



NetUP.ru
UP YOUR NETWORK

УТМ

биллинговая система

РУКОВОДСТВО АДМИНИСТРАТОРА

© Компания NetUP, 2001–2006.

Версия документа 2.1 от 18 сентября 2006 г. для УТМ 5.2.1-001 и выше. Наиболее свежую версию документации можно найти на сайте <http://www.netup.ru>.

Все упомянутые торговые марки являются собственностью их соответствующих владельцев.

Содержание

Руководство по установке. Общее описание

NetUP UTM версия 5.0. Лицензионное соглашение	10
Описание системы.....	13
Основные функции системы	13
Способы включения системы в сеть.....	14
Структура системы UTM	16
Ядро биллинговой системы	17
Разграничение прав	19
UTM Remote Function Access (URFA).....	19
Установка и первоначальная настройка системы.....	21
Краткая последовательность шагов при установке и настройке системы.....	21
Установка серверной части.....	22
Запуск интерфейса администратора	29
Перенос данных из предыдущих версий UTM, либо из других баз данных.....	29
Быстрый старт	31
Предварительная настройка системы.....	31
Настройка тарификации.....	33
Настройка пользователей	37
Работа с учётными записями пользователей	41
Пользователи и группы	41
Системные пользователи и группы	43
Тарификация.....	46
Подключение услуг.....	46
Удаление услуги.....	47
Разовые услуги.....	47
Периодические услуги	47
Услуга передачи IP-трафика	48
Группы IP-адресов	59
Временные диапазоны.....	59
Услуги коммутируемого доступа и хотспот.....	59

Тарификация IP-трафика при динамическом распределении IP-адресов	61
Расчетные периоды	62
Предоплата	63
Налоговые ставки	64
Валюты	64
Телефонные направления	65
Телефонные зоны	65
Методы платежей	67
Тарифные планы	67
Краткое описание таблиц базы данных, отвечающих за тарификацию	70
 ПЛАТЕЖИ	 73
Поддержка нескольких валют	73
Персональные настройки валюты абонента	73
Ввод платежей	76
Откат платежа	80
 Отчёты	 81
Основной отчёт	81
Отчёт по трафику	81
Графический отчёт по трафику	82
Детальный отчёт по трафику	82
Отчёт по услугам	83
Отчёты по модемным сессиям, VPN и телефонии	83
Отчёт по платежам	84
Отчёт по блокировкам	84
 Настройки	 86
Список параметров	86
Конфигурационный файл ядра	92
Конфигурационный файл веб-интерфейса пользователя	95
Список брандмауэров	96
Правила файрволов	96
Список IP-зон	97
Список домов	97
Список банков	97
Настройка и отладка работы с почтовым сервером	98

ИСПОЛЬЗОВАНИЕ ФАЙРВОЛОВ	100
Настройка политики безопасности файрвола в ОС Linux с ipchains и iptables	100
Включение поддержки файрвола в ОС FreeBSD	101
Настройка файрвола на маршрутизаторе Cisco	102
Использование NAT	105
Добавление правил файрвола в центре управления.....	110
 РАБОТА С ПРЕДОПЛАЧЕННЫМИ КАРТАМИ.....	115
 NETUP DATA STREAM ACCOUNTING DAEMON (NDSAD).....	118
Конфигурационный файл	121
 УНИВЕРСАЛЬНЫЕ СБОРЩИКИ СТАТИСТИКИ	127
Схема сбора статистики с использованием NetUP get_xyz.	127
Сбор статистики по протоколу IP-accounting с маршрутизатора Cisco	129
Сбор статистики по протоколу IP-accounting с коллектора ipscad	131
Сбор статистики по протоколу NetFlow с маршрутизатора Cisco	132
Сбор статистики по протоколу NetFlow с маршрутизатора Cisco в случае использования NAT.....	133
Универсальный сборщик статистики utm5_unif.....	137
 ВСПОМОГАТЕЛЬНЫЕ УТИЛИТЫ.....	141
Генератор статистики по протоколу NetFlow	141
Генератор статистики по протоколу RADIUS	142
Утилита для резервного копирования базы данных.....	144
Утилита для загрузки IP-сетей из файла.....	144
Утилита для сканирования ARP-таблицы	145
Утилита для связки IP-адрес / MAC-адрес	146
 ВЕРИФИКАТОР БАЗЫ ДАННЫХ	146
 ИМПОРТ ДАННЫХ ИЗ ДРУГИХ СИСТЕМ.....	148
Создание учётной записи абонента.....	148
Создание лицевого счёта.....	149
Создание родительской периодической услуги	149
Создание родительской услуги передачи IP-трафика.....	150
Создание тарифного плана с включёнными в него услугами.....	151
Создание расчётного периода.....	153

Привязка тарифного плана к лицевому счёту абонента	153
ПРЕДОСТАВЛЕНИЕ УСЛУГИ ХОТСПОТ	157
Конфигурация сервера DHCP	157
Настройка файрвола для FreeBSD	158
Настройка файрвола для Linux	160
Настройка веб-сервера Apache	160
Настройка услуги хотспот	161
ПРИЁМ ПЛАТЕЖЕЙ ЧЕРЕЗ ПЛАТЁЖНУЮ СИСТЕМУ «РАПИДА»	163
Подготовка системы.....	163
Проверка подписи на сообщениях	164
Настройки модуля utm5_garida_check	164
Проверка работоспособности	165
Формат файлов с информацией о платеже	167
СОВМЕСТНАЯ РАБОТА UTM И LDAP	169
Установка программного обеспечения	170
Настройка биллинговой системы.....	182
КОНТРОЛЬНЫЙ ПРИМЕР	184
РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ	188
Личный кабинет	188
Утилита utm5 wintray.....	189

Модуль коммутируемых и VPN-соединений

МОДУЛЬ КОММУТИРУЕМЫХ СОЕДИНЕНИЙ	193
ОПИСАНИЕ ПРОТОКОЛА RADIUS.....	194
НАСТРОЙКА СЕРВЕРА RADIUS.....	197
Файл конфигурации сервера RADIUS.....	197
НАСТРОЙКА VPN	201
Настройка сервера доступа (NAS)	204
Настройка компьютера клиента на работу с VPN.....	209
НАСТРОЙКА КОММУТИРУЕМОГО ДОСТУПА	213
Настройка сервера доступа (NAS)	219
Дополнительная информация.....	221

АВТОМАТИЧЕСКАЯ РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ.....	222
Гостевой доступ	222
Доступ с автоматической регистрацией.....	224

КОНТРОЛЬНЫЙ ПРИМЕР	227
--------------------------	-----

Модуль телефонии

Модуль IP-ТЕЛЕФОНИИ.....	233
Терминология.....	233

НАСТРОЙКА СЕРВЕРА	239
Установка и запуск H323 гейткипера.....	239

НАСТРОЙКА CISCO ATA-186	243
-------------------------------	-----

НАСТРОЙКА ШЛЮЗА VOIP НА БАЗЕ CISCO 26xx, 36xx, 53xx.....	244
--	-----

НАСТРОЙКА UTM	246
Создание направлений и зон	246
Создание услуги IP-телефонии	247
Механизм тарификации	250

НАСТРОЙКА СЕРВЕРА RADIUS.....	253
Настройка сервера tftp	253
Настройка шлюза VOIP при дебетной (карточной) системе оплаты	254

СОВМЕСТНАЯ РАБОТА ALTERTEKS PROXYSOFTSWITCH И UTM.....	256
Настройка ProxySoftSwitch	256
Настройка UTM	261
Настройка Cisco ATA-186	262
Тестовый звонок	262

КОНТРОЛЬНЫЙ ПРИМЕР	263
Подготовка сервера.....	263
Контрольные данные	263

Руководство по установке. Общее описание

NetUP UTM версия 5.0. Лицензионное соглашение

Настоящее лицензионное соглашение (далее «соглашение») является юридическим соглашением, заключаемым между вами (физическим или юридическим лицом, далее «пользователь») и ЗАО «НетАП» (далее «компания НетАП»), относительно указанного выше программного продукта компании НетАП, включающего в себя программное обеспечение, записанное на соответствующих носителях, любые печатные материалы и любую «встроенную» или «электронную» документацию (далее «продукт»).

1. Объем лицензии.

1.1. Единичный комплект продукта может быть использован для инсталляции только на одном компьютере.

1.2. Продукт считается используемым, если он загружен в оперативную память или записан на жестком диске, компакт диске или ином запоминающем устройстве определенного компьютера.

1.3. Пользователь имеет право на создание архивной копии, предназначенной исключительно для индивидуального использования в целях восстановления продукта, либо на перенесение продукта на жесткий диск при условии, что оригинальный экземпляр сохраняется исключительно в качестве резервного или архивного.

2. Компания НетАП или ее поставщики гарантируют замену некачественных оптических, магнитных или иных носителей, на которых поставляется продукт для инсталляции.

Права пользователя и услуги, обеспеченные гарантийными обязательствами, предоставляются только зарегистрированным пользователям.

Зарегистрированный пользователь получает дополнительные права на:

- техническую поддержку по электронной почте;

- расширение, замену модификаций продукта;
- получение скидок при переходе на новые версии продукта;
- регулярное информирование об изменениях, вносимых в продукт, о выпусках новых модификаций, о предоставлении новых услуг.

Гарантийное обслуживание и техническая поддержка продукта, находящегося у пользователя, осуществляется только в отношении зарегистрированных пользователей и только той модификации продукта, которая указана в регистрационной карте, являющейся приложением к настоящему соглашению. Регистрационная карта заполняется на сайте компании НетАП по адресу <http://www.netup.ru>.

3. Настоящая лицензия относится также к обновлениям и добавлениям исходного продукта, предоставляемым компанией НетАП, если иное не указано в документах, сопровождающих обновление или добавление.

4. Продукт разрешается переносить на другую рабочую станцию. Первоначальный пользователь продукта имеет право единовременной передачи его другому лицу. Такая передача должна включать все составные части: носители и печатные материалы, настоящее соглашение и сертификат подлинности, если таковой имеется. Запрещается предоставлять продукт в прокат, в аренду или во временное пользование.

5. Запрещается вскрывать технологию или декомпилировать продукт, за исключением тех случаев и только в той степени, когда это явно разрешено действующим законодательством, несмотря на наличие в лицензионном соглашении данного ограничения.

6. Компания НетАП вправе прекратить действие настоящего соглашения при несоблюдении пользователем его положений и условий. В этом случае пользователь обязан уничтожить все имеющиеся у него копии продукта и его составных частей.

7. Пользователь согласен с тем, что компания НетАП вправе собирать и использовать по своему усмотрению технические сведения, сообщаемые пользователем службе технической поддержки компании.

8. В наибольшей степени, допускаемой применимым законодательством, ни при каких обстоятельствах компания НетАП и её поставщики не несут ответственность за какой-либо особый, случайный, косвенный или опосредованный ущерб или убытки (включая, но не ограничиваясь только перечисленным: упущенную выгоду; утрату конфиденциальной или иной информации; убытки, вызванные перерывами в коммерческой или производственной деятельности; нанесение ущерба здоровью; нарушение неприкосновенности частной жизни; неисполнение любого обязательства, включая обязательство действовать добросовестно и с разумной осмотрительностью; убытки, вызванные небрежностью; любой иной ущерб и прочие убытки имущественного или иного характера), возникающие в связи с использованием или невозможностью использования продукта, оказанием или неоказанием услуг по поддержке или в иных случаях, предусмотренных или связанных с положениями данного лицензионного соглашения, даже в случае нарушения обязательства, возникновения гражданского правонарушения (включая небрежность), объективной (независящей от вины) ответственности за какой-либо ущерб, нарушения компанией НетАП или её поставщиками договорных или гарантийных обязательств, даже если компания НетАП или её поставщики были заранее извещены о возможности такого ущерба. Компания НетАП и её поставщики не несут ответственности и не имеют никаких обязательств в случае несанкционированного использования продукта, не предусмотренного настоящим соглашением.

9. Настоящее соглашение вступает в силу с момента установки продукта. Настоящее соглашение действует в течение неограниченного срока, за исключением случая передачи прав на использование продукта, предусмотренного п. 4 настоящего соглашения.

10. Все права собственности, авторские права на продукт и в отношении него принадлежат компании НетАП или её поставщикам. Данный продукт предоставляется в пользование («лицензируется»), а не продается.

11. Внедрение и техническая поддержка продукта осуществляются компанией НетАП на основании отдельно заключаемого договора с пользователем.

Описание системы

Основные функции системы

Биллинговая система (автоматизированная система расчётов, АСР) NetUP UTM является полноценным решением для организации автоматического расчёта операторов связи с абонентами за предоставляемые услуги. Базовый модуль системы поддерживает обшчёт выделенных линий. Помимо этого, система позволяет создавать и вести учёт как периодических, так и разовых услуг. При использовании дополнительных модулей система может обшчитывать услуги IP-телефонии, коммутируемого доступа с учётом стоимости времени и беспроводного доступа к сети (хотспот).

В систему заложен универсальный механизм сбора статистики потреблённого трафика, что позволяет одновременно обшчитывать неограниченное количество каналов связи, построенных на основе разнородных устройств.

АСР NetUP UTM поддерживает ведение справочника клиентов, справочника банков, справочника маршрутизаторов и брандмауэров, справочника зон IP-адресов, справочника подключённых домов, справочника предоставляемых услуг и других справочников.

Настоящая версия системы NetUP UTM создавалась с учётом опыта работы и пожеланий пользователей предыдущих версий программы. Так, в системе реализована функция клиента, как дилера оказываемых провайдером услуг. Для удобства работы программа администрирования выполнена в виде графического совместимого с любой платформой интерфейса, написанного на языке программирования Java.

Система полностью поддерживает работу с предоплаченными картами. Есть возможность экспорта сгенерированных карт во внешний файл формата XML. Система поставляется с поддержкой русского и английского языков, но при необходимости пользовательский и администраторский интерфейс системы можно перевести на любой язык. Система может работать с несколькими денежными единицами одновременно.

Систему можно использовать для генерирования бухгалтерских счетов и различных отчётов, ведения базы договоров. Для более удобной технической поддержки клиентов в системе имеется встроенная служба обмена сообщениями.

При необходимости система может блокировать доступ клиента к услугам, например, при исчерпании средств на личном счёте.

Пользовательский интерфейс системы построен на основе веб-технологий, что позволяет клиенту получать доступ к своему счёту, выпискам и статистике из любой точки мира с помощью любого браузера через интернет. Использование технологии XML и шаблонов при создании клиентского интерфейса позволяет администратору системы самостоятельно менять внешний вид интерфейса без ущерба его функциональности.

Использование в системе такого понятия, как «класс трафика» позволяет вести учёт трафика из разных сетей, например, разделение трафика на отечественный и зарубежный, пиринговый и локальный. Разделение классов трафика можно производить по самым различным признакам: сети источника и получателя, порты источника и получателя, тип службы (TOS), протокол, автономные системы источника и получателя, интерфейс маршрутизатора, через который проходит пакет и многое другое.

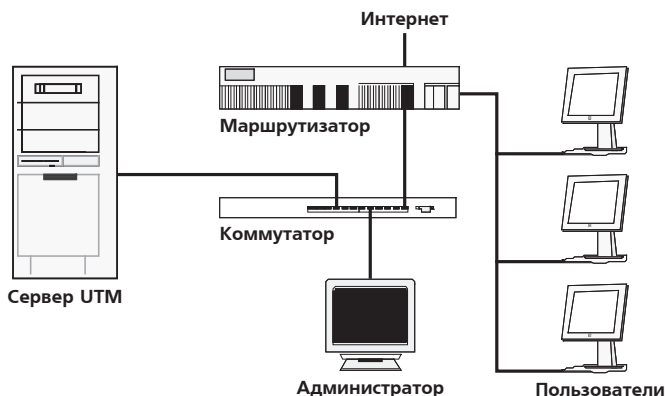
Серверная часть биллинга (ядро системы) представляет собой многопоточное оптимизированное приложение, обеспечивающее высокую производительность системы в целом. Это особенно актуально для сетей с большой клиентской базой и потребляющих большие объёмы трафика.

Способы включения системы в сеть

Универсальность биллинга допускает множество способов интеграции системы в существующую или планируемую инфраструктуру сети. ACP NetUP UTM поддерживает работу с множеством аппаратных и программных маршрутизаторов и не накладывает ограничения на количество одновременно обчитываемых каналов связи и тип используемых при организации этих каналов устройств. Рассмотрим основные варианты.

Локальная сеть подключена к интернету через аппаратный маршрутизатор, поддерживающий сбор статистики

Маршрутизаторы Cisco, Mikrotik, NSG, Revolution и других производителей, как правило, включают возможность экспорта статистики о переданном трафике. В этом случае сервер с биллингом может быть установлен как внутри локальной сети, так и вне неё (например, в головном офисе, доступном через интернет). Сбор статистики о трафике и управление маршрутизаторами производится удалённо.



Локальная сеть подключена к интернету через коммутатор или аппаратный маршрутизатор, не поддерживающий сбор статистики

В данном случае сервер устанавливается в сегмент локальной сети так, чтобы весь трафик, подлежащий учёту, был доступен серверу на уровне пакетов IP. Например, между коммутатором и локальной сетью включается концентратор (хаб), к порту которого подключается сервер. При работе сервер перехватывает все пакеты, идущие из локальной сети к коммутатору и обратно, анализирует их заголовки и обрабатывает полученную информацию.

Локальная сеть подключена к интернету через программный маршрутизатор (PC-роутер)

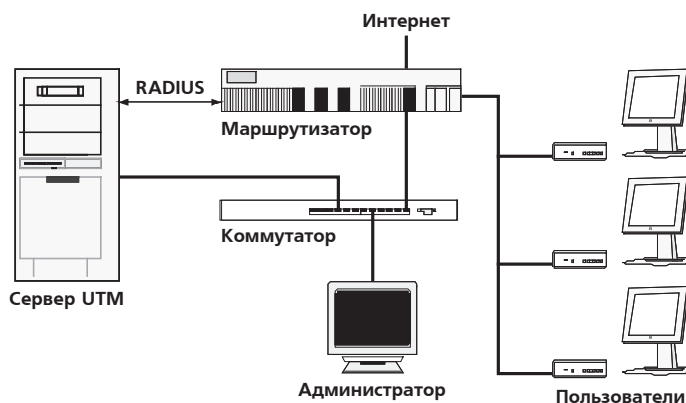
При таком способе подключения биллинговую систему можно установить как на самом роутере, так и на удалённом сервере. Статистика снимается с интерфейса роутера и обрабатывает-

ся на локальной машине (в первом случае) или передаётся по сети и обрабатывается на другом сервере (во втором случае).

Помимо описанных выше случаев подсчёта трафика локальных сетей возможно множество других вариантов, например, обсчёт спутниковых каналов, либо произвольная комбинация приведенных выше способов подключений.

Клиент подключается к интернету посредством коммутимого доступа

В данном случае сервером доступа может быть как Cisco, так и PC-роутер с подключёнными к нему модемами. Авторизация клиентов производится по протоколу RADIUS. Тарификация может производиться как по времени соединения, так и по объёму трафика клиентов.

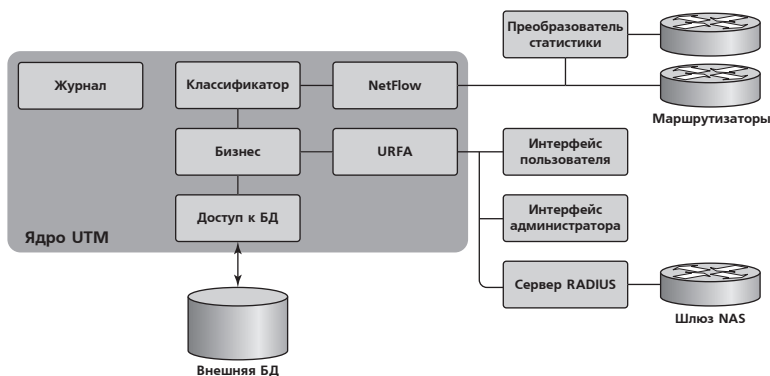


Клиент подключается к интернету по технологии Wi-Fi

Система поддерживает учёт услуг беспроводного доступа по технологии Wi-Fi, широко известных также как хотспот. Данный способ подключения часто используется в местах общественного доступа, например, гостиницы, кафе, аэропорты.

Структура системы UTM

Биллинговая система UTM представляет собой комплекс приложений, составляющий три группы: ядро системы, интер-



фейс администратора и интерфейс пользователя. Ядро системы — основная программа, запускаемая на сервере и отвечающая за функционирование биллинга в целом. Интерфейс администратора представляет собой Java-приложение, устанавливаемое на рабочую станцию администратора и позволяющее настраивать систему и управлять ею. Это приложение является платформенно-независимым и может исполняться под управлением любой ОС: Windows, Linux, FreeBSD. Интерфейс пользователя — это набор программ, работающих совместно с веб-сервером и реализующих виртуальный кабинет пользователя системы.

Ядро биллинговой системы

Ядро системы — это основной модуль, отвечающий за работу с базой данных, обеспечение доступа к ней и обработку входящей информации согласно внутренним правилам (таких как тарификация, периодические списания). Ядро — это отдельный многопоточный процесс, работающий в пользовательском режиме. При запуске ядро требует администраторских привилегий. Структура ядра такова, что оно органично вписывается в многопроцессорные архитектуры и при высоких нагрузках равномерно использует все предоставленные ресурсы.

Основные компоненты ядра

Обработчик запросов URFA (UTM Remote Function Access) является сервером вызовов удалённых процедур. Он принимает

соединения от клиентов системы и осуществляет выполнение запрошенных команд внутри ядра. Эта компонента служит в большей степени для организации пользовательских и администраторских интерфейсов.

Буфер NetFlow принимает данные о трафике в формате NetFlow версии 5. Для устройств, не поддерживающих выдачу статистики по этому протоколу, необходимо воспользоваться преобразователем статистики из любого протокола в NetFlow версии 5 – утилитой `get_xyz`.

Классификатор трафика – модуль ядра, осуществляющий сортировку всего трафика на категории (классы трафика) по признакам, обозначенным в настройках системы. Признаки классификации задаются в центре управления UTM.

Модуль бизнес-логики отвечает за тарификацию всех услуг, в том числе и передачу IP-трафика. Он осуществляет перевод количества оказанных оператором услуг в денежный эквивалент, принимая во внимание все зависимости, указанные администратором системы.

Системный журнал сообщений ведёт все записи о функционировании UTM. Он позволяет администраторам проводить диагностику системы и получать информацию о сбоях в работе системы.

Модуль доступа к базам данных представляет собой унифицированный интерфейс БД и осуществляет перевод внутрисистемных запросов к данным в запросы к внешней базе данных. Это позволяет добиться независимости UTM от какой-либо конкретной системы управления БД.

Прием данных происходит посредством буфера NetFlow и URFA. Исходные данные считываются из базы данных при запуске. Изменения, сделанные впоследствии напрямую в базу, могут привести к неконтролируемому поведению системы.

NetFlow данные поступают на обработку в бизнес-модуль, где рассчитываются все необходимые списания. В случае высокой пиковой загрузки NetFlow поток может быть буферизован, что несколько снизит возможные потери. «Сырые» данные

NetFlow сохраняются посредством объектно-ориентированной базы данных GigaBase (<http://www.garret.ru/~knizhnik/gigabase.html>). При старте модуль этой БД создаётся в отдельной нити и, по возможности, с высоким приоритетом.

URFA поддерживает динамическую загрузку модулей (`liburfa`). Они могут быть как выгружаемыми, так и постоянными. Последние – это модули, содержащие критичные для управления системой вызовы или выгрузка которых может привести к сбоям. Первые – это, обычно, просто библиотеки вызовов. Загруженные в данный момент модули можно просмотреть в интерфейсе администратора во вкладке (Дополнительно | Плагины).

Разграничение прав

В системе пользователи делятся на две категории: пользователи (клиенты, абоненты) и администраторы (системные пользователи). В зависимости от типа пользователя, у него есть некоторый список разрешённых операций. Проверить список разрешённых пользователям операций можно в разделе (Дополнительно | Символы). Операции с идентификатором, большим 0x80000000, разрешены на исполнение только клиентам, остальные операции – только администраторам.

Разделение ролей администраторов происходит на основе системных групп, которым принадлежит администратор. Существует специальная группа с идентификатором 1 (`wheel`). Если системный пользователь в неё входит, то ему разрешено исполнение любых операций. Иначе права будут ограничены списком вызовов, разрешённых группам, в которых он состоит. Случаи вызова запрещённых операций заносятся в системный журнал ядра.

UTM Remote Function Access (URFA)

URFA – это модуль доступа к ядру системы из внешних приложений. Он проводит авторизацию пользователей по схеме SHAP и обеспечивает работу удалённого пользователя. Протокол поддерживает передачу данных и вызов функций. URFA проверяет, разрешён ли данному пользователю доступ к вызы-

ваемой функции и, если разрешён, пользователю позволяет начать обмен данными. В противном случае система дает отказ в доступе.

Каждой сессии выделяется 128-битный случайный идентификатор (SID), повторение которого исключается. Этот SID может быть использован повторно для открытия доступа. В случае сбоя при восстановлении сессии SID будет удален, и пользователь вновь будет вынужден ввести логин и пароль. SID привязывается к IP-адресу клиента и автоматически удаляется после некоторого времени простоя (см. переменную `web_session_timeout`). Восстановление сессии возможно лишь в случае, когда получен доступ с правами системного пользователя.

При открытии сессии создается таблица разрешенных вызовов, состоящая из списка символов, имевшихся на момент генерации в системе, и прав доступа к ним. Если после открытия сессии будет подгружен дополнительный модуль, то эти вызовы будут в числе запрещённых для пользователя. В таком случае, пользователю необходимо подключиться заново.

В случае, если в момент выгрузки модуля, кто-то работает с ним, операция выгрузки завершится неудачей. Однако все символы этого модуля будут помечены как удаленные и в дальнейшем все вызовы к ним не будут успешными. В тот момент, когда последняя ссылка на символы будет удалена (сессия закрыта), модуль можно окончательно выгрузить. Постоянные модули выгружать нельзя, при попытке их выгрузить будет возвращена ошибка и на работе модуля это никак не скажется.

В случае сбоя при проверке лицензий модуль не будет подгружен. Лицензии привязываются к двоичному коду модуля, что гарантирует пользователю то, что загруженный модуль действительно собран в компании NetUP и полностью отвечает требованиям безопасности и корректности работы. Однако это требует, чтобы при обновлении модуля была получена обновленная лицензия.

Установка и первоначальная настройка системы

Краткая последовательность шагов при установке и настройке системы

Установка и запуск

- Установите биллинговую систему на сервер согласно инструкции. Запустите программу `utm5_core`.
- Загрузите и установите на компьютер администратора виртуальную машину Java версии 2. Запустите программу `UTM_admin`.
- Смените пароли для системных пользователей `web`, `init` и `radius`.
- После смены паролей внесите соответствующие коррективы в файлы `/netup/utm5/web5.cfg` и `/netup/utm5/radius5.cfg`.

Настройка тарификации (в случае первой установки системы)

- Создайте в интерфейсе администратора нужные расчётные периоды.
- Создайте необходимые классы трафика, временные диапазоны в настройках тарификации.
- Выставьте курсы валют в системе. По умолчанию курс рубля к курсу внутренней единицы равен 1, т. е. баланс пользователей отображается в рублях. Измените этот курс, если хотите вести лицевые счета в других единицах.
- Создайте услуги, выставьте периоды их действия и стоимость.
- Приступайте к добавлению пользователей.

Конвертирование базы данных (в случае обновления системы)

Произведите преобразование базы данных предыдущей версии биллинга по инструкции. Необходимые параметры для тарификации будут перенесены из существующей БД.

Проверка корректности работы

- Настройте и запустите коллектор.
- Прокачав некоторое количество трафика в сторону заведённого в системе клиента, проверьте появление данных о прокачанном трафике в отчётах (детальный отчет по трафику, отчет по трафику).

Проверить корректность работы бизнес-модуля можно, проведя тест по контрольному примеру. Тест следует проводить непосредственно после установки системы.

Установка серверной части

Linux

На сервер должна быть установлена операционная система Linux (RedHat 9.0, либо любой другой дистрибутив) и дополнительные пакеты: веб-сервер Apache 1.3.x с поддержкой SSL и сервер баз данных MySQL 3.x, 4.x, либо PostgreSQL 7.x. Настоятельно рекомендуем использовать MySQL с поддержкой InnoDB, так как данное решение позволит существенно повысить надежность хранения целостности данных. Более подробная информация доступна на сайте разработчика <http://dev.mysql.com/doc/mysql/ru/InnoDB.html>.

Для установки необходимо выполнить команду:

```
rpm -i utm-5-0.i386.rpm
```

В результате будут созданы директории:

`/netup` – содержит основные рабочие файлы, файлы конфигурации, директорию для системного журнала.

`/usr/local/apache/cgi-bin/utm5` – веб-интерфейс пользователя.

`/usr/local/apache/htdocs/utm` – таблица стилей, скрипты.

Если у вашего веб-сервера другие пути, то следует переместить файлы в соответствующие директории.

Также будут скопированы скрипты запуска:

```
/etc/rc.d/init.d/utm5_core  
/etc/rc.d/init.d/ndsad
```

Для создания первоначальной базы данных выполните команды:

Для MySQL

```
mysqladmin create UTM5  
mysql UTM5 < /netup/utm5/UTM5_MYSQL.sql
```

Для Postgresql

```
createdb -U postgres UTM5  
psql -f /netup/utm5/UTM5_PG.sql -U postgres UTM5
```

Если все предыдущие команды были выполнены успешно, запустите ядро биллинговой системы командой

```
/etc/rc.d/init.d/utm5_core start
```

Для автоматического запуска ядра UTM при загрузке Linux выполните команды:

```
chkconfig --add utm5_core  
chkconfig utm5_core on
```

FreeBSD

На сервер должна быть установлена операционная система FreeBSD 4.x, 5.x, а также дополнительные пакеты: веб-сервер Apache 1.3.x с поддержкой SSL и сервер баз данных MySQL 3.x, 4.x, либо Postgresql 7.x. Настоятельно рекомендуем использовать MySQL с поддержкой InnoDB, так как данное решение позволит существенно повысить надежность хранения целостности данных. Более подробная информация доступна на сайте разработчика <http://dev.mysql.com/doc/mysql/ru/InnoDB.html>.

Для установки необходимо выполнить команду

```
pkg_add utm5.tgz
```

В результате будут созданы директории.

`/netup` – содержит основные рабочие файлы, файлы конфигурации, директорию для системного журнала.

`/usr/local/apache/cgi-bin/utm5` – веб-интерфейс пользователя.

`/usr/local/apache/htdocs/utm` – таблица стилей, скрипты.

Если у вашего веб-сервера другие пути, то следует переместить файлы в соответствующие директории.

Также будут скопированы скрипты запуска.

```
/usr/local/etc/rc.d/utm5_core.sh
```

```
/usr/local/etc/rc.d/ndsad.sh
```

Для создания первоначальной базы данных выполните команды.

Для MySQL.

```
mysqladmin create UTM5
```

```
mysql UTM5 < /netup/utm5/UTM5_MYSQL.sql
```

Для Postgresql.

```
createdb -U postgres UTM5
```

```
psql -f /netup/utm5/UTM5_PG.sql -U postgres UTM5
```

Если все предыдущие команды были выполнены успешно, запустите ядро биллинговой системы командой

```
/usr/local/etc/rc.d/utm5_core.sh start
```

Внимание: Под FreeBSD может появиться ошибка вида: `/usr/libexec/ld-elf.so.1: Shared object "libc.so.4" not found`. В этом случае понадобится установить библиотеки `comp4x`.

Solaris

На сервер должна быть установлена операционная система SUN Solaris 9 либо 10 на плат-форме SPARC. Требования к веб-серверу и базе данных аналогичны Linux и FreeBSD.

Для установки необходимо выполнить команды:

```
gzip -d utm-5-solaris9-sparc-demo.gz
```

```
pkgadd -d utm-5-solaris9-sparc
```

Для создания первоначальной базы данных выполните команды.

Для MySQL.

```
mysqladmin create UTM5
```

```
mysql UTM5 < /netup/utm5/UTM5_MYSQL.sql
```

Для Postgresql.

```
createdb -U postgres UTM5
```

```
psql -f /netup/utm5/UTM5_PG.sql -U postgres UTM5
```

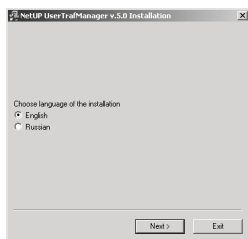
Если все предыдущие команды были выполнены успешно, запустите ядро биллинговой системы командой

```
/usr/local/etc/rc.d/utm5_core.sh start
```

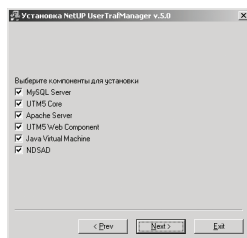
Windows

Запустите программу установки UTM UTM5Setup.exe.

После загрузки инсталлятора появится окно выбора языка для установки.



Выберите язык и нажмите кнопку «Next». Появится окно выбора компонентов для установки.

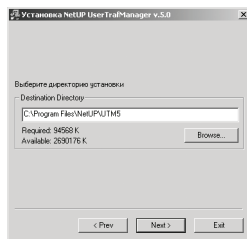


Если какие-либо компоненты уже были установлены ранее, уберите соответствующие галочки и нажмите «Next».

При обновлении UTM с предыдущего выпуска программы до более новой сборки или версии не требуется переустанавливать сервер баз данных MySQL. Поэтому в этом окне следует убрать галочку напротив MySQL, говоря, чтобы осталась текущая установка MySQL. Однако при обновлении до более новой версии UTM может измениться структура базы данных. Поэтому далее, когда программа установки спросит о том, нужно ли обновлять структуру базы данных, необходимо ответить утвердительно.

Если компонент «Java Virtual Machine» был выбран для установки, запустится его инсталлятор.

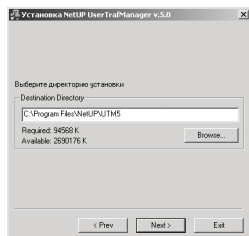
После этого будет запущена программа установки UTM. На экране появится текст лицензионного соглашения. Для успешной установки необходимо принять его, отметив галочку «I agree with the above terms and conditions» и нажав «Next». Если вы не согласны с лицензионным соглашением, нажмите «Exit», в этом случае установка программы будет прекращена.



Выберите директорию для установки UTM. Нажмите «Browse...», чтобы сменить директорию по умолчанию.

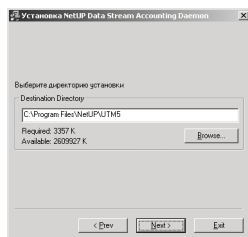
Будет запущена программа установки сервера баз данных MySQL.

После установки MySQL устанавливается служба сбора статистики. Появится окно выбора языка для установки.

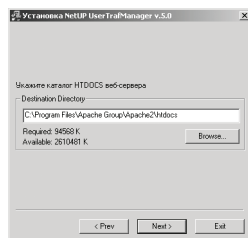


Выберите язык и нажмите «Next».

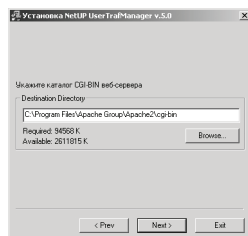
После этого будет запущена программа установки NetUP Data Stream Accounting Daemon. На экране появится текст лицензионного соглашения. Для успешной установки необходимо принять его, отметив галочку «I agree with the above terms and conditions» и нажав «Next». Если вы не согласны с лицензионным соглашением, нажмите «Exit», в этом случае установка программы будет прекращена.



Выберите директорию для установки службы статистики. Нажмите «Browse...», чтобы сменить директорию по умолчанию. Нажмите «Next».



Выберите директорию, которая является корневой для установленного веб-сервера Apache. Нажмите «Next».



На этом установка UTM завершена.

Серверная часть UTM устанавливается как системная служба Windows NT под названием `utm5_core`. Для её запуска можно выполнить команду

```
net start utm5_core
```

Для запуска серверной части UTM в режиме отладки (при этом вся информация выводится на экран вместо файлов протокола) нужно выбрать (Пуск | Программы | UserTrafManager 5.0 | UTM5 Core Debug Mode) или выполнить следующую команду:

```
C:\program files\NetUP\UTM5\utm5_core.exe -d
```

Для установки и удаления службы `utm5_core` нужно запустить `utm5_core.exe` с опциями `-install` или `-uninstall` соответственно:

```
C:\Program Files\NetUP\UTM5>utm5_core.exe --uninstall
```

```
Successfully deleted utm5_core service  
C:\Program Files\NetUP\UTM5>utm5_core.exe --install  
Successfully created utm5_core service
```

Активация лицензионного ключа

Для активации лицензионного ключа необходимо выполнить команду под Linux/FreeBSD/Solaris:

```
mysql UTM5 < reg.sql
```

В случае использования операционной системы Windows инсталляционный пакет автоматически запросит путь к директории где находится файл reg.sql.

Запуск интерфейса администратора

На рабочей станции администратора необходимо установить пакет Sun Java 2 (<http://www.sun.com/>), а затем запустить приложение UTM_Admin.jar. По умолчанию логин init и пароль init. После входа в систему рекомендуется изменить пароль для системных пользователей. После смены пароля на системного пользователя web, также укажите его в файле /netup/utm5/web5.cfg.

Для входа в виртуальный кабинет пользователя необходимо запустить интернет-браузер (например, Internet Explorer, Opera, Netscape Navigator, Konqueror) и набрать в адресной строке URL <https://your.server/cgi-bin/utm5/aaa5>.

Перенос данных из предыдущих версий UTM, либо из других баз данных

Для осуществления переноса данных об учетных записях пользователей, тарифах, списаниях служит утилита

```
/netup/utm5/to_utm.pl
```

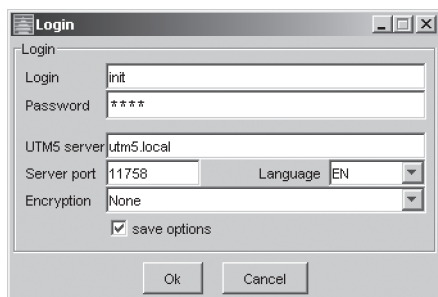
Утилита написана на языке perl и поставляется в исходном коде. Благодаря этому имеется возможность перенести дан-

ные практически из любой системы, исправив код скрипта согласно структуре базы данных, из которой осуществляется перенос.

Быстрый старт

Управление учётными записями и настройками биллинговой системы производится с помощью центра управления UTM. Для функционирования программы на компьютере администратора необходимо наличие операционной системы с поддержкой графической оболочки и установленной виртуальной машины Java версии 2.

Для начала работы необходимо запустить центр управления UTM (программа UTM_Admin.jar) и указать логин и пароль системного пользователя



Помимо этого указываются IP-адрес сервера и порт для подключения. Также можно указать опции шифрования. Настоятельно рекомендуется использовать шифрование. Если отмечена галочка «Сохранить параметры», то выбранные параметры (кроме пароля) сохраняются в конфигурационном файле и автоматически подставляются в форму при следующем запуске программы.

Предварительная настройка системы

Настройка валют

Все операции внутри системы производятся в условных единицах. Для правильной настройки работы с валютами выполните следующие шаги.

Зайдите в раздел (Тарификация | Валюта). Нажмите кнопку «Обновить». Появится список доступных валют.

Идентификатор валюты	Классификация валюты	Временные диапазоны	Расчётные периоды	Результаты
Валюта	Методы платёжей	Тарифные планы	Телефонные начисления	Телефонные звонки
Добавить Редактировать Обновить				
ID	Сокр. назв.	Название	Percent	
010	RUR	Russian Rouble	0.0	
040	USD	USA Dollar	0.0	
070	EUR	Euro	0.0	

Если валюта, с которой предполагается работать, отсутствует в списке, нажмите кнопку «Добавить».

Добавить валюту

Свойства валюты

ID валюты

756

Сокр. назв.

CHF

Название

Швейцарский франк

Курс

23.1249

Online update

Provider %

0

История изменения курса

Дата	Курс

OK

Отмена

В появившемся окне введите идентификатор, сокращённое название, полное название, курс и поправочный процент. После ввода данных нажмите кнопку «OK».

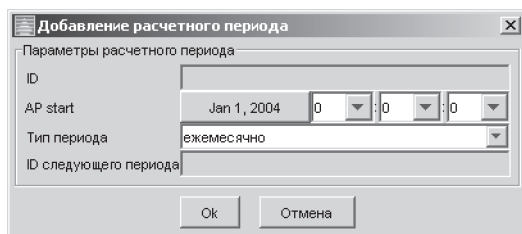
Повторите процедуру добавления новой валюты при необходимости добавить ещё одну или несколько валют.

После того, как все необходимые валюты добавлены в список, можно переходить к добавлению расчётных периодов.

Настройка расчётных периодов

Зайдите в раздел (Тарификация | Расчётные периоды). Нажмите кнопку «Обновить». Появится список доступных расчётных периодов.

Нажмите кнопку «Добавить» для добавления нового расчётного периода.



В появившемся окне выберите дату начала расчётного периода и его тип (ежедневный, еженедельный, ежемесячный, ежеквартальный, ежегодный). После ввода нажмите кнопку «ОК».

При необходимости добавить несколько расчётных периодов, повторите процедуру.

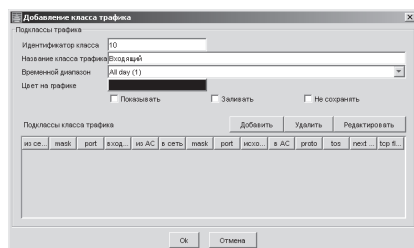
После добавления всех расчётных периодов можно переходить к созданию классов трафика.

Настройка тарификации

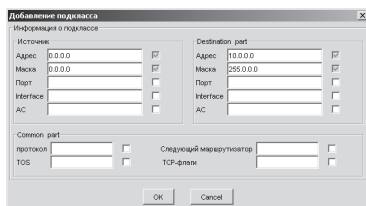
Настройка классов трафика

Зайдите в раздел (Тарификация | Классы трафика). Нажмите кнопку «Обновить». Появится список существующих классов трафика.

Нажмите кнопку «Добавить» для создания нового класса трафика. Введите идентификатор класса «10» и название «Входящий».



Нажмите кнопку «Добавить» над списком подклассов трафика.

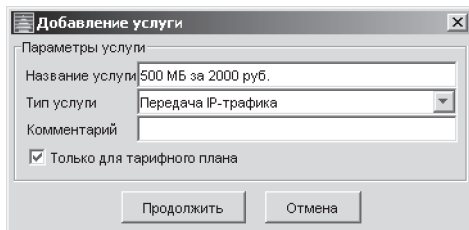


Введите IP-адреса и маски сетей для входящего трафика, нажмите «ОК». После добавления всех подклассов нажмите кнопку «ОК» в окне «Добавление класса трафика».

Повторите указанную последовательность действий и создайте классы трафика «Исходящий» с идентификатором «20» и «Локальный» с идентификатором «1000».

Настройка услуги IP-трафика

Зайдите в раздел (Тарификация | Услуги). Нажмите кнопку «Обновить». Появится список существующих услуг.



Нажмите кнопку «Добавить» для создания новой услуги.

В появившемся окне «Добавление услуги» введите название услуги и выберите её тип – «Передача IP-трафика». Отметьте галочку «Только для тарифного плана», если создаваемая услуга в дальнейшем будет частью пакета (тарифного плана). Кроме того, можно добавить комментарий, введя его в соответствующем поле. Нажмите кнопку «Продолжить».

Появится окно с дополнительными параметрами услуги. Введите размер периодической составляющей стоимости услуги и выберите способ её списания (в начале или в конце расчётного периода, либо плавное снятие в течение всего расчёт-

Добавление услуги IP-трафика

Параметры услуги IP-трафика

Название услуги: 500 MB за 2000 руб.

Комментарий:

Периодическая составляющая стоимости: 2000

Ввод снятия денег: в течение всего учетного периода

Дата начала: Ян 1, 2004 Выбрать

Дата окончания действия: Ян 1, 2007 Выбрать

Включать предоплаченный трафик: ☐ (Add service by default)

Границы: Добавить Удалить Редактировать

Класс трафика	Количество	Стоимость

Предоплаченные единицы: Добавить Удалить Group T-Classes Добавить Удалить

Класс трафика	Количество	Класс трафика	Операция

OK Отмена

ного периода). Обозначьте дату введения в действие услуги и дату окончания действия услуги.

Нажмите кнопку «Добавить» над списком границ.

Add border

Border parameters

Идентификатор класса: incoming

Количество: 0 ☒ HS

Стоимость: 5

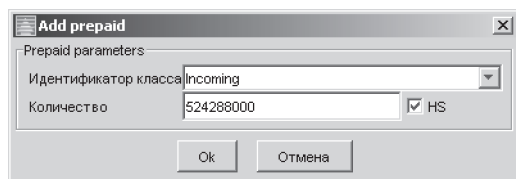
OK Отмена

В появившемся окне «Добавить границу» выберите класс трафика, для которого устанавливается граница, введите положение границы в байтах (0) и стоимость трафика при превышении границы в условных единицах за мегабайт. Нажмите кнопку «ОК».

Для добавления предоплаченного трафика в состав услуги нажмите кнопку «Добавить» над списком предоплаченных единиц в окне «Добавление услуги IP-трафика».

В появившемся окне «Добавление предоплаченных единиц» выберите класс предоплаченного трафика и введите количество в байтах. Нажмите кнопку «ОК».

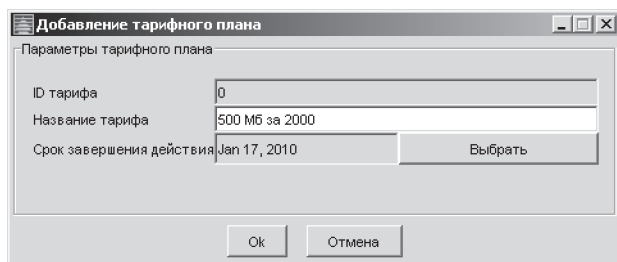
Нажмите кнопку «ОК» в окне «Добавление услуги IP-трафика». Если услуга не предназначалась для тарифного плана, то



она появится в списке доступных услуг. Иначе, если галочка «Только для тарифного плана» в самом начале была отмечена, то созданная услуга не появится в списке.

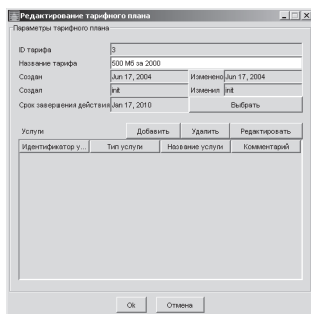
Настройка тарифных планов

Зайдите в раздел (Тарификация | Тарифные планы). Нажмите кнопку «Обновить». Появится список существующих та-

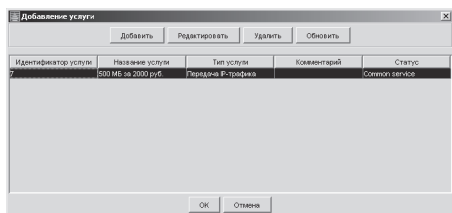


рифных планов. Нажмите кнопку «Добавить».

В появившемся окне «Добавление тарифного плана» введите название пакета и дату завершения действия плана. Нажмите «ОК». Вновь созданный тарифный план появится в списке доступных пакетов. Выделите его и нажмите кнопку «Редактировать».



Нажмите кнопку «Добавить» над списком услуг в окне «Редактирование тарифного плана».



В появившемся окне появится список услуг, созданных для тарифных планов. Выберите название услуги из списка и нажмите «ОК». Услуга появится в списке включённых в пакет услуг.

После добавления всех необходимых услуг в состав тарифного плана нажмите «ОК» в окне «Редактирование тарифного плана».

Настройка пользователей

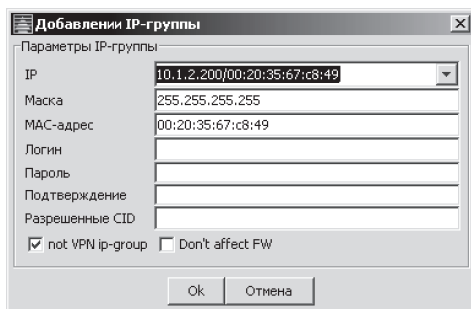
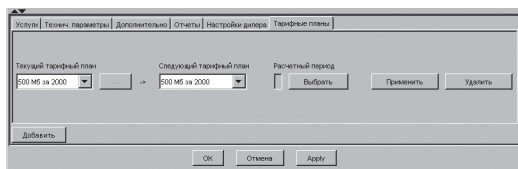
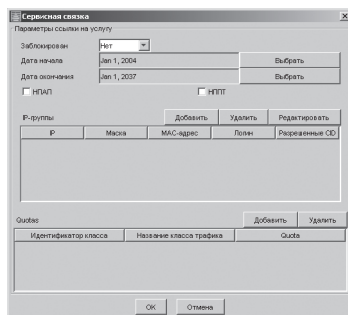
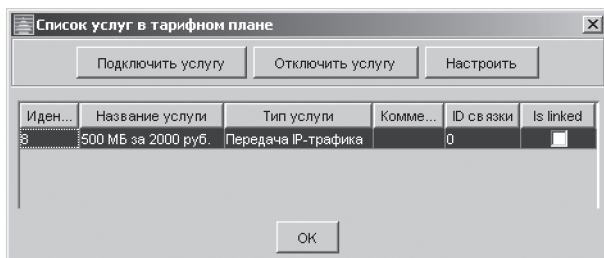
Зайдите в раздел (Пользователи и группы | Пользователи) и нажмите кнопку «Обновить». Появится список существующих пользователей. Нажмите кнопку «Добавить» для создания нового пользователя.

В окне «Добавление пользователя» введите логин пользователя, при необходимости – персональную информацию и нажмите «Применить». В нижней части окна появятся дополнительные вкладки.

ID	Дата начала	Дата окончания	Periodic type	ID следующего пер.	Длительность, с
1	Thu Jan 01 00:00:00	Wed May 10 07:33:21	daily	0	200000000
2	Thu Jan 01 00:00:00	Thu Jul 01 00:00:00	monthly	0	2500000

Выберите вкладку «Дополнительно» и нажмите кнопку «Обновить». В списке «Основная валюта» выберите валюту для

расчётных операций с данным пользователем. Нажмите кнопку «Сохранить».



Перейдите во вкладку «Тарифные планы» и нажмите кнопку «Добавить». Выберите текущий тарифный план и тарифный план следующего расчётного периода в появившихся выпадающих списках. Нажмите кнопку «Выбрать» в столбце «Расчётный период».

Выберите соответствующий расчётный период из появившегося списка и нажмите «ОК».

Нажмите кнопку «Применить». Выпадающее меню текущего тарифного плана станет неактивным, а кнопка «...» рядом – активной. Нажмите на эту кнопку.

В появившемся списке услуг, которые включены в тарифный план, выберите соответствующую услугу передачи IP-трафика и нажмите кнопку «Подключить услугу».

В появившемся окне «Сервисная связка» выберите даты начала и окончания подключения пользователя к услуге и нажмите кнопку добавить над списком IP-групп. Введите IP-адрес и маску сети, которые следует привязать к пользователю. Нажмите кнопку «ОК» сначала в окне «Добавление IP-группы», а потом, после добавления всех IP-адресов, в окне «Сервисная связка».

Нажмите кнопку «ОК» для закрытия списка услуг в тарифном плане.

Нажмите кнопку «ОК» ниже вкладок в окне «Добавление пользователя». Новый пользователь с установленными тарифным планом и параметрами будет создан.

Далее необходимо проконтролировать появление трафика в разделе «Отчёты».

Работа с учётными записями пользователей

Пользователи и группы

В сводном списке пользователей содержится основная информация о клиентах: полное имя, логин в системе, идентификатор пользователя, основной лицевой счёт, идентификатор расчётного периода, статус блокировки клиента и баланс его лицевого счёта.

Создание учётной записи пользователя

Создание новой учётной записи клиента осуществляется при помощи диалогового окна добавления пользователя. Обязательной информацией являются логин и пароль пользователя. При создании новой учётной записи пароль генерируется автоматически, но есть возможность его изменения. Одновременно с учётной записью, для пользователя заводится основной лицевой счёт.

После того, как учётная запись пользователя создана, можно приступить к добавлению услуг пользователю.

Удаление учётной записи пользователя

Перед удалением учётной записи пользователя из системы необходимо произвести ряд предварительных операций.

1. Удалить все подключенные услуги, не входящие в тарифные планы. Для этого следует зайти в раздел «Услуги» свойств пользователя и последовательно удалить все записи о подключенных услугах, не входящих в тарифные планы.

2. Удалить все подключенные услуги, входящие в тарифные планы. Для этого следует зайти в раздел «Тарифные планы» свойств пользователя, нажать кнопку «...» и в открывшемся окне последовательно удалить все подключенные услуги.

3. Удалить все подключенные тарифные планы. Для этого в разделе «Тарифные планы» свойств пользователя необходимо нажать кнопку «Удалить» напротив соответствующего подключенного тарифного плана.

В том случае, когда пользователю принадлежат несколько лицевых счетов, указанную выше последовательность действий нужно повторить для каждого лицевого счёта.

После удаления всех подключенных услуг и тарифных планов учётную запись можно удалить, выделив соответствующую строку в списке пользователей и нажав на кнопку «Удалить».

Контактные лица

Для каждого пользователя поддерживается список контактных лиц. Для каждого лица можно задать телефон, адрес электронной почты, личную информацию.

Памятка пользователя

Памятка пользователя содержит время и дату подключения, логин и пароль пользователя. Она предназначена для передачи пользователю при подключении или в любой другой момент.

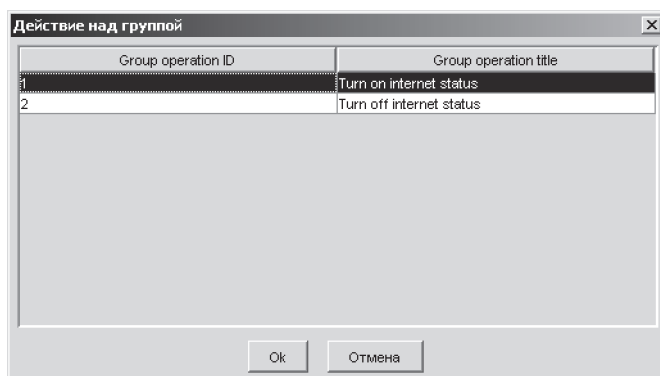
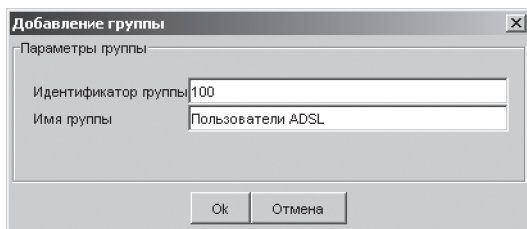
Дополнительные параметры

Каждому пользователю отдельно можно настроить валюту, в которой будут производиться все расчёты, и изменение курса валюты относительно заданного в системе.

Создание группы

Для создания группы нужно указать идентификатор группы и название группы. После того, как группа создана, можно добавлять пользователей в неё.

Над группами пользователей можно проводить групповые операции: включение и выключение доступа в сеть.



Также для групп пользователей можно задавать правила файрвола для блокирования доступа.

Системные пользователи и группы

Системные пользователи составляют отдельный класс пользователей, и только они имеют доступ к администрированию системы через центр управления UTM. Отличительной особенностью системных пользователей является то, что они имеют отрицательный идентификатор. Таким образом, обычный пользователь не может одновременно являться администратором и наоборот.

В системе три встроенных системных пользователя: init – учётная запись системного администратора; web – учётная запись, под которой программа пользовательского интерфейса осуществляет доступ к системе; radius – учётная запись, под которой входит в систему сервер RADIUS.

Как и обычных пользователей, системных пользователей можно объединять в группы. Для каждой группы системных пользователей настраивается политика безопасности. Политика безопасности – это набор прав на выполнение системных функций. С точки зрения политик безопасности, можно выделить следующие типовые группы системных пользователей: администраторы (полные права), кассиры (пополнение лицевых счетов пользователей), бухгалтеры (доступ к отчётам системы) и другие.

Если системный пользователь входит в состав нескольких системных групп, то действует правило добавления: пользователь имеет суммарные привилегии всех групп, членом которых он является.

Создание системной учётной записи

При создании системной учётной записи обязательными параметрами являются логин и пароль. Можно указать IP-адрес компьютера или подсеть, из которой разрешается доступ пользователю. Создаваемую учётную запись можно сразу включить в одну или несколько системных групп.

Добавление пользователя

Параметры системного пользователя

ID пользователя:

Логин:

Пароль:

IP:

Маска:

Системные группы

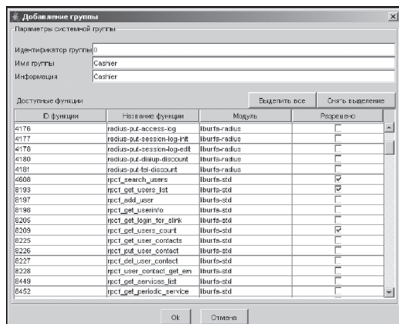
Идентификатор группы	Имя группы	Информация
2	Cashier	Cashier

Добавить Удалить

Ok Отмена

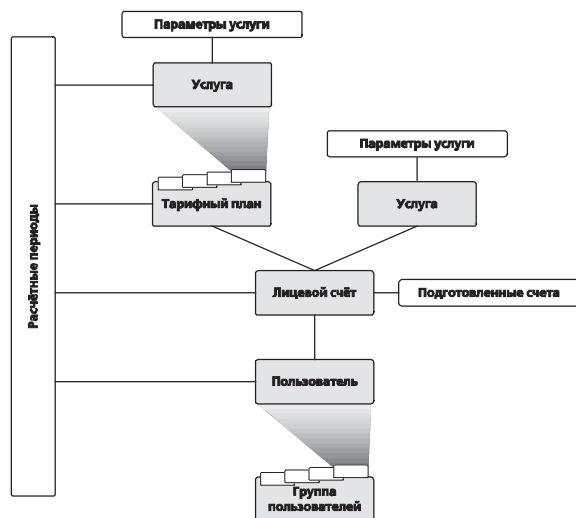
Создание системной группы

В UTM системные группы являются носителями прав на исполнение системных функций. При создании группы нужно указать, какие системные функции разрешены на исполнение её членам. Описание системных функций приведено в приложении «Системные функции».



Тарификация

В биллинговой системе предусмотрены следующие сущности.



Основным объектом служит пользователь, который идентифицируется большим количеством параметров, и к которому привязаны договора.

К пользователю привязан основной лицевой счёт. На счету хранится текущий баланс. При оказании услуг пользователю средства списываются с основного лицевого счёта. При приёме платежа от пользователя баланс лицевого счёта увеличивается. Все лицевые счета ведутся в условных единицах.

К лицевым счетам производится привязка услуг. Существуют несколько типов услуг: разовые услуги, периодические услуги, услуги передачи IP-трафика, услуги коммутируемого доступа, услуги хотспот и услуги телефонии. Каждая услуга имеет название и уникальный целочисленный идентификатор.

Подключение услуг

Подключенная услуга – это «сервисная связка». При подключении услуги создается запись в таблице `service_links` и в со-

ответствии с типом услуги записи в таблицах `periodic_service_links`, `iptraffic_service_links`, `hotspot_service_links`, `dialup_service_links`, `once_service_links`. Если услуга не разового типа, то также создается запись в таблице `periodic_service_links`.

Удаление услуги

Для того чтобы удалить услугу, необходимо произвести следующие действия.

1. Отключить все подключения этой услуги ко всем лицевым счетам.
2. В разделе (Тарификация | Услуги) выбрать нужную услугу (она должна иметь статус «обычная услуга») и нажать кнопку «Удалить».

Разовые услуги

Стоимость разовой услуги списывается с лицевого счёта абонента единовременно при оказании услуги.

Параметры разовой услуги	
Название	Установка оборудования
Комментарий	Приходит мастер и всё устанавливает
Стоимость	2000

Ok Отмена

Периодические услуги

Стоимость периодической услуги списывается с лицевого счёта абонента каждый учётный период: ежедневно, еженедельно, ежемесячно, ежеквартально или ежегодно. Средства могут сниматься как в начале или в конце учётного периода, так и плавно в течение всего учётного периода.

При этом расчётный период указывается при подключении услуги на пользователя. Кроме того, можно указать период актуальности услуги (дата начала оказания услуги предприяти-

Сервисная связка

Параметры ссылки на услугу

Заблесткован: Нет

Расчетный период: 3

Дата начала: 05.04.2004

Дата окончания: 05.04.2020

☒ НПДП ☒ ННПТ

IP-группы:

IP	Маска	MAC-адрес	Логин	Разрешенные CID
10.0.0.101	255.255.255.255			
192.168.0.109	255.255.255.255			
172.16.0.70	255.255.255.255		test	

ем и дата окончания оказания услуги). Предоставление услуги и списания за неё будут остановлены при наступлении срока окончания действия услуги.

Услуга передачи IP-трафика

В настройках услуги передачи IP-трафика в свойствах услуги указываются стоимость её периодической составляющей, количество предоплаченного трафика и стоимость трафика сверх предоплаченного. В стоимости трафика, составляющего превышение предоплаченных единиц, можно указать несколько диапазонов с различной стоимостью. Сначала добавляется граница с размером 0 и указывается стоимость – это стоимость трафика после исчерпания предоплаченного. После этого можно указать другую границу для того же класса трафика, например, 104 857 600 байт, которая будет указывать на стоимость трафика, потребленного после использования предоплаченного трафика плюс 104 857 600 байт.

Редактировать

Параметры услуги IP-трафика

Название услуги: Передача в услугу

Комментарий:

Периодическая составляющая стоимости: 0.0

Тип периода: Ежедневно

Метод отсчета: с начала учетного периода

Дата начала: 05.04.2004 0:00:00

Срок завершен действия: 05.04.2011 0:00:00

Объем трафика: ☒ Предоплаченный трафик

Границы:

Класс трафика	Количество	Стоимость
Входной	0	1.0
Входной	104857600	0.9
Входной	104857600	0.07

Предоплаченные единицы:

Класс трафика	Количество	Класс трафика	Описание
Входной	0	Входной	Итог
		Итог трафика	Итог

Неизрасходованный предоплаченный трафик переносится на следующий расчётный период, если не отмечена галочка «Обнулять предоплаченный трафик».

Если трафик предоплаченный, то его цена нулевая. Иначе, в зависимости от того, сколько клиент скачал в текущем расчётном периоде, определяется цена трафика.

Если предоплаченный трафик задан в виде границы, т. е. от 0 байт до определённого количества байт стоимость трафика равна 0 у. е. за 1 МБ, то трафик не будет перенесён на следующий расчётный период вне зависимости от того, превысил ли пользователь границу или нет.

Также имеется возможность списывать средства за превалярующий трафик. Для этого при добавлении услуги типа «Передача IP-трафика» необходимо классы трафика объединить в группу. При этом средства будут списываться только за тот класс трафика, которого пользователь потренил больше.

Класс трафика	Количество	Стоимость
Входящий	0	0.0
Входящий	104857600	0.0
Входящий	1048576000	0.07

Класс трафика	Количество
Входящий	0

При этом стоимость с границами и количество предоплаченного трафика указывается только для одного из классов трафика входящих в группу. Для остальных классов трафика входящих в группу стоимость будет такой же.

При указании границ стоимости для удобства ввода больших объемов можно использовать условные обозначения: К – килобайт, М – мегабайт, Г – гигабайт.

Чтобы данные обозначения корректно обработались системой, необходимо отметить галочку “HS”. Например, если в поле «Количество» ввести следующую строку:

1G 100M 100K

То система пересчитает данную строку в байты по следующей формуле:

$$1 * (1024^3) + 100 * (1024^2) + 100 * 1024 = 1178701824 \text{ байт.}$$

При этом количество байт в килобайте будет выбрано из параметра bytes_in_kbyte в разделе настройки. По умолчанию в килобайте 1024 байт. Соответственно в мегабайте 1024 во второй степени и в гигабайте 1024 в третьей степени.

При подключении услуги данного типа к лицевого счёту пользователя необходимо указать IP-адреса, назначенные пользователю (IP-группы). По ним будет происходить соотнесение трафика и пользователя при тарификации потока NetFlow.

Сервисная ссылка

Параметры ссылки на услугу

Забронирован: Нет

Расчетный период: 3

Дата начала: 06.04.2004

Дата окончания: 06.04.2020

☒ ННП

IP-группы	Маска	MAC-адрес	Логин	Разрешение CID
10.0.0.101	255.255.255.255			
192.168.0.109	255.255.255.255			
172.16.0.70	255.255.255.255		test	

Добавить Удалить Редактировать

OK Отмена

При этом если для IP-группы указаны логин и пароль, то эти данные будут автоматически переданы серверу RADIUS и по ним будет возможно установление VPN-соединения. В случае, если указано поле «Разрешённые CID», то при подключении пользователя по VPN либо Dial-up это значение будет сравниваться с атрибутом RADIUS Calling-Station-Id (31). Обычно в этом атрибуте записывается адрес вызывающей станции (компьютера клиента). В случае VPN это может быть IP-адрес, в случае PPPoE это может быть MAC-адрес, в случае Dial-up это может быть телефонный номер вызывающего абонента.

Ответственность за заполнение этого поля полностью лежит на сервере доступа. Если не будет найдено точного совпадения между значением, указанным в поле «Разрешённые CID» и тем, что указано в радиус атрибуте Calling-Station-Id, то авторизация не пройдёт и пользователь не сможет воспользоваться услугой.

Более подробную информацию о настройке серверов доступа можно найти в документации «Модуль коммутируемых и VPN-соединений».

При подключении услуги данного типа к лицевому счёту пользователя можно указать, каким образом списывать средства за периодическую составляющую услуги, а так же какой объем предоплаченного трафика предоставлять. Управление осуществляется галочками: ППТ – пересчитывать предоплаченный трафик и ПАП – пересчитывать абонентскую плату.

Примеры

1. Если не отмечены обе галочки, то за оставшееся время в текущем учетном периоде будет списан полный объем абонентской платы и предоставлен полный объем предоплаченного трафика. Например, услугу с периодической составляющей в 10 у. е. и 100 МБ предоплаченного трафика подключаем 15-го числа, при этом учетный период длится с 1-го числа по 1-е число. В этом случае с пользователя будет списано 10 у. е. и будет предоставлено 100 МБ трафика.

2. Если не отмечена галочка ППТ, а галочка ПАП отмечена, то за оставшееся время в текущем учетном периоде будет списана часть абонентской платы пропорционально оставшемуся времени и предоставлен полный объем предоплаченного трафика. Например, услугу с периодической составляющей в 10 у. е. и 100 МБ предоплаченного трафика подключаем 15-го числа, при этом учетный период длится с 1-го числа по 1-е число (длительность месяца 30 дней). В этом случае с пользователя будет списано 5 у. е. и будет предоставлено 100 МБ трафика.

3. Если не отмечена галочка ПАП, а галочка ППТ отмечена, то за оставшееся время в текущем учетном периоде будет списан полный объем абонентской платы и предоставлен объем пре-

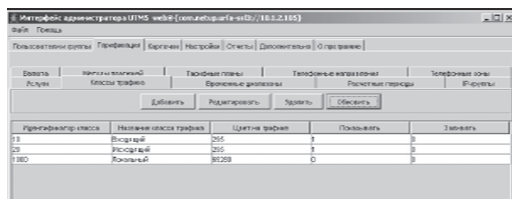
доплаченного трафика пропорционально оставшемуся времени. Например, услугу с периодической составляющей в 10 у. е. и 100 МБ предоплаченного трафика подключаем 15-го числа, при этом учетный период длится с 1-го числа по 1-е число (длительность месяца 30 дней). В этом случае с пользователя будет списано 10 у. е. и будет предоставлено 50 МБ трафика.

4. Если отмечены обе галочки, то за оставшееся время в текущем учетном периоде будет списана часть абонентской платы пропорционально оставшемуся времени и предоставлен объем предоплаченного трафика пропорционально оставшемуся времени. Например, услугу с периодической составляющей в 10 у. е. и 100 МБ предоплаченного трафика подключаем 15-го числа, при этом учетный период длится с 1-го числа по 1-е число (длительность месяца 30 дней). В этом случае с пользователя будет списано 5 у. е. и будет предоставлено 50 МБ трафика.

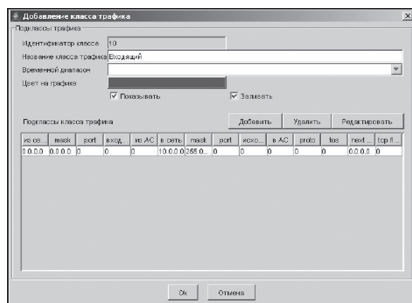
Аналогично галочки действуют при блокировках.

Классы трафика

Весь трафик, прошедший в сторону клиента или от него, разделяется на классы. Набор признаков, по которым происходит объединение записей о трафике в классы, задается при помощи определённых правил. Признаки, по которым можно объединять записи о трафике в классы, – это любые поля в записи NetFlow версии 5: принадлежность IP-адреса источника или получателя какой-либо сети, порт источника или получателя, автономная система источника или получателя, сетевой протокол, следующий маршрутизатор, TOS, TCP-флаги, интерфейс маршрутизатора, через который проходит пакет. Помимо этого запись о трафике можно отнести к тому или иному классу в зависимости от времени суток и дня недели.



Для правильного учёта интернет-трафика, как правило, достаточно завести три класса: «Входящий», «Исходящий» и «Локальный» трафик. Входящий трафик определяется как трафик из сети, составляющей всё множество IP-адресов (сеть 0.0.0.0 маска 0.0.0.0), в локальную сеть (например, сеть 10.0.0.0 маска 255.255.255.0). Исходящий трафик определяется как трафик от IP-адресов локальной сети в сеть 0.0.0.0/0.0.0.0. Для исключения учёта локального трафика как интернет-трафика следует создать класс трафика «Локальный», определяемый как трафик из локальной сети в эту же сеть. Для раздельного учёта трафика по другим признакам необходимо создавать класс трафика с указанием признака, по которому необходимо классифицировать трафик. В каждом классе можно указывать неограниченное количество правил для отбора записей о трафике. Эти правила называются подклассами.



Следует обратить внимание на то, что принадлежность записи о трафике какому-либо классу определяется классификатором путём перебора «совместимости» записи о трафике с правилами, указанными в классах, начиная с класса трафика с максимальным идентификатором (id). Трафик маркируется первым совпавшим классом. Таким образом, классы трафика нужно размещать под такими номерами, чтобы идентификатор класса трафика, являющегося подмножеством другого класса трафика, был больше идентификатора последнего.

Например, используя приведенные выше обозначения, запись о трафике «от IP 10.0.0.5 к IP 10.0.0.10» попадает как под правила класса трафика «Входящий» (класс трафика 10), так и под правила классов трафика «Исходящий» (класс трафика 20) и «Локальный» (класс трафика 1000). Чтобы эта запись правильно обрабатывалась классификатором, классы нужно

расположить в порядке: «Входящий», «Исходящий», «Локальный». В этом случае запись о трафике будет помечена как класс трафика 1000 («Локальный» трафик).

Если отмечена галочка «Не сохранять», то детальная информация по трафику данного класса не будет сохраняться в базу данных с детальным трафиком. Данная опция будет полезна для трафика, стоимость которого равно нулю или детализация по которому не понадобится. Таким трафиком может быть, например, локальный трафик. Данный функционал позволяет уменьшить размер базы данных с детальным трафиком.

Если отмечена галочка «Пропустить», то совпадающий с указанным шаблоном трафик не будет маркироваться данным классом. При этом продолжается сравнение с другими классами трафика. Данная схема удобна в том случае, если необходимо отдельный адрес из всей сети выделить в отдельный класс трафика.

Пример работы классов трафика

В системе присутствует абонент с IP-адресом 10.0.0.10. При этом данный абонент осуществил закачку 50 МБ с сайта www.netup.ru (IP-адрес сайта 195.161.112.6).

Ниже приводится последовательность действия системы для определения класса трафика.

1. Проверяется совпадение с классом трафика с наибольшим идентификатором. Идентификатор класса трафика: 1000. Название класса: «Локальный». Направление из сети 10.0.0.0/255.0.0.0 в сеть 10.0.0.0/255.0.0.0.
2. Трафик с адреса 195.161.112.6 к адресу 10.0.0.10 не попадает под данные условия. Следовательно, система проверяет совпадение со следующим по убыванию идентификатора классом трафика. Идентификатор класса трафика: 20. Название класса: «Исходящий». Направление из сети 10.0.0.0/255.0.0.0 в сеть 0.0.0.0/0.0.0.0.
3. Трафик с адреса 195.161.112.6 к адресу 10.0.0.10 не попадает под данные условия. Следовательно, система проверяет сов-

падение со следующим по убыванию идентификатора классом трафика. Идентификатор класса трафика: 10. Название класса: «Входящий». Направление из сети 0.0.0.0/0.0.0.0 в сеть 10.0.0.0/255.0.0.0. Трафик с адреса 195.161.112.6 к адресу 10.0.0.10 попадает под данные условия. На этом система заканчивает поиск класса трафика и маркирует данный трафик классом 10.

Соотнесение трафика на пользователей

После определения класса трафика производится определение пользователя, для которого будет тарифицирован данный трафик. Определение производится по IP-адресам, указанным в прикрепленной к пользователю услуге «Передача IP-трафика». Если к пользователю прикреплена группа IP-адресов, то соотнесение будет происходить для всей группы.

В том случае, если происходит обмен данными между пользователем системы и внешними сетями, происходит тарификация как входящего, так и исходящего трафика согласно стоимости, указанной в параметрах услуги «Передача IP-трафика».

В случае передачи данных между двумя пользователями системы, каждому из пользователей будет приписан и соответствующим образом тарифицирован входящий для него трафик.

Например, к пользователям А и Б подключена услуга «Передача IP-трафика». К пользователю А прикреплен IP-адрес 10.0.0.10 (маска сети – 255.255.255.255), а к пользователю Б – IP-сеть 10.1.20.0 (маска сети – 255.255.255.0). В UTM поступила следующая информация от коллектора:

IP-адрес источника	IP-адрес получателя	Объём трафика
195.161.112.6	10.0.0.10	10МБ
195.161.112.6	10.1.20.34	15МБ
10.0.0.10	10.1.20.1	20МБ
10.1.20.1	10.0.0.10	30МБ

Основываясь на этих данных, UTM припишет и тарифицирует 10 МБ входящего трафика для пользователя А (строка

1), 15 МБ входящего трафика для пользователя Б (строка 2), 20 МБ входящего трафика для пользователя А (строка 3) и 30 МБ входящего трафика для пользователя Б.

Агрегация трафика

Для более экономного использования ресурсов базы данных производится процесс агрегирования поступающих записей по протоколу NetFlow v. 5. Агрегирование производится по полям «Сервисная связка» (`slink_id`), «IP-адрес» (`ipid`), «Класс трафика» (`tclass`), «Идентификатор расчётного периода» (`discount_period_id`). Запись в базу данных агрегированного трафика происходит периодически через количество секунд указанное в настройках в поле `traffic_agregation_interval`. Если в течение указанного времени придёт два пакета, у которых параметры `slink_id`, `ipid`, `tclass`, `discount_period_id` совпадают, то они будут объединены в одну запись. В итоге в базе данных в таблице `discount_transactions_iptraffic_all` будет одна запись, а не две.

Запись агрегированного трафика в базу данных происходит также, если количество средств на лицевом счёте клиента стало меньше кредитного предела, в случае закрытия расчётного периода, либо если к списанию накоплено средств больше, чем указано в настройках в поле `aggregation_todisc_barrier`.

В связи с агрегацией трафика может возникнуть ситуация, когда в разделе (Отчёты | Детальный отчёт по трафику) записи появляются сразу, после того как их передал в ядро коллектор, но списания с лицевого счёта за этот трафик не производится и в разделе (Отчёты | Отчёт по трафику) новые записи не появляются. В этом случае необходимо выполнение следующих условий:

1. Дождаться, когда истечёт интервал агрегации (по умолчанию время `traffic_agregation_interval` равно 15 минутам).
2. Дождаться, когда стоимость агрегированного трафика превысит барьер агрегации (по умолчанию `aggregation_todisc_barrier` равен 5 условным единицам).

Счет

Выставлен: "БЕТ-Ин" -
17701, Москва, Ленинский, 81/7

Оформляем выписку программы

Всего	17701	17701	17701
Всего	17701	17701	17701
Всего	17701	17701	17701

Счет № 9
От 01.04.2014

Исчисление: ТАО "Ташки", КОД 1771440550

№	Тип	Имя	Время	Вс	Сумма
1	Служба связи	0.00	1.000		0.00
2	Служба связи	1.00	100.000		100.00
3	Служба связи	0.00	100.000		0.00
4	Служба связи	0.00	100.000		0.00

Сумма 100.00

Сумма 100.00

Всего начислено 4.00 руб. Сумма начислено 4.00 руб. из суммы

Уплачено 0.00 / 0.00

Всего 0.00 / 0.00

Действие

Печать Экспорт

2. В тариф включено 100 мегабайт входящего в сторону абонента трафика. Абонентская плата за данную услугу – 100 у. е. Стоимость превышения – 1 у. е. за мегабайт. Незрасходованный трафик не переносится на следующий расчетный период.

В данном случае периодическая стоимость услуги составляет 100 у. е. В границах по трафику прописываются две записи. Первая - граница 0, стоимость 0. Вторая – 104 857 600 байт – стоимость 1.

Количество предоплаченного трафика равно нулю.

3. В тариф включено 100 мегабайт входящего в сторону абонента трафика. Абонентская плата за данную услугу – 100 у. е. Стоимость превышения – 1 у. е. за мегабайт. Незрасходованный трафик переносится на следующий расчетный период.

Стоимость услуги составляет 100 у. е., предоплаченные единицы (для входящего трафика) – 104 857 600. В границы заносится одна запись: граница – 0 байт, стоимость – 1 у. е.

Группы IP-адресов

Группы IP-адресов					
Имя	IP	Маска	МАС	Логин	Пользователь (ID)
1	192.168.1.0/24	255.255.255.0		adm	
2	192.168.1.0/24	255.255.255.0		user	
3	192.168.1.0/24	255.255.255.0		guest	
4	192.168.1.0/24	255.255.255.0		...	

Отображение IP-адресов, присвоенных пользователям, реализовано в системе в виде списка групп IP. В списке указываются сеть, присвоенная пользователю (IP-адрес и маска сети), и логин.

Временные диапазоны

Для настройки зависимости стоимости услуг от времени суток или дней недели используются временные диапазоны.

Параметры временного диапазона

Настройка:

Начало	Окончание
День:	День:
День:	День:
День:	День:
День:	День:
День:	День:

Например, чтобы организовать льготную тарификацию в ночное время, можно создать временной диапазон «Ночной» и указать временные границы с 2:00 по 8:00, все дни недели: с воскресенья по субботу (система воспринимает последовательность дней недели, начиная с воскресенья по субботу).

Для тарификации с учётом временных диапазонов необходимо создать отдельный класс трафика и привязать к нему диапазон. Затем создать услугу, включающую данный класс трафика, и привязать её к пользователю.

Услуги коммутируемого доступа и хотспот

Услуги коммутируемого доступа и хотспот тарифицируются по времени. Они имеют периодическую составляющую, которая может играть роль абонентской платы. Стоимость пов-

ремени можно задавать в зависимости от времени суток и дней недели, в которые оказывается услуга.

Стоимость указывается для одного часа соединения. Так же необходимо указать название пула IP-адресов на сервере доступа. Более подробная информация по настройке серверов доступа приведена в документации «Модуль коммутируемых и VPN-соединений».

Примеры

1. Стоимость услуги с 00 часов 00 минут до 08 часов 00 минут каждого дня составляет 10 р. за час. Стоимость услуги с 08 часов 00 минут до 23 часов 59 минут каждого дня составляет 20 р. за час.

В системе заводятся два временных диапазона – с 00:00 до 07:59, все дни недели – «Ночной» и с 08:00 до 23:59, все дни недели – «Дневной». При добавлении услуги периодическая стоимость выставляется 0, и добавляются две позиции: временной диапазон «Ночной» со стоимостью 10 р. и временной диапазон «Дневной» со стоимостью 20 р.

2. Ночной неограниченный доступ. Стоимость услуги – 500 р. в месяц.

Периодическая стоимость услуги выставляется 500 р. Выставляется стоимость временного диапазона «Ночной», равная нулю. Диапазон «Дневной» не добавляется. В этом случае днем авторизация пользователя будет невозможна.

Тарификация IP-трафика при динамическом распределении IP-адресов

В случае если IP-адреса абонентам распределяются из пула IP-адресов, то в этом случае применяется особая схема настройки биллинговой системы.

Необходимо настроить пулы IP-адресов либо в биллинговой системе либо на сервере доступа. Описание настройки пулов на сервере доступа Cisco можно посмотреть в разделе «Модуль коммутируемых и VPN-соединений». В биллинговой системе пулы настраиваются в разделе «Настройки» - «IP-пулы».

После настройки пулов необходимо создать тарифный план с услугами «Передача IP-трафика» и «Коммутируемый доступ». В настройках услуги «Коммутируемый доступ» необходимо указать стоимость соединения 0 у.е./час, а так же указать наименование существующего пула IP-адресов. Во всех услугах должна быть отмечена галочка «Подключать по умолчанию».

Редактирование тарифного плана

Параметры тарифного плана

ID тарифа: 21

Название тарифа: Динамический IP-трафик

Создан: 14.10.2005 Изменен: 14.10.2005

Создал: jgl Изменил: jgl

Срок завершения действия: 14.10.2005

Услуги	Добавить	Удалить	Редактировать
Идентификатор ус...	Тип услуги	Название услуги	Комментарий
54	Коммутируемый д...	Динамический ко...	
56	Передача IP-трафи...	Динамический IP-т...	

При подключении тарифного плана к абоненту необходимо указать логин и пароль в сервисной связке «Коммутируемый доступ». В сервисной связке «Передача IP-трафика» можно указать любой IP-адрес из неиспользуемой сети (например, сетей 172.16.0.0, 10.0.0.0, 192.168.0.0).

При авторизации абонента на сервере доступа будет использоваться логин и пароль из настроек услуги «Коммутируемый доступ». При успешной авторизации сервер доступа устано-

вит соединение и произведет динамическую выдачу абоненту IP-адреса из пула. Этот адрес будет динамически привязан к услуге «Передача IP-трафика» данного абонента. Таким образом, биллинговая система всегда содержит актуальную информацию о том, какой IP-адрес используется в данный момент абонентом и может корректно соотносить по абонентам приходящую с сервера статистику.

Расчётные периоды

Расчётный период – это период времени, в течение которого производится удержание средств с лицевого счета пользователей за периодические услуги. Каждый пользователь, лицевой счёт, услуга и тарифный план имеют свои расчётные периоды.

Стандартные расчётные периоды: ежедневный, еженедельный, ежемесячный, ежеквартальный, ежегодный, период с фиксированным числом дней.

Ведение общего справочника расчётных периодов позволяет вести расчеты со всеми либо группами абонентов в одно и то же время, например, с первого по первое число каждого месяца.

При закрытии расчётного периода осуществляется подведение итогов: пересчёт абонентской платы и prepaid трафика с учётом блокировок, перенос неистраченного prepaid трафика на следующий расчётный период, выписка счетов. При закрытии производится продление расчётного периода без участия оператора. Например, если имеется расчётный период с длительность 1 месяц и производится его закрытие 1 сентября 2004 года, то данный период будет автоматически продлен до 1 октября 2004 года и так далее.

Интерфейс администратора: webf (admin@webf-002/18.12.2003)

Файл Печать

Поиск абонента по логину | Профиль | Баланс | Настройки | Счета | Дополнительно | Операции

Возраст | Индивидуальный | Тарифный план | Запрещенные услуги | Группы услуг

Услуга | Классификация | Временные диапазоны | Расчетные периоды | Прогноз

Добавить | Редактировать | Удалить | Обновить

ID	Дата начала	Дата окончания	Тип периода	ID сервиса/периода	Длительность, д
0	08.04.2004 17:05:10	07.04.2004 17:05:10	ежедневный	0	3600
0	08.04.2004 17:05:10	07.05.2004 17:05:10	ежемесячный	0	30.000

Любая периодическая услуга имеет расчетный период. Если поле `discount_period_id` в «Сервисной связке» не поль, то берется расчетный период из этого поля, иначе берется расчетный период, который прописан на лицевом счете пользователя либо если на лицевой счет так же не указан расчетный период, то на пользователя.

При закрытии расчетного периода создается новый расчетный период и привязывается к сервисной связке. Обнуляются поля `discounted_in_curr_period` и `downloaded` (для услуги `iptraffic`). Так же при необходимости осуществляется перенос prepaid трафика, пересчитывается абонентская плата и prepaid трафик в соответствии с блокировками. В таблицах `invoices` и `invoice_entry` подготавливаются счета на оплату с учетом списаний произведенных в закрываемом расчетном периоде.

Предоплата

Система поддерживает работу с пользователями по схеме предоплаты. Суть заключается в следующем. При закрытии расчетного периода система генерирует счёт на оплату на лицевой счёт пользователя. Счёт на оплаты включает в себя помимо позиций, соответствующих задолженности пользователя перед провайдером за использования услуг (например, в случае услуги «Передача IP-трафика» это будут позиции, соответствующие суммарной стоимости переданного объёма информации за весь расчетный период), ещё и позицию, соответствующую периодической составляющей услуги на следующий расчетный период (абонентская плата за следующий расчетный период). При такой схеме работы система также генерирует счёт на оплату и при подключении услуги к лицевому счёту пользователя, такой счёт будет содержать единственную позицию – периодическую составляющую подключаемой услуги (абонентскую плату). Вышеописанная схема выставления счетов работает только при выполнении следующих условий: пользователь работает по предоплате и подключаемая услуга имеет в качестве значения параметра «Метод снятия денег» – «В начале расчетного периода», то есть в счета на оплату включается абонентская плата за следующий расчетный период только при выполнении вышеуказанных условий.

Для того чтобы регламентировать работу с пользователем по схеме предоплаты, необходимо в окне редактирования пользователя в закладке «Основные параметры» выставить галочку «Работа по предоплате».

Налоговые ставки

Налоговые ставки задаются в разделе редактирования данных абонента. Имеется возможность задать ставку налога на добавленную стоимость (НДС) и налога с продаж (НСП). Стоимость всех услуг указывается без НДС и НСП. При списаниях за услуги так же будет вычислена и списана сумма налогов.

Примеры

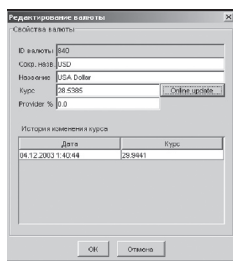
1. Стоимость разовой услуги –100 у. е. Ставка НДС указана 18 %, ставка НСП – 0 %. Со счёта абонента за эту услугу будет списано $(100 \cdot 1.18) \cdot 1.00 = 118$ у. е., из которых 18 у. е. составляют налоги.

2. Стоимость разовой услуги –100 у. е. Ставка НДС указана 0 %, ставка НСП – 0 %. Со счёта абонента за эту услугу будет списано $(100 \cdot 1.0) \cdot 1.0 = 100$ у. е., из которых налоги составляют 0 у. е.

Валюты

Система поддерживает работу с любым количеством валют. Все лицевые счета и расчеты ведутся в условных единицах. По умолчанию, условная единица равна российскому рублю. При добавлении или редактировании валюты указываются её идентификатор, сокращённое название, полное название, курс по отношению к условной единице и произвольный про-

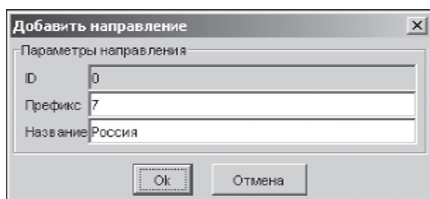
центный коэффициент, на который умножается официальный курс валюты для получения внутреннего курса провайдера. Также в окне редактирования валюты доступна история изменения курса.



При нажатии на кнопку «Online Update» произойдёт обновление курса валюты из интернета. Новый курс установится равным курсу ЦБ РФ на текущую дату.

Телефонные направления

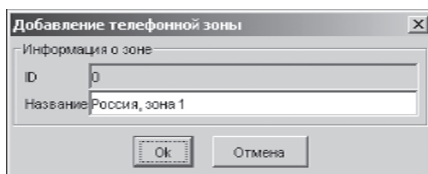
В системе имеется возможность ведения справочника телефонных направлений для последующей организации тарификации телефонных звонков. При добавлении направления указываются префикс и название направления.



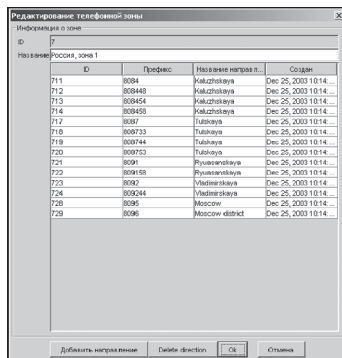
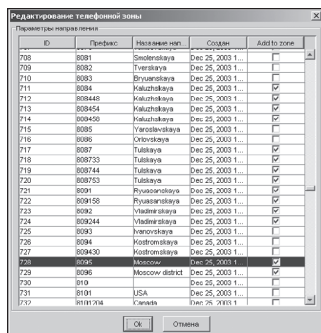
Более подробно о направлениях смотрите в разделе «Модуль телефонии».

Телефонные зоны

Для удобства тарификации телефонных разговоров телефонные направления объединяются в зоны. Телефонная зона – это набор определённых телефонных направлений.



После создания телефонной зоны можно изменять её состав: добавлять и удалять направления.



Стоимость телефонного звонка указывается в настройках услуги типа «Телефония» для любой созданной зоны с учетом временных диапазонов.

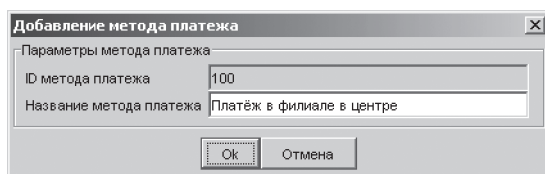
Более подробно о телефонных зонах смотрите в разделе «Модуль телефонии».

Методы платежей

Система поддерживает множество способов оплаты услуг пользователями. Среди стандартных: оплата наличными, банковский перевод, оплата банковской картой, оплата через дилера и оплата через платёжную систему «Рапида».

Способ платежа указывается оператором при приёме оплаты у пользователя.

Встроенные методы оплаты имеют идентификаторы меньше 100. Администратор может создавать новые методы платежей с идентификаторами больше 100, но не может редактировать стандартные способы оплаты. Создание новых методов оплаты может служить для построения, в дальнейшем, отдельных отчётов по платежам с группировкой по способу платежа.



Для выплат комиссии дилеру существует соответствующий способ платежа.

Тарифные планы

Тарифный план представляет собой пакет услуг, которые предоставляются в комплексе. Система позволяет создавать такие пакеты, а затем одной операцией (выбор тарифного плана) добавлять услуги пользователям.

Редактирование тарифного плана

Параметры тарифного плана

ID тарифа: 1

Название тарифа: Тестовый тариф

Создан: 06.04.2004 18:07:14

Изменено: 06.04.2004 18:00:22

Создан: итвб

Изменен: итвб

Срок заархивации действия: 06.04.2004 0:00:00

Выбор: [Выбор]

Заблокирован: [Нет]

Добавить Удалить Редактировать

Идентификатор у.	Тип услуги	Название услуги	Комментарий
7	Расовая услуга	Расовая услуга	
9	Периодна Р-тарифа	Тест Р-тарифа	

OK Отмена

При подключении тарифного плана к пользователю необходимо выбрать учётный период и указать настройки подключаемых услуг.

Контракты Услуги Технич. параметры Дополнительно Контакты Счеты Настройки дилера Тарифные планы Группы Памятка пользователя

Текущий тарифный план: [Тестовый тариф] --> Следующий тарифный план: [Тестовый тариф]

Расчетный период: 1 [Выбор]

[Применить] [Удалить]

Добавить

OK Отмена Apply

При этом можно выборочно подключать услуги из тарифного плана. Учётный период тарифного плана устанавливается для всех услуг, подключаемых в составе этого тарифного плана.

Список услуг в тарифном плане

Подключать услугу Отключить услугу Настроить

Идентифик.	Название услуги	Тип услуги	Комментар.	ID сс связи	is linked
7	Расовая услуга	Расовая у...		0	1
9	Тест Р-тарифа	Периодна Р...		0	1

OK

Для корректного переключения настроек услуг необходимо, чтобы тарифный план, на который происходит переключение, был совместим с тем, что подключен в текущий момент.

У совместимых тарифных планов между услугами в этих тарифных планах есть взаимнооднозначное соответствие. Это означает, что система без вмешательства оператора может поменять тарифный план, сохраняя полезную информацию из сервисных связей, такую, как, например, IP-адреса в услуге «Передача IP-трафика».

Несовместимые тарифные планы система также может переключать, но услуги, которых нет в тарифном плане следующего учётного периода, будут удалены.

Услуги группируются посредством родительской услуги. В этом случае можно выделить 3 группы услуг.

1. Простейшие услуги, не включаемые в состав тарифного плана. Подключение таких услуг производится напрямую.
2. «Фиктивные» услуги, которые не содержат в себе полезной информации, кроме названия, и только играют роль родительских для услуг третьей группы.
3. Услуги, имеющие родителя и находящиеся в составе тарифного плана.



При закрытии учётного периода происходит переключение на тарифный план следующего учётного периода, если он отличается от текущего тарифного плана. Пусть пользователю подключена услуга А в составе тарифного плана 1, и тарифный план следующего учётного периода – 2, в состав которого входит услуга Б. Для того, чтобы произошёл корректный перенос всех параметров подключенной услуги А, необходимо, чтобы обе услуги А и Б имели общую родительскую услугу В, как показано на рисунке.

В течение текущего учётного периода идентификатор тарифного плана следующего учётного периода можно менять без ограничений, но переключение тарифного плана произойдёт только при закрытии учётного периода.

Краткое описание таблиц базы данных, отвечающих за тарификацию

service_links

id – сквозной идентификатор услуги, появляется также в таблицах *_service_link.

user_id – идентификатор пользователя из таблицы users.

account_id – идентификатор лицевого счёта пользователя из таблицы accounts.

service_id – идентификатор услуги.

is_deleted – если услуга отключается от пользователя, то is_deleted устанавливается в ненулевое значение.

periodic_service_links

is_blocked – битовая маска, характеризующая блокировку.

discount_period_id – идентификатор расчётного периода.

discounted_in_curr_period – сколько было списано со счёта за эту услугу в текущем расчётном периоде.

start_date – дата начала предоставления услуги. В момент наступления start_date is_planned переводится в 0.

is_planned – пока услуга находится в планируемом состоянии, средства за неё списываться не будут. Услуга является планируемой, если значение в этом поле равно нулю.

expire_date – дата отключения услуги.

`need_del` – услуга требует удаления. При наступлении даты большей, чем `expire_date` поле `need_del` устанавливается в 1.

Любая периодическая услуга имеет расчётный период (`discount_period`), при закрытии которого проверяется поле `need_del`. Если `need_del` не равно нулю, то услуга отключается от лицевого счёта пользователя.

`iptraffic_service_links`

`ip_group_id` – идентификатор группы IP-адресов.

`downloaded_id` – идентификатор в таблице `downloaded`.

`downloaded`

Таблица описывает, сколько трафика каждого класса скачал пользователь в текущем расчётном периоде.

`downloaded_id` – идентификатор из `iptraffic_service_links`.

`tclass_id` – идентификатор класса трафика.

`qnt` – количество скачанного трафика в байтах.

`old_prepay` – количество prepaid трафика, который был перенесён из предыдущего расчётного периода.

`ip_groups`

`ip_group_id` – идентификатор группы IP-адресов. Допускается наличие нескольких записей с одинаковым `ip_group_id`.

`ip` – IP-адрес.

`mask` – маска подсети.

`uname` – имя пользователя.

`upass` – пароль.

`mac` – MAC-адрес.

discount_periods

Информация обо всех расчётных периодах, зарегистрированных в системе, находится в базе данных в этой таблице.

`id` - идентификатор расчётного периода.

`start_date` - начало расчётного периода в формате UNIX timestamp.

`end_date` - дата окончания расчётного периода.

`periodic_type` - тип расчётного периода. Используется при вычислении длительности следующего расчётного периода. Возможные следующие значения: 1 - ежедневный расчётный период, 2 - еженедельный, 3 - ежемесячный, 4 - ежеквартальный, 5 - ежегодный, 0x100000 - фиксированное количество дней.

`canonical_len` - длина расчётного периода в секундах, заполняется при создании расчётного периода и в дальнейшем не изменяется. Цель данного поля - правильный пересчёт абонентской платы и предоплаченного трафика, когда были изменены границы расчётного периода.

`is_expired` - устанавливается не ноль, когда `end_date` больше, чем текущее время.

Платежи

Поддержка нескольких валют

АСР NetUP UTM поддерживает работу с любым количеством валют. Курсы валют указываются, по умолчанию, по отношению к российскому рублю. Более подробно смотрите в разделе (Тарификация | Валюты).

Персональные настройки валюты абонента

АСР NetUP UTM предоставляет провайдеру возможность настройки валюты и её коэффициента для каждого абонента в отдельности.

Закреплённая валюта

Настройка валюты заключается в закреплении за абонентом валюты, в которой будут происходить операции взаиморасчетов между провайдером и абонентом.

NetUP UTM поддерживает смену в любой момент времени закреплённой за абонентом валюты на любую другую, зарегистрированную в системе. В результате смены валюты все счета на оплату услуг будут отображаться во вновь выбранной валюте, не зависимо от того, были ли они сгенерированы системой до момента смены валюты или же после.

По умолчанию закреплённая валюта абонента есть российский рубль.

Смена закреплённой валюты производится администратором или оператором АСР NetUP UTM через центр управления. Для этого необходимо во вкладке «Дополнительно» окна детализации пользователя выбрать из списка «Основная валюта» необходимую валюту, затем сохранить выбор путем нажатия кнопки «Сохранить» на панели управления этой вкладки.

Персональный коэффициент валюты

Персональный коэффициент валюты – персональная настройка абонента, регламентирующая процент увеличения или уменьшения суммы оплаты услуг провайдера абонентом при внесении платежа на основании счета, в валюте, отличной от закреплённой. Смена персонального коэффициента производится администратором или оператором АСР NetUP UTM через центр управления. Для этого необходимо во вкладке «Дополнительно» окна детализации пользователя выставить значение, от 0 до 100, и знак, «+» или «-», процента, затем сохранить значение путем нажатия кнопки «Сохранить» на панели управления этой вкладки.

Пример

Закрепленная валюта – 840, доллар США (USD); персональный коэффициент +10%; оплата на основании счёта за услугу стоимостью 300.00 российских рублей; курс USD – 29,9441; ввод платежа осуществляется в российских рублях.

Исходя из начальных условий, счёт выставлен на сумму 10.02USD. Счёт выглядит следующим образом.

Платеж: ЮНН					
Валюта: 840 - USD(USA Dollar), Курс: ЦБ РФ на день оплаты					
#	Товар	Цена	Кол-во	Ед.	Сумма
1	Подсоединен(5)	10.02	1.000		10.02
Сумма					10.02
Сумма налога					0.00
Итого					10.02

После выбора данного счета в качестве основания платежа, диалог «Внести платеж» содержит следующие данные:

Внести платеж

Параметры платежа

Логин: rupkin

Сумма: 10.02

Валюта: USD

Дата платежа: 18.04.2004 Выбрать

Коммент. для админ.:

Коммент. для польз.:

Метод платежа: Оплата наличными

Номер плат. документа:

Платеж по счету: 3 от 18.04.2004 на сумму 10.02 USD Выбрать

OK Отмена

Если сменить валюту оплаты счёта, сумма будет вычислена с учётом персонального коэффициента и станет равной 330.00 рублям, что на 10% больше стоимости услуги.

Внести платеж

Параметры платежа

Логин: rupkin

Сумма: 330.00

Валюта: RUR

Дата платежа: 18.04.2004 Выбрать

Коммент. для админ.:

Коммент. для польз.:

Метод платежа: Оплата наличными

Номер плат. документа:

Платеж по счету: 3 от 18.04.2004 на сумму 10.02 USD Выбрать

OK Отмена

После подтверждения ввода платежа на счёт абонента поступят средства в размере 300.00 рублей, а 10% (30 рублей) пойдут в пользу провайдера.

Если бы персональный коэффициент был установлен в значение не +10%, а -10%, тогда при оплате этого же счёта в рублях абоненту пришлось бы заплатить не 330.00 рублей, а 270.00 рублей, при этом на счёт абонента поступили бы средства в размере 300.00 рублей. Таким образом, провайдер оплачивает часть стоимости услуги в размере 10% за свой счет.

Ввод платежей

Платежи в системе могут вводиться несколькими способами, а именно:

- автоматический ввод платежей на лицевой счет абонента при оплате абонентом услуг провайдера через расчётную систему «Рапида»;
- автоматический ввод платежей на лицевой счёт абонента из стороннего программного обеспечения;
- ручной ввод платежа администратором системы (оператором) посредством центра управления UTM.

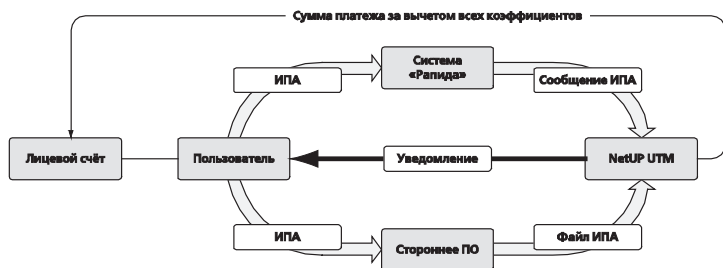
Оплата через систему «Рапида»

Абонент пополняет свой лицевой счёт посредством платёжной системы «Рапида», например, через кассу в супермаркете. Расчётная система Рапида после приема информации от абонента (идентификационные данные абонента, сумма платежа, основание платежа и т. п.), для краткости – ИПА (Информация о Платеже Абонента), оповещает систему о факте ввода платежа абонентом посредством сообщения, содержащего ИПА в виде файла. Система разбирает сообщение и вносит на счёт абонента сумму платежа, указанную в сообщении. После внесения платежа на счёт система уведомляет абонента о приёме платежа, путём отправки сообщения на адрес электронной почты.

Для предоставления провайдером возможности внесения платежей через платёжную систему «Рапида» для своих абонентов, он должен заключить договор с системным интегратором, предоставляющим техническое подключение к системе «Рапида».

Схема взаимодействия между участниками операции ввода платежа отображена на рисунке.

Технические детали взаимодействия ACP NetUP UTM с платёжной системой «Рапида» смотрите в разделе «Приём платежей в ACP NetUP UTM через платёжную систему «Рапида».



Ввод платежа посредством стороннего ПО

В АСР NetUP UTM предусмотрена возможность ввода платежа на счёт абонента, исходя из данных, находящихся в стороннем ПО – программное обеспечение и автоматизированные системы, не имеющие отношения к UTM. Такой способ ввода платежей осуществляется на базе модуля ввода платежей через расчётную систему «Рапида». Для ввода платежа стороннее ПО должно иметь возможность генерировать файлы с информацией о платеже, структура которых в точности совпадает со структурой сообщений от расчётной системы «Рапида». Разница между этим методом и методом ввода платежей через расчётную систему «Рапида» состоит в том, что сообщение (файл), содержащее ИПА, генерируется не системой «Рапида», а именно сторонним ПО. Для доступа АСР NetUP UTM к этому сообщению достаточно его поместить в системную папку, из которой модуль ввода платежей через расчётную систему «Рапида» получает доступ к сообщениям о платежах от «Рапида».

Технические детали взаимодействия АСР NetUP UTM с платёжной системой «Рапида» смотрите в разделе «Приём платежей в АСР NetUP UTM через платёжную систему «Рапида».

Ввод платежа администратором системы

Ввод платежа производится администратором или оператором системы через центр управления. Возможны два варианта внесения платежа. Первый вариант – выбрать абонента из списка пользователей и выбрать операцию «Внести платёж».

Второй вариант – выбрать операцию «Внести платёж» в окне детализации информации по пользователю (абоненту). Нажатие кнопки «Внести платёж» инициирует вызов диалога «Внести платёж».

В диалоге ввода платежа администратору предоставляется возможность внести следующие данные о платеже (обязательные к заполнению поля выделены жирным):

- Сумма – сумма платежа;
- Валюта – валюта ввода платежа;
- Дата платежа – дата ввода платежа, по умолчанию – текущая дата;
- Коммент. для админ. – комментарий о платеже для администратора системы;
- Коммент. для польз. – комментарий о платеже для абонента системы;
- Метод платежа – метод ввода средств на счет абонента, по умолчанию – Оплата наличными;
- Номер плат. документа – номер платёжного документа – номер внешнего (не системного) платёжного документа, являющегося основанием ввода платежа, например, номер счёта выписанного из какой-либо бухгалтерской программы или выписанного какой-либо организацией;
- Платеж по счёту – внутренний номер счёта (номер счёта внутри системы), по которому производится оплата. Если счёт выбран, то он является основанием платежа.

Флаг «Turn on inet» означает, что интернет должен быть включен для пользователя, если это позволяет его баланс после проведения платежа. Если галочка «Turn on inet» не отмечена, то статус интернета для пользователя меняться не будет. Значение этого флага по умолчанию может быть задано в конфигураци-

онном файле `utm5admin.cfg`, находящемся в текущей директории, при помощи параметра `payment_inet_switch`. Параметр может принимать значения `on` (галочка отмечена по умолчанию) и `off` (галочка не отмечена по умолчанию).

Ввод платежа без основания

Ввод платежа без основания соответствует пополнению счёта абонента. Для ввода платежа достаточно ввести сумму платежа, указать дату платежа и указать метод платежа «Оплата наличными», метод не обязательно должен быть таковым.

Ввод платежа на основании счёта

Для ввода платежа на основании внутреннего счёта системы, который генерируется по окончании расчётного периода, закреплённого за абонентом, достаточно выбрать счёт из списка неоплаченных счетов, выставленных абоненту в диалоге «Счета». Диалоговое окно вызывается путём нажатия кнопки «Выбрать» в строке «Платёж по счёту».

Внутренний номер	Внешний номер	Дата	Сумма
3		18.04.2004	10.0187

После выбора счёта в поле «Сумма» диалога «Внести платеж» автоматически выставится сумма, указанная в счёте, поле станет нельзя отредактировать, в поле «Платёж по счёту» пропишется номер счёта, дата генерации счёта, сумма с указанием сокращённого названия валюты, закреплённой за пользователем.

Ввод обещанного платежа (кредита)

Для осуществления платежа без реального внесения средств на счет (обещанного платежа) необходимо в поле «Метод платежа» выбрать «Кредит» и в поле «Истекает» выбрать дату, до которой этот платеж должен быть погашен. С момента внесения платежа пользователю открывается кредит на указанную сумму. Если за указанный промежуток времени пользователь внес обещанные средства, то кредит снимается с пометкой «успешно закрыт». В этом случае оператор связи может позволить пользователю и в дальнейшем вносить обещанные платежи т.к. у него положительная кредитная история. В случае если деньги не были внесены, то кредит закрывается со статусом «неуспешно закрыт». В дальнейшем оператор связи может запретить этому пользователю вносить обещанные платежи.

Откат платежа

В ACP NetUP UTM реализована функция отката платежа. Операция отката платежа производится администратором или оператором ACP NetUP UTM через центр управления.

Операция осуществляется в отчёте по платежам (Отчёты | Платежи) в главном окне приложения или в окне детализации пользователя. Далее необходимо сформировать отчёт за выбранный период времени, выбрать в таблице нужный платёж и вызвать всплывающее меню нажатием правой кнопки мыши. В меню необходимо выбрать пункт «Откат». Наиболее простая навигация по платежам абонента осуществляется через окно детализации пользователя, так как в нем в отчете по платежам отображается информация о платежах в пользу конкретного абонента.

После применения процедуры отката платежа, с лицевого счёта абонента снимется сумма равная фактической сумме платежа, поступившей на счёт абонента (см. пример в подразделе «Персональные настройки валюты абонента»).

Отчёты

Система поддерживает все основные виды отчётов, необходимых для ведения успешной операторской деятельности. Отчёты могут быть сформированы как по одному конкретному пользователю, так и по всем пользователям сразу. Можно выбрать любой промежуток времени, за который необходимо создать отчёт. Сформированные отчёты можно записать во внешний файл формата XML.

Основной отчёт

Основной отчёт (оборотная ведомость) суммирует списания с лицевых счетов пользователей за оказание различных услуг за заданный промежуток времени.

В основной отчёт входят следующие данные:

- номер лицевого счёта;
- входящий остаток;
- сумма списаний за разовые услуги;
- сумма списаний за периодические услуги;
- сумма списаний за услугу передачи IP-трафика;
- сумма списаний за услугу хотспот;
- сумма списаний за услугу коммутируемого доступа;
- сумма списаний за услугу телефонии;
- сумма налогов;
- общая сумма с учётом налогов;
- сумма осуществлённых платежей;
- исходящий остаток.

Отчёт по трафику

Отчёт по трафику суммирует объёмы переданного IP-трафика для каждого лицевого счёта и класса трафика за заданный промежуток времени.

В отчёт по трафику входят следующие данные:

- номер лицевого счёта;

- логин;
- количество байт в килобайте;
- класс трафика;
- объём переданного трафика в мегабайтах;
- цена за единицу переданного трафика (стоимость 1 МБ трафика);
- сумма списания с лицевого счёта пользователя.

Графический отчёт по трафику

Графический отчёт по трафику служит для визуального представления предыдущего отчёта и представляет собой график зависимости потребления различных классов трафика всеми пользователями от времени за выбранный период. Так же в этом отчете доступна информация по максимальной, минимальной и средней скорости потребления IP-трафика.

Детальный отчёт по трафику

Детальный отчёт по трафику строится на базе исходных данных о переданном трафике и включает детализированную информацию:

- дата;
- идентификатор прикреплённой услуги;
- номер лицевого счёта;
- класс трафика;
- IP-адрес и порт источника;
- IP-адрес и порт получателя;
- количество переданных пакетов;
- количество переданных байт;
- флаги TCP;
- протокол;
- TOS.

За большие промежутки времени накапливается огромное количество статистики, поэтому создание такого детализированного отчёта может занять длительное время. Для создания отчёта за большой промежуток времени мы рекомендуем воспользоваться опцией «Отчёт по трафику».

Отчёт по услугам

Отчёт по услугам суммирует информацию о списаниях с лицевых счетов пользователей за оказание конкретных услуг за определённый промежуток времени. В отчёте присутствуют:

- номер лицевого счёта;
- дата списания средств с лицевого счёта;
- расчётный период;
- тип услуги;
- название услуги;
- объём оказанной услуги;
- комментарий к списанию.

Отчёты по модемным сессиям, VPN и телефонии

Отчёт по модемным сессиям и сессиям VPN базируется на статистике сервера RADIUS и суммирует данные о сессиях коммутируемого доступа. В отчёте присутствуют:

- идентификатор сессии;
- номер лицевого счёта;
- дата и время начала сессии;
- дата и время окончания сессии;
- выданный IP-адрес;
- вызывающий абонент;
- вызываемый абонент;
- порт сервера доступа (NAS);
- идентификатор сессии на сервере доступа;
- логин;
- IP-адрес сервера доступа;
- статус сессии;
- объём входящего трафика;
- объём исходящего трафика;
- длительность сессии;
- объём списанных средств.

Отчёт по телефонии аналогичен отчёту по модемным сессиям, но содержит дополнительную информацию:

- телефонная зона;
- направление звонка.

Отчёт по платежам

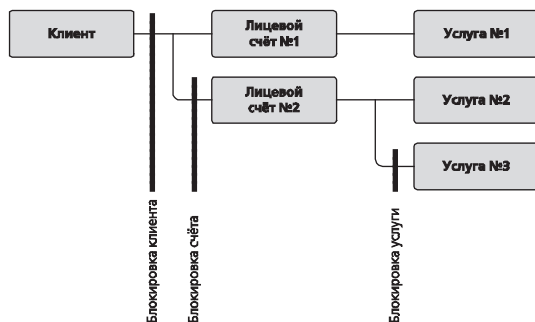
Отчёт по платежам представляет информацию о зачисленных на лицевые счета пользователей средствах за заданный промежуток времени. В отчёте присутствует следующая информация:

- номер лицевого счёта;
- фактическая дата платежа;
- дата введения платежа в систему;
- сумма платежа в валюте системы;
- сумма платежа в валюте оплаты;
- валюта оплаты;
- метод осуществления платежа;
- лицо, внёсшее платеж;
- комментарий к платежу.

Так же в отчете по платежам имеется возможность отменить любой платеж.

Отчёт по блокировкам

Блокировка – это приостановка предоставления одной или нескольких услуг. Блокировка может применяться к клиенту (блокируются все счета клиента), к счёту (блокируются все ус-



луги, предоставляемые по данному счету данному клиенту) и к услуге (блокируется данная услуга, предоставляемая данному клиенту по определённом счету).

Блокировки могут быть трёх типов: администраторская блокировка, системная и добровольная. Администраторская блокировка производится администратором. Системная блокировка производится системой при выполнении определенного условия, например, появлении задолженности на лицевом счету клиента. Добровольная блокировка производится самим клиентом.

Отчёт по блокировкам суммирует информацию обо всех блокировках осуществлённых за заданный период времени. В отчёте собрана следующая информация:

- номер лицевого счёта;
- дата начала действия блокировки;
- срок блокировки;
- что заблокировано;
- тип блокировки;
- комментарий к блокировке.

Настройки

Список параметров

Различные параметры системы задаются в списке параметров в виде «переменная – значение». В списке можно как редактировать существующие параметры, так и добавлять новые.

Описание доступных параметров:

raw_max_files

Максимальное количество файлов с детальной информацией о переданном трафике. Если число файлов больше, чем указано, то старые файлы удаляются. Значение по умолчанию: 10.

raw_max_size

Максимальный размер каждого файла с детальной статистикой о переданном трафике. Значение по умолчанию: 100 000 000 байт (около 100 МБ).

raw_prefix

Путь к файлам с детальной статистикой о прокачанном трафике. Значение по умолчанию: /netup/utm5/db.

В этой директории создаются и хранятся файлы со статистикой. В каждом файле хранятся данные о трафике за период, предшествующий цифре в названии файла (дата в формате Unix timestamp). Названия файлов имеют вид `iptraffic_raw_unixtimestamp.dbs`.

Примеры названий файлов:

`iptraffic_raw_1070957880.dbs`

`iptraffic_raw_1070957930.dbs`

`iptraffic_raw_1070957980.dbs`

smtp_relay

IP-адреса сервера SMTP, через который производится отсылка уведомлений и почтовых сообщений. Значение по умолчанию: 127.0.0.1.

smtp_relay

Порт сервера SMTP. Значение по умолчанию: 25.

smtp_fqdn

Полное доменное имя при отправке почтовых сообщений. Значение по умолчанию: localhost.

smtp_sender

Адрес отправителя при отправке почтовых сообщений. Значение по умолчанию: admin@localhost.

smtp_subject

Тема сообщения при отправке почтовых сообщений.

smtp_recipient

Почтовый адрес администратора, на который будут высылаться сообщения об ошибках.

invoice_subject

Тема сообщения со счетом на оплату.

invoice_text

Текст сообщения со счетом на оплату.

bytes_in_kbyte

Количество байт в килобайте. Из этого значения вычисляется количество байт в мегабайте как bytes_in_kbyte в квадрате. Значение по умолчанию: 1024 (соответственно, в 1 МБ содержится 1048576 байт).

notification_borders

Указываются действительные числа-границы. Когда количество средств на счету переходит через одну из указанных границ, всем пользователям, владеющих этим лицевым счётом, высылается уведомление. Возможно указание нескольких значений.

notification_message

Текст уведомления, который будет отсылаться на e-mail пользователя при переходе баланса через границы указанные в `notification_borders`. В сообщении можно использовать следующие переменные:

`FULL_NAME` – полное имя абонента;

`ACCOUNT_ID` – идентификатор основного лицевого счёта абонента;

`BALANCE` – баланс основного лицевого счёта абонента на момент подготовки сообщения;

`DATE` – дата на момент подготовки сообщения;

`EMAIL` – адрес e-mail, на который производится отсылка.

notification_message_subject

Тема уведомления, которое будет отсылаться на e-mail пользователя при переходе баланса через границы, указанные в `notification_borders`.

notification_message_from

Имя отправителя уведомления. Будет записано в поле `From`: сообщения.

notification_by_wintray

В случае если данный параметр установлен в значение “yes”, уведомление при переходе баланса через границы указанные в `notification_borders` будет дополнительно отослано пользователю с помощью системного сообщения.

balance_notification_email

Адрес электронной почты, на который будут отсылаться копии сообщений о переходе баланса через границы указанные в `notification_borders`.

discount_barrier

При плавном списании платы за периодические услуги со счёта не будут списываться суммы меньше чем `discount_barrier`, чтобы не накапливалась арифметическая ошибка.

traffic_agregation_interval

Как часто производить сброс агрегированного трафика в базу. Значение по умолчанию – 900 секунд.

aggregation_todisc_barrier

Сбрасывать агрегированный трафик в базу, если агрегированного трафика больше, чем на указанную в этом поле сумму. Значение по умолчанию: 5.

flow_discounts_per_period

Минимальное количество списаний в расчётном периоде за периодические услуги, если выбран режим плавного списания.

flow_discount_random_coef

Если у большого количества периодических услуг стоит плавный метод списания, увеличение этого параметра способствует балансировке нагрузки. Когда вычисляется время для следующего снятия средств, к нему прибавляется небольшая случайная величина, максимальное значение которой пропорционально этому параметру.

web_session_timeout

Указывает максимальное время, в течение которого хранится уникальный ключ сессии (SID) веб-интерфейса пользователя.

hotspot_refresh_timeout

Сколько времени действительна хотспот сессия, считая от последнего обновления страницы пользователем.

traffic_mult_coef

Коэффициент, на который умножается собранный трафик (поправочный коэффициент). Если не указывать эту строку, то коэффициент будет равен 1.

`block_recalc_abon`

Переменная задаёт порядок перерасчёта абонентской платы (периодической составляющей стоимости услуги) при автоматической блокировке лицевого счёта или пользователя. Может принимать следующие значения: 0 (абонентская плата должна быть списана даже за те промежутки времени, когда пользователь был заблокирован) и 1 (абонентская плата списывается только за время, когда пользователь не находится в состоянии системной блокировки).

`block_recalc_prepaid`

Переменная задаёт порядок перерасчёта prepaid-единиц (мегабайты трафика или минуты в случае услуг коммутируемого доступа, хотспот и телефонии) при автоматической блокировке лицевого счёта или пользователя. Может принимать следующие значения: 0 (prepaid-единицы предоставляются в полном объёме, несмотря на блокировки пользователя) и 1 (производится перерасчёт prepaid-единиц пропорционально тому времени, в течение которого пользователь не находился в состоянии системной блокировки).

`default_vat_rate`

Значение НДС по умолчанию.

`card_tel_uid_len`

Переменная задает длину логина для услуги телефонии по умолчанию.

`card_user_prefix`

Значение переменной добавляется к логину пользователя при авторегистрации. Пользователи, начало логина которых совпадает со значением переменной, считаются карточными.

`radius_max_session_age`

Переменная задаёт максимальный возраст открытых сессий, которые будут восстановлены из базы данных при старте сервера RADIUS. Сессия остаётся открытой в том случае, если был получен пакет RADIUS Accounting-Start, но по какой-либо причине не пришёл пакет Accounting-Stop. Значение пере-

менной задаётся в секундах. При значении 0 загрузка открытых сессий производиться не будет. Значение по умолчанию – 86400 (24 часа).

card_callback_enable

Если данный параметр равен 1, то при подключении услуги «Коммутируемый доступ» к абоненту автоматически устанавливается возможность воспользоваться Callback.

default_dialup_cid

Значение указанное в данном параметре будет автоматически указано в поле «Разрешенные CID» для услуги «Коммутируемый доступ» при регистрации абонентов по картам предоплаты.

default_dialup_csid

Значение указанное в данном параметре будет автоматически указано в поле «Разрешенные CSID» для услуги «Коммутируемый доступ» при регистрации абонентов по картам предоплаты.

special_write

Если указана данная опция, то ядро биллинговой системы будет делать записи в таблицу special_transactions. По умолчанию данная опция отключена.

tel_attrs_write

Если указана данная опция, то ядро биллинговой системы будет делать записи в таблицу tel_sessions_log_attrs, в которой хранятся все RADIUS-атрибуты для всех телефонных звонков. По умолчанию данная опция отключена.

dialup_attrs_write

Если указана данная опция, то ядро биллинговой системы будет делать записи в таблицу dhs_sessions_log_attrs, в которой хранятся все RADIUS-атрибуты для всех сессий услуг «Коммутируемый доступ». По умолчанию данная опция отключена.

access_attrs_write

Если указана данная опция, то ядро биллинговой системы будет делать записи в таблицу `dhs_access_log_attrs`, в которой хранятся все RADIUS-атрибуты для всех запросов на авторизацию. По умолчанию данная опция отключена.

Конфигурационный файл ядра

Конфигурационный файл ядра биллинговой системы доступен по пути `/netup/utm5/utm5.cfg`. Файл состоит из строк вида `параметр=значение`

В некоторых случаях возможно указание нескольких строк с одинаковым значением «параметр». Строки, начинающиеся с символа «#», считаются комментарием.

Список возможных параметров.

database_type

Тип базы данных. Возможны значения: `mysql`, `postgres`.

database

Название базы данных. По умолчанию: `UTM5`.

database_host

Адрес хоста, на котором располагается база данных. Значение по умолчанию: `localhost`.

database_login

Логин для доступа к базе данных.

database_password

Пароль для доступа к базе данных.

database_sock_path

Путь к unix-сокету, используемому для подключения к серверу базы данных. Используется только для базы данных MySQL и только в случае, когда параметр `database_host` не указан или его значение равно `localhost`. Значение по умолчанию `/tmp/mysql.sock`.

database_port

Номер порта для доступа к базе данных. Используется только для базы данных MySQL. Значение по умолчанию 3306.

dbcount

Количество соединений открываемых ядром биллинговой системы к базе данных. Значение по умолчанию 6.

database_reconnect_count

Количество попыток соединения с базой данных, если соединение не было установлено или количество попыток выполнения SQL-запроса, если его выполнение закончилось неудачно. Значение по умолчанию 5.

database_reconnect_sleep

Задержка в секундах перед повторной попыткой соединения с базой данных или перед повторным выполнением SQL-запроса. Значение по умолчанию 2.

pthread_attr_setstacksize

Размер памяти выделяемой под стек потоков. Значение по умолчанию 8 МБ.

urfa_bind_host

Хост, на котором будет прослушиваться TCP-порт для принятия URFA-запросов. По умолчанию сервер отключен. Значение `0.0.0.0` - на всех интерфейсах. Может быть несколько записей.

urfa_bind_port

Порт, на котором будет слушать сервер URFA. По умолчанию: 11758.

`urfa_lib_file`

Файл динамического модуля (.so), который будет загружен при старте ядра. Значения по умолчанию нет. Может быть указано несколько файлов. Путь может быть как абсолютным (/netup/utm5/lib/liburfa-utils.so), так и относительным (./liburfa/liburfa-utils.so, liburfa/liburfa-utils.so). В случае, если путь либо абсолютен, либо начинается с ./, перегрузка из центра управления UTM будет происходить корректно. Иначе будет загружен именно тот код, который был на момент запуска ядра.

`nfbuffer_port`

Порт, на котором ядро принимает поток NetFlow. По умолчанию: 9996.

`nfbuffer_host`

Хост, на котором будет прослушиваться UDP-порт для принятия NetFlow-потока. По умолчанию: 0.0.0.0 (все интерфейсы).

`log_level=3`

Уровень протоколирования ядра. Число от 0 до 3, большие и меньшие значения будут сброшены до ближайшей границы. Значение по умолчанию – 1. Чем выше уровень, тем больше сообщений попадает в основной поток логов. Уровень 3 – всё, 2 – всё без информационных сообщений, 1 – всё без замечаний, 0 – только ошибки.

`log_file_main`

Файл записи журнала уровня информации, замечаний, предупреждений, ошибок.

`log_file_debug`

Файл записи журнала отладочного уровня.

`log_file_critical`

Файл записи журнала уровня критических ошибок и сбоев.

Конфигурационный файл веб-интерфейса пользователя

Конфигурационный файл для веб-интерфейса пользователя называется `/netup/utm5/web5.cfg`. В данном файле записываются параметры доступа веб-интерфейса к ядру биллинговой системы.

Список возможных параметров.

`core_host`

Адрес хоста, на котором запущено ядро биллинговой системы. Значение по умолчанию: `127.0.0.1`.

`web_login`

Логин системного пользователя в биллинговой системе. Значение по умолчанию: `web`.

`web_password`

Пароль системного пользователя в биллинговой системе. Значение по умолчанию: `web`.

`traffic_detail_report`

Директива включает возможность отображения детального отчета по трафику в веб-интерфейсе пользователя. Принимает значение: `enable`.

Также для включения отображения детального отчета по трафику в файле `user_reports_traffic_menu.xml` (расположен в директории с cgi-скриптами UTM 5.0) необходимо раскомментировать сток:

```
<item name="user_reports_traffic_detail" mvalue="M_
REPORTS_TRAFFIC_DETAIL" href="user5?cmd=user_reports_
traffic_detail&key=" />
```

`traffic_detail_report_size`

Максимальное число выводимых записей детального отчета по трафику.

Список брандмауэров

Список брандмауэров содержит информацию о типе брандмауэра, его идентификационном имени (может быть IP-адрес). По этому имени происходит идентификация подключающихся модулей `utm5_rfw`.

Правила файрволов

В этом разделе администратором задаются команды, при выполнении которых на соответствующих удалённых маршрутизаторах происходит блокирование или разблокирование доступа клиентов в интернет. В свойствах раздела указываются: идентификатор брандмауэра, на котором выполнять команды; собственно команда для открытия доступа к ресурсам сети и команда для закрытия доступа к ресурсам. Если выполнение данных команд на конкретном маршрутизаторе актуально не для всех клиентов, то указывается идентификатор клиента, идентификатор группы, или идентификатор тарифа, для которых актуально выполнение команд для манипулирования доступом в сеть.

При задании команд для включения и выключения доступа к ресурсам сети можно использовать следующие переменные:

`UID` – идентификатор пользователя в системе;

`RULE_ID` – идентификатор пользователя плюс 5000;

`UIP` – IP-адрес (сеть) пользователя без маски, например, 10.0.0.1;

`UMASK` – маска подсети через точку, например, 255.255.255.255;

`UBITS` – маска в виде битов, например, 32 (означает то же, что и 255.255.255.255);

`UINVERTMASK` – инвертированная маска (используется при работе с маршрутизаторами Cisco), например, 0.255.255.255.

Пример для FreeBSD. Включение:

```
/sbin/ipfw add RULE_ID allow ip from UIP to any
```

Выключение:

```
/sbin/ipfw delete RULE_ID
```

Следует обратить внимание на то, что выполнение команд происходит не при их добавлении в список, а при включении и выключении нета для пользователя.

Более полную информацию по настройке файрволла можно найти в разделе «Использование файрволлов».

Список IP-зон

Справочник «Список IP-зон» ведётся для удобства работы с большими многоsegmentными и распределёнными сетями и содержит информацию о различных сегментах сети: сеть, маску и шлюз. IP-зону могут составлять один или несколько сегментов.

Список домов

Справочник подключенных домов ведётся для удобства работы с сетями, объединяющими несколько зданий. Запись о доме содержит его адрес и идентификатор IP-зоны.

Список банков

Данные из справочника банков предназначены для удобства заполнения форм. Например, при создании новых клиентов в системе, нет необходимости вводить данные банка клиента каждый раз. Достаточно один раз внести данные в список банков или импортировать списки из файла формата XML. С идентификатором банка в системе связаны следующие данные: БИК, название, адрес и корреспондентский счет банка.

Настройка и отладка работы с почтовым сервером

В интерфейсе администратора в разделе (Настройки | Список параметров) укажите корректно следующие параметры (через символ «=» указаны значения для примера):

smtp_relay = 10.0.0.1

smtp_port = 25

smtp_fqdn = host.example.org

smtp_sender = utm@host.example.org

smtp_subject = Message from UTM5

admin_email = utm@host.example.org

notification_borders = 5

notification_borders = 3

notification_borders = 0

notification_message = Уважаемый абонент, FULL_NAME!
На Вашем лицевом счёте номер ACCOUNT_ID возник дефицит средств в размере BALANCE. Дата сообщения: DATE Данное сообщение послано на EMAIL. С уважением, Провайдер.

notification_message_subject = Уведомление

notification_message_from = Отдел биллинга

Адреса электронной почты абонента, на которые производится рассылка уведомлений, можно задать в свойствах пользователя, в разделе «Контакты».

Для проверки корректности отсылки сообщений пользователям можно искусственно провести баланс пользователя через одну из указанных границ – 5, 3 либо 0 условных единиц. Это можно сделать внеся платеж на сумму 10 у. е. и затем оказав разовую услугу на 6, 8 либо 11 условных единиц. В этом случае баланс пользователя будет изменен с 10 у. е. до 4, 2 либо у. е.

При этом можно проверить прохождение пакетов к почтовому серверу командой:

```
tcpdump -ni eth0 port 25
```

где eth0 – интерфейс, через который осуществляется соединение с почтовым сервером.

Должны появиться пакеты примерно следующего вида:

```
12:45:34.738410 127.0.0.1.57021 > 127.0.0.1.25: . ack
1 win 35840 <nop,nop,timestamp 603505811 603505811>
(DF)
```

```
12:45:34.875100 127.0.0.1.25 > 127.0.0.1.57021: P
1:37(36) ack 1 win 35840 <nop,nop,timestamp 603505824
603505811> (DF)
```

```
12:45:34.875187 127.0.0.1.57021 > 127.0.0.1.25:
P 1:16(15) ack 37 win 35840 <nop,nop,timestamp
603505824 603505824> (DF)
```

```
12:45:34.875249 127.0.0.1.25 > 127.0.0.1.57021:
P 37:59(22) ack 16 win 35840 <nop,nop,timestamp
603505824 603505824> (DF)
```

Если пакеты есть, но почтовые сообщения не приходят к абонентам, то необходимо убедиться в правильности настройки почтового сервера. Подробная информация о его настройке приведена в его документации, а возможные причины некорректной работы можно извлечь из файлов журнала почтового сервера.

Ещё один способ инициировать отправку почтовых сообщений пользователям – выполнить отсылку счёта на адрес электронной почты абонента. Для этого необходимо оказать пользователю разовую услугу, в результате чего будет подготовлен счёт в разделе (Отчёты | Счета). Необходимо выделить подготовленный счёт и нажать кнопку «Отослать на email». При этом в файле журнала ядра UTM должна появиться запись:

```
?Debug : Jul 21 12:54:04 BusLogic: call SmtplibLogger::
smtp
```

При прослушивании трафика должны появляться пакеты, отправленные на почтовый сервер.

Если все шаги проходят успешно и почтовые сообщения попадают в почтовые ящики абонентов, то настройку связи с почтовым сервером можно считать успешной.

Использование файрволов

Файрвол (брандмауэр) – это программа, которая, основываясь на некоторых правилах, разрешает или запрещает передачу информации, проходящей через маршрутизатор, с целью ограждения сети от внешнего доступа или, наоборот, для недопущения прохождения IP-пакетов во внешние сети.

Включение и выключение доступа в интернет пользователям в биллинговой системе UTM осуществляется посредством добавления и удаления правил файрвола. По умолчанию, прохождение пакетов через маршрутизатор для пользователей закрыто. При включении интернета пользователям в файрвол добавляются правила, разрешающие прохождение пакетов до и с IP-адреса пользователя, заведенного в биллинговой системе UTM.

Кроме того, файрвол используется для трансляции сетевых адресов (NAT, Network Address Translation). Технология NAT сводится к подмене в заголовках IP-пакетов приватного IP-адреса источника данных, IP-адресом внешнего интерфейса маршрутизатора. Использование технологии NAT позволяет машинам, не имеющим реальных IP-адресов, практически полноценно работать в сети интернет.

Система NetUP UTM поддерживает работу с удалёнными брандмауэрами для блокирования доступа клиентов к ресурсам сети. Блокирование может производиться как автоматически (например, при появлении задолженности на счету клиента), так и вручную (самим клиентом или администратором). Состояние физической блокировки доступа в сеть определяется статусом интернета для данного пользователя. Статус может принимать два значения: включен или выключен.

Настройка политики безопасности файрвола в ОС Linux с ipchains и iptables

Запрет прохождения пакетов пользователям по умолчанию в ОС Linux осуществляется настройкой политики безопасности (policy) в цепочке forward в файрволах ipchains или iptables.

Настройка политики безопасности в ipchains:

```
ipchains -P forward DENY
```

Настройка политики безопасности в iptables

```
iptables -P FORWARD DROP
```

Проверка правил файрвола в ipchains или iptables осуществляется выполнением команд.

В ipchains:

```
[root@rh73 /]# ipchains -nL
Chain input (policy ACCEPT):
Chain forward (policy DENY):
Chain output (policy ACCEPT):
[root@rh73 /]# _
```

В iptables:

```
[root@rh73 /]# iptables -nL
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy DROP)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
[root@rh73 /]# _
```

Включение поддержки файрвола в ОС FreeBSD

По умолчанию ОС FreeBSD устанавливается с ядром GENERIC, в которое не включена поддержка файрвола. Для использования файрвола в ОС FreeBSD, ядро системы следует пересобрать с опцией

```
options IPFIREWALL
```

Файрвол ipfw в ОС FreeBSD также может быть загружен в форме модуля. С этой целью в файл `/boot/loader.conf` следует добавить строку

```
ipfw_load="YES"
```

Для включения запуска файрвола при загрузке ОС FreeBSD в конфигурационный файл `/etc/rc.conf` следует добавить строку

```
firewall_enable="YES"
```

В процессе загрузки системы правила файрвола подгружаются из конфигурационного файла `/etc/rc.firewall`. Если необходимо разрешить прохождение пакетов к серверу и от него, то в этом файле необходимо прописать следующие правила:

```
fwcmd="/sbin/ipfw -q"
${fwcmd} -f flush
${fwcmd} add 100 allow ip from any to me
${fwcmd} add 200 allow ip from me to any
```

При загрузке правил `ipfw`, последнее правило, по умолчанию, запрещает прохождение пакетов через маршрутизатор.

Просмотр загруженных правил файрвола осуществляется командой.

```
server# ipfw show
00100 8 736 allow ip from any to me
00200 8 596 allow ip from me to any
65535 0 0 deny ip from any to any
server# _
```

Настройка файрвола на маршрутизаторе Cisco

Управление доступом в сеть осуществляется динамическими `access-list`. Необходимо создать два листа – для прохождения пакетов к клиенту и от него. Для этого перейдите в режим конфигурирования маршрутизатора командой.

```
configure terminal
```

Затем выполните команды.

```
access-list 105 dynamic test1 permit ip any any
access-list 106 dynamic test2 permit ip any any
```

При этом будут созданы два динамических access-list, в которые будут добавляться правила для разрешения выхода пользователей в сеть. Если необходимо определенному адресу разрешить доступ в сеть статически, то необходимо выполнить команду.

```
access-list 105 permit ip host 10.0.0.10 any
access-list 106 permit ip any host 10.0.0.10
```

Важно! Добавьте разрешение для адреса хоста, с которого осуществляется администрирование маршрутизатора. В противном случае возможна потеря управления.

Остальные правила будут добавляться в лист динамически в зависимости от статуса Интернета у абонента. По умолчанию доступ для всех абонентов закрыт.

Созданные листы необходимо привязать к интерфейсу на маршрутизаторе. Рекомендуется привязку делать на интерфейсе, к которому непосредственно подключаются абоненты. Для этого выполните команды.

```
interface Ethernet 1/0
ip access-group 105 in
ip access-group 106 out
```

Добавление и удаление правил на маршрутизаторе осуществляется по протоколу rsh, поэтому необходимо разрешить выполнять эти действия на маршрутизаторе командами:

```
CiscoRouter#conf t
CiscoRouter(config)#username netup privilege 8 password 0 plain_text_password
CiscoRouter(config)#ip rcmd rsh-enable
CiscoRouter(config)#no ip rcmd domain-lookup
CiscoRouter(config)#ip rcmd remote-host netup REMOTE_IP_ADDRESS REMOTE_USER_NAME enable
CiscoRouter(config)#privilege exec level 8 access-template
CiscoRouter(config)#privilege exec level 8 clear access-template
```

REMOTE_IP_ADDRESS – IP-адрес сервера с запущенным utm5_rfw.

REMOTE_USER_NAME – имя пользователя на сервере с utm5_rfw, от которого производится запуск сборщика. Имя по умолчанию – netup.

После настройки маршрутизатора сохраните конфигурацию командой write.

В интерфейсе администратора правила для включения интернета пользователю будут выглядеть следующим образом:

```
access-template 105 test1 host UIP any
access-template 106 test2 any host UIP
```

Правила для выключения:

```
clear access-template 105 test1 host UIP any
clear access-template 106 test2 any host UIP
```

Непосредственная отправка правил на маршрутизатор Cisco по протоколу rsh осуществляется модулем utm5_rfw. В конфигурационном файле rf5w.cfg обязательно должны быть указаны параметры:

```
firewall_type=cisco
cisco_ip=IP_ADDRESS
```

где IP_ADDRESS – IP-адрес маршрутизатора Cisco.

После этого произведите запуск utm5_rfw командой

```
/netup/utm5/bin/utm5_rfw
```

Для проверки прохождения правил на маршрутизатор Cisco можно использовать команду

```
tcpdump -nXli eth0 -s 65000 port 514
```

Пример настройки Cisco при работе с Windows

```
CiscoRouter(config)#username Administrator privilege
8 password 0 plain_text_password
CiscoRouter(config)#ip subnet-zero
```

```
CiscoRouter(config)#no ip rcmd domain-lookup
CiscoRouter(config)#ip rcmd rsh-enable
CiscoRouter(config)#ip rcmd remote-host Administrator
REMOTE_IP_ADDRESS REMOTE_USER_NAME enable
```

В данном примере необходимо настроить запуск служб Windows таким образом, чтобы они работали от имени учётной записи Administrator (по умолчанию все службы Windows запускаются от имени учётной записи SYSTEM).

Использование NAT

Использование NAT в ОС FreeBSD с ipfw

Для использования NAT в ОС FreeBSD необходимо пересобрать ядро системы с опцией IPDIVERT.

Для этого в конфигурационный файл нового ядра следует добавить строку.

```
options IPDIVERT
```

Трансляция сетевых адресов в ОС FreeBSD осуществляется посредством демона natd, который слушает порт 8668.

Для включения NAT при загрузке системы в конфигурационном файле /etc/rc.conf следует добавить строки.

```
natd_enable=«YES»
natd_interface=«rl0»
```

Указать на автоматический запуск демона natd при загрузке системы можно так же в файле /etc/rc.local. В него следует добавить строку.

```
/sbin/natd -n rl0
```

Проверить, запущен ли демон natd, можно выполнив команду.

```
server# ps ax | grep natd
145 ?? Is 0:00.51 /sbin/natd -n rl0
server# _
```

Проверить, слушает ли демон `natd` порт 8668, можно выполнив команду.

```
server# sockstat | grep 8668
root natd 145 3 div4 *:8668 *:*
server# _
```

При трансляции сетевых адресов перенаправление пакетов на порт 8668 осуществляется посредством файрвола.

Для перенаправления всех пакетов на интерфейс, на IP-адрес которого транслируются сетевые адреса (NAT), следует выполнить команду.

```
ipfw add 50 divert natd ip from any to any via rl0
```

Если необходимо транслировать определенную сеть, например, 192.168.0.0/16, то необходимо выполнить команды.

```
ipfw add 50 divert natd ip from 192.168.0.0/16 to any
via rl0
ipfw add 50 divert natd ip from any to me via rl0
```

Правила, осуществляющие перенаправление пакетов на `natd`, должны находиться в самом начале списка правил `ipfw`.

```
00050 0 0 divert 8668 ip from any to any via rl0
00200 8 736 allow ip from any to me
00300 8 596 allow ip from me to any
65535 0 0 deny ip from any to any
```

Для того чтобы правила, осуществляющие перенаправление пакетов на `natd`, выполнялись при загрузке системы, в конфигурационный файл `/etc/rc.firewall` необходимо добавить строки:

```
${fwcmd} add 50 divert 8668 ip from any to any via
rl0
```

или

```
${fwcmd} add 50 divert natd ip from 192.168.0.0/16 to
any via rl0
${fwcmd} add 50 divert natd ip from any to me via rl0
```

Строки, которые необходимо добавить в самое начало списка правил:

```
fwcmd="/sbin/ipfw -q"
${fwcmd} -f flush
${fwcmd} add 50 divert 8668 ip from any to any via
r10
${fwcmd} add 100 allow ip from any to me
${fwcmd} add 200 allow ip from me to any
```

В указанных выше примерах предполагается, что трансляция IP-адресов осуществляется на IP-адрес интерфейса `r10`. Вместо него следует указать название интерфейса, на IP-адрес которого необходимо осуществлять NAT.

Для того чтобы посмотреть сетевые интерфейсы в системе, необходимо выполнить команду `ifconfig`.

Использование NAT в ОС Linux

Трансляция сетевых адресов в `iptables` осуществляется в таблице `nat` в цепочке `POSTROUTING`. Для того чтобы транслировать адреса сети `192.168.0.0/16` на IP-адрес интерфейса `eth0` с IP-адресом `195.161.112.6`, необходимо выполнить следующую команду.

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o
eth0 -j SNAT --to-source 195.161.112.6
```

где `192.168.0.0/16` – адрес локальной сети;

`eth0` – внешний интерфейс с IP-адресом `195.161.112.6`, на который осуществляется NAT.

Посмотреть список текущих правил `iptables` в таблице `nat` можно, выполнив команду.

```
[root@rh73 /]# iptables -t nat -nL
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
SNAT all -- 192.168.0.0/16 0.0.0.0/0 to:195.161.112.6
```

```
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
[root@rh73 /]# _
```

Переход на другой файрвол в ОС Linux

Последовательность перехода в Linux с ipchains на iptables.

Необходимо отключить ipchains, чтобы предотвратить загрузку соответствующих модулей в будущем.

```
chkconfig --level 0123456 ipchains off
```

Необходимо остановить сервис ipchains.

```
service ipchains stop
```

Если ipchains загружен в форме модуля ядра Linux, его необходимо выгрузить.

```
rmmmod ipchains
```

Включить iptables на автозагрузку.

```
chkconfig --level 235 iptables on
```

Активировать сервис iptables.

```
service iptables start
```

Переход с iptables на ipchains осуществляется аналогичным образом. После остановки iptables необходимо выгрузить все загруженные для его работы модули ядра Linux. Посмотреть, какие модули ядра загружены, можно, выполнив команду lsmod.

Некоторые модули ядра, которые используются для iptables.

```
[root@rh73 /]# lsmod | grep ip
ip_table_nat
ip_conntrack
ip_table_filter
ip_tables
[root@rh73 /]# _
```

Также следует проверить конфигурационный файл программы `sudo`, в нём должна быть записана строка на выполнение исполняемого файла файрвола, на который осуществляется переход.

```
nobody ALL= NOPASSWD: /sbin/iptables
```

Автосохранение правил файрвола в Linux при перезагрузке системы

Для того, чтобы при перезагрузке маршрутизатора сохранялись текущие правила файрвола `ipchains` или `iptables`, следует изменить конфигурационные файлы.

Для `ipchains` в файле `/etc/init.d/ipchains` после строки `stop()`

добавить запись

```
/sbin/ipchains-save > /etc/sysconfig/ipchains
```

Для `iptables` в файле `/etc/init.d/iptables` после строки `stop()` {

добавить запись

```
/sbin/iptables-save > /etc/sysconfig/iptables
```

Добавление правил файрвола в центре управления

Добавление правил файрвола осуществляется в администраторском интерфейсе биллинговой системы UTM в закладке (Настройки | Правила файрволов).

Таблица отображает шаблоны команд, по которым строятся и выполняются конкретные команды при включении и выключении интернета пользователя.

Пользователи и группы Тарификация Картонки Настройки Счеты Дополнительно О программе									
Список параметров Список брендмауэров Правила фтпчал Список NAS Список P-лов Дома Список банков Шаблоны договоров Провайдер									
Добавить Редактировать Обновить									
ID	Все пользователи	ID пользователя	Группа	Тариф	Включение	Выключение	Брендмауэр		
1	0	1	0	0	iptables -w RULE_ID -s 10.10.10.1 -j ACCEPT	iptables -w RULE_ID -j ACCEPT	1		
2	0	1	0	0	iptables -w FORWARD -j ACCEPT	iptables -w FORWARD -j ACCEPT	2		
3	0	0	100	0	iptables -w FORWARD -j ACCEPT	iptables -w FORWARD -j ACCEPT	2		

Команды, в которых поле «ID пользователя» соответствует идентификатор конкретного пользователя, выполняются при включении и выключении интернета только данному пользователю. То же относится к значениям полей «ID группы» и «ID тарифа»: они выполняются при включении и выключении интернета пользователям, входящим в конкретную группу или подписанным на конкретный тариф соответственно. Если установлена галочка «Все пользователи», то команда выполняется при включении и выключении интернета любому пользователю. Если на одного пользователя приходится несколько команд, то они выполняются в порядке возрастания идентификатора.

При добавлении нового правила, помимо вышеописанных параметров необходимо указать команду для включения интернета, команду для выключения и идентификатор брандмауэра.

Для построения шаблонов команд, выполняемых при включении и выключении интернета, доступны следующие переменные, которые заменяются непосредственно при выполнении команды соответствующими значениями:

UID – идентификатор пользователя в системе;

RULE_ID – идентификатор пользователя + 5000;

UIP – IP-адрес (сеть) пользователя без маски, например 10.0.0.1;

ULOGIN – логин пользователя из IP-группы;

UMASK – маска подсети через точку, например 255.255.255.255;

UBITS – маска подсети в виде битов, например 32;

UINVERTMASK – инвертированная маска (используется при работе с Cisco), например 0.255.255.255;

SLINK_ID – идентификатор сервисной связки услуги IP-трафика;

SPLINK_ID – идентификатор сервисной связки услуги IP-трафика + 10000.

Например, команды для добавления правил, разрешающих пользователю выход в интернет по любому протоколу и порту при использовании FreeBSD будут выглядеть так:

```
/sbin/ipfw add RULE_ID allow ip from UIP/UBITS to any
/sbin/ipfw add RULE_ID allow ip from any to UIP/UBITS
```

Команда для удаления правил:

```
/sbin/ipfw delete RULE_ID
```

При использовании Linux с ipchains команды будут выглядеть примерно так:

Включение:

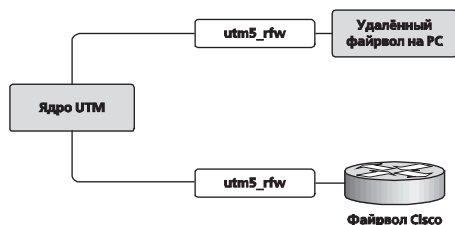
```
/sbin/ipchains -A forward -b -s UIP/UBITS -j ACCEPT
```

Выключение:

```
/sbin/ipchains -D forward -b -s UIP/UBITS -j ACCEPT
```

Также можно добавлять правила, запрещающие доступ на определенные порты или ресурсы, либо ограничивающие скорость скачивания из интернета.

Полностью подготовленные для выполнения правила передаются на исполнение соответствующему модулю utm5_rfw. Количество зарегистрированных в ядре биллинговой системы модулей utm5_rfw не ограничено.



Следует обратить внимание, что выполнение команд для включения и выключения интернета производится через `sudo`, поэтому нужно следить за тем, чтобы права на исполнение этих команд были заданы в файле `sudoers` для пользователя, от которого будет запущен `utm5_rfw`. В целях безопасности рекомендуется запускать `utm5_rfw` от пользователя `nobody` и в файле `sudoers` указывать разрешение на выполнение только определенных команд от этого пользователя.

Параметры запуска `utm5_rfw`

При запуске модуля `utm5_rfw` необходимо в командной строке указать путь к конфигурационному файлу. Например:

```
utm5_rfw /netup/utm5/rfw5.cfg
```

Если при запуске модуля не был указан путь к конфигурационному файлу, то по умолчанию параметры будут взяты из файла `/netup/utm5/rfw5.cfg`.

Версию программы и список загружаемых параметров можно увидеть, запустив команду

```
utm5_rfw -v
```

Для того чтобы при запуске модуля произошла синхронизация правил фаервола с сервером UTM, нужно запустить команду

```
utm5_rfw -f
```

Синхронизацию правил рекомендуется использовать при автоматическом запуске модуля при старте системы.

Файл конфигурации `utm5_rfw`

Файл состоит из строк вида

параметр=значение

Строки, начинающиеся с символа «#», считаются комментарием.

Список возможных параметров:

r fw_name

Имя модуля, по которому происходит идентификация модулей. Например, 127.0.0.1. Это же значение должно быть указано при добавлении записи в список брандмауэров. При включении или выключении интернета пользователям именно по этому полю происходит идентификация файрвола, на котором производится выполнение команд.

sudo_path

Путь к программе sudo. Например, /usr/bin/sudo.

firewall_path

Путь к файрвол. Например, /sbin/ipfw.

firewall_flush_cmd

Команда для очистки правил файрвола. Например, /sbin/iptables -F.

core_host

Адрес хоста, на котором запущено ядро биллинговой системы. Значение по умолчанию: 127.0.0.1.

core_port

Порт, на котором запущено ядро биллинговой системы. Значение по умолчанию: 11758.

r fw_login

Логин системного пользователя в биллинговой системе.

r fw_password

Пароль системного пользователя в биллинговой системе.

firewall_type

Тип файрвола. Возможные значения: local, cisco.

cisco_ip

IP-адрес маршрутизатора фирмы Cisco, управление которым производится по протоколу rsh.

dont_fork

Если не указана данная опция либо значение не равно “yes”, то правила выполняются параллельно т.е. последующее правило применяется на файрволле не дожидаясь выполнения предыдущего. На некоторых типах файрволл, в частности для linux iptables, крайне рекомендуется указать данную опцию равную “yes”. При этом правила применяются на файрволле последовательно.

Включение интернета пользователям осуществляется через центр управления или через веб-интерфейс пользователя системы.

Работа с предоплаченными картами

Добавить, просмотреть или экспортировать информацию о предоплаченных картах можно в разделе «Карточки». Для удобства работы карточки объединяются в группы (пулы).

Вновь созданные карты добавляются в пул: новый или уже существующий. Чтобы добавить карточки в существующую группу, в окне «Добавление карты» нужно указать её номер. Если не существует пула с указанным номером, то такой пул автоматически создаётся, и в него добавляются карты.

Параметры карты	
Идентификатор пула	34
Количество	1000
Баланс	200
Валюта	RUR
Длина ПИН-кода	12
Использовать до	Oct 31, 2006 Выбрать
Service ID	0 Выбрать

Ok Отмена

Для создания пула карт или добавления новой партии карт в уже существующий пул в меню добавления карт кроме номера пула нужно указать количество генерируемых карт, номинал карт, валюту, длину пин-кода и срок действия карт. Информацию о созданных картах нельзя изменить или удалить. Пулы также не могут быть удалены.

Различаются два типа предоплаченных карт: карты с фиксированной датой истечения срока действия и карты с плавающей датой истечения срока действия.

Карты первого типа используются для регистрации пользователей в системе, которