Based on your language, you are probably located in one of these countries or regions. Choose a country, territory or area:»

Следует выбрать «other» и нажать клавишу Enter на клавиатуре. Затем необходимо найти «Europe», выбрать «Belarus» и нажать кнопку Enter на клавиатуре.

5. На экране монитора появится окно с текстом:

«Choose language. Based on your language and country chooses, following locale parameters are supported. Choose a locale:»

Следует выбрать «en_US.UTF-8» и нажать кнопку Enter на клавиатуре.

6. На экране монитора появится окно с текстом:

«You may choose additional locales to be installed from this list. Choose other locales to be supported».

Необходимо найти «ru_Ru.UTF-8» и нажать кнопку «пробел» на клавиатуре, чтобы выбрать эту позицию. Также необходимо найти «ru_RU.KOI8-R, ru_RU.cp1251, ru_RU» и нажать пробел, чтобы выбрать эти позиции.

Далее следует нажать кнопку tab на клавиатуре, выбрать стрелками «continue» и нажать Enter на клавиатуре.

7. На экране монитора появится окно с названием «[!] Select keyboard layout» и текстом:

«keymap to use».

Следует выбрать «American English» и нажать кнопку Enter на клавиатуре.

8. На экране монитора появится окно с последовательно меняющимся текстом:

«Detecting hardware to find CD-ROM Drivers»,

«Scanning CD-ROM»,

«Loading additional components»,

«Detecting network hardware»,

«Configuring the network with DHCP».

Затем появится окно с названием «[!] Configuring the network» и текстом:

«Network auto configuration failed. Your network is probably not using the server DHCP protocol. Alternatively, the DHCP is not working properly».

Необходимо нажать кнопку Enter на клавиатуре.

9. На экране монитора появится окно с текстом:

«From here you can choose to retry DHCP network auto configuration (which may succeed if your DHCP server takes long time to respond) or to configure the network manually. Some DHCP servers require a DHCP hostname to be sent by the client, so you can also choose to retry DHCP network auto configuration with a hostname that you provide.

Network configuration method:»

Следует выбрать «Configure network manually» и нажать кнопку Enter на клавиатуре.

10. На экране монитора появится окно с текстом:

«The IP address is unique to your computer and consist of four numbers separated by periods. If you don't know what to use here, consult your network administrator.

IP address:»

Следует ввести IP-адрес, например «192.168.39.190», и нажать кнопку Enter на клавиатуре.

11. На экране монитора появится окно с текстом:

«The netmask is used to determine which machines are local to your network. Consult your network administrator if you do not know the value. The netmask should be entered as four numbers separated by periods.

Netmask:»

Следует ввести «255.255.255.0» и нажать кнопку Enter на клавиатуре.

12. На экране монитора появится окно с текстом:

«The gateway is an IP address (four numbers separated by periods) that indicated the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router, in that case, you can leave this blank. If you don't know the proper answer to this question, consult your network administrator.

Gateway:»

Следует ввести IP-адрес Gateway, например «192.168.39.2», и нажать кнопку Enter на клавиатуре.

13. На экране монитора появится окно с текстом:

«The name servers used to look up host names on the network. Please enter the IP addresses (not host names) of up to 3 name servers, separated by spaces. Do not use

commas. The first name server in the list will be the first to be queried. If you don't want to use any name server, just leave this field blank.

Name servers addresses:»

Следует ввести IP-адрес, например «192.168.39.1», и нажать кнопку пробел на клавиатуре, а затем IP-адрес «192.168.251.1» и нажать кнопку Enter на клавиатуре.

14. На экране монитора появится окно с текстом:

«Please enter the hostname for this system. The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:»

Следует ввести «repository» и нажать кнопку Enter на клавиатуре.

15. На экране монитора появится окно с текстом:

«The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:»

Следует нажать кнопку Enter на клавиатуре.

16. На экране монитора появится окно с последовательно меняющимся текстом:

«Detecting disks and all other hardware».

«Stating up the partitioner».

«The installer can guide you through partitioning a disk (using different standard schemes) or if you preffer, you can do it manually. With guided partitioning you will still have a chance later to review and customize the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.»

Следует выбрать с помощью стрелок на клавиатуре «Guided – use entire disk» и нажать кнопку Enter на клавиатуре.

17. На экране монитора появится окно с текстом:

«Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:»

Из списка:

«SCSI2 (0,0,0)	(sda) – 9,1 GB	IBM DDRS-39130W	
SCSI2 (0,1,0)	(sdb) – 9,1 GB	IBM-PSG ST39175LC	!#
SCSI2 (0,2,0)	(sdc) – 9,1 GB	IBM-PSG ST39175LC	!#
SCSI2 (0,3,0)	(sdd) – 9,1 GB	IBM DDRS-39130W»	

необходимо выбрать с помощью стрелок на клавиатуре «SCSI2 (0,0,0) (sda) – 9,1 GB IBM DDRS-39130W» и нажать кнопку Enter на клавиатуре.

18. На экране монитора появится окно с текстом:

«Selected for partitioning:

SCSI2 (0,0,0) (sda) – IBM DDRS-39130W: are 9,1 GB

The disk can be partitioned using several different schemes. If you are unsure, choose first one.

Partitioning scheme:»

Следует выбрать с помощью стрелок на клавиатуре «All files in one partition (recommended for new users)» и нажать кнопку Enter на клавиатуре.

19. На экране монитора появится окно с текстом:

«This is an overview of your currently configured partitions and mount points. Select a partition to modify it's settings (file system, mount point, etc.), a free space create partitions, or a device to initialize it's partition table.

SCSI2 (0,1,0) (sdb) – 9,1 GB IBM-PSG ST39175LC»

Следует выбрать с помощью стрелок на клавиатуре «pri/log 9,1 GB Free space» и нажать кнопку Enter на клавиатуре. Далее необходимо выбрать с помощью стрелок на клавиатуре «create a new partition» и нажать кнопку Enter на клавиатуре.

20. На экране монитора появится окно с текстом:

«The maximum size you can use is 9,1 GB. Hint: use «20%» (or «30%», etc.) of the available free space for partition. Use «max» as a shortcut for the max allowed size.

New partition size:»

С помощью стрелок на клавиатуре необходимо выбрать последовательно следующие опции, нажимая кнопку Enter на клавиатуре.

«9,1 GB»,

«Logical»,

«mount point»,

«/opt – add a application software packages»,

«Done setting up the partition»,

«SCSI2 (0,2,0) (sdc) – 9,1 GB IBM-PSG ST39175LC»,

«pri/log 9,1 GB Free space»,

«Create»,

"9,1 GB»,

«Logical»,

«mount point»,

«/usr – static data»,

«Done»,

«SCSI2 (0,3,0) (sdd) – 9,1 GB IBM DDRS-39130W»,

«pri/log 9,1 GB Free space»,

«Create»,

«9,1 GB»,

«Logical»,

«mount point»,

«/tmp – temporary files»,

«Finish partitioning and write changes to disk»,

«Set up users and passwords».

21. На экране монитора появится окно «[!] Set up users and passwords» с текстом:

«You need to set a password for root: the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word they could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals. Note that you will not be able to see the password as you type it.

Root password».

Необходимо ввести пароль администратора, например «siutroot», и нажать Enter.

22. На экране монитора появится окно с текстом:

«Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:»

Необходимо ввести пароль повторно, например «siutroot», и нажать Enter.

23. На экране монитора появится окно с текстом:

«A user account will be created for you to use instead of the root account for non-administrative activity.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user real name. Your full name is a reasonable choice.

Full name for the new user:»

Следует ввести имя пользователя, например «siutuser», и нажать клавишу Enter.

24. На экране монитора появится окно с текстом:

«Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower case letter, which can be followed by any combination of numbers and more lower-case letters.

Username for your account:

Следует ввести имя пользователя, например «siutuser», и нажать клавишу Enter.

25. На экране монитора появится окно с текстом:

«A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user siutuser. Password:

Следует ввести имя пользователя, например «siutuserpass», и нажать клавишу Enter.

26. На экране монитора последовательно появятся окна «[!] Installing base system», «[!] Configuring APT».

Затем на экране монитора появится окно «[!] Configuring the package manager» с текстом:

«A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer version of software available. If you are installing from a netinst CD and you choose not to use a mirror, you will end up with only a very minimal base system. Use a network mirror?»

Следует выбрать «no» и нажать Enter.

27. На экране монитора появится окно «Scanning the security updates repository...».

Далее на экране монитора появится окно «[!] Configure the package manager» с текстом:

«Cannot access security updates. The security updates on security.debian.org couldn't be accessed, so those updates will not be made available to you at this time. You should investigate this later. Commented out entries for security.debian.org have been added to the /etc/apt/sources.list file.»

Следует выбрать «continue» и нажать Enter.

28. На экране монитора появится окно «Select and install software».

Далее на экране монитора появится окно «[!] Configuring popularity-contest» с текстом:

«The system may anonymously supply the distribution developers by with statistics about the most used packages on this system. This information influence decisions such as which packages should go on the first distribution CD.

If you choose to participate, the automatic submission script will run once every week, sending statistics to the distribution developers. The collected statistics can be viewed on <http://popcon.debian.org>.

This choice can be later modified by running «dpkg-reconfigure popularity-contest.

Participate in the package usage survey!»

Необходимо выбрать «No» и нажать Enter.

29. На экране монитора появится окно «[!] Software selection» с текстом:

«At the moment only the core of the system is installed. To tune the system to your needs you can choose to install one or more of the following predefined collections of software.

Choose software to install:»

С помощью клавиши «пробел» необходимо выбрать «Desktop environment» и «Base system» и нажать Enter.

30. На экране монитора появится окно «[!] Install Grub boot loader on a hard disk».

Следует выбрать «Yes» и нажать Enter.

31. На экране монитора появится окно «[!] Configuring X server-xorg» с текстом:

«Please keep only the resolutions you would like the X server to use. Removing all of them is the same as removing none since in both cases the X server will attempt to use the highest possible resolution.

Video modes to be used by the X server:»

С помощью клавиши «пробел» необходимо выбрать «640x480», «800x600», «1024x768» и нажать Enter.

32. На экране монитора появится окно «Finishing the installation» с текстом: «Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation.»

Следует извлечь диск из CD-ROM, выбрать «continue» и нажать кнопку Enter на клавиатуре.

Инсталляция операционной системы Debian 4.0-r3 завершена.

Библиотека БГУИР

Учебное издание

**Цветков Виктор Юрьевич
Смирнов Юрий Вячеславович
Кулешевский Антон Николаевич**

**БИЛЛИНГ-УПРАВЛЕНИЕ ТРАФИКОМ
МУЛЬТИСЕРВИСНОЙ СЕТИ**

Методическое пособие
по курсу
«Документальные службы и терминальные устройства телекоммуникаций»
для студентов специальности
«Сети телекоммуникаций»
всех форм обучения

Редактор Н. В. Гриневич
Корректор Е. Н. Батурчик
Компьютерная верстка Ю. Ч. Ключкевич

Подписано в печать 25.02.2011.
Гарнитура «Таймс».
Уч.-изд. л. 2,1.

Формат 60x84 1/16
Отпечатано на ризографе.
Тираж 50 экз.

Бумага офсетная.
Усл. печ. л. 3,14.
Заказ 319.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6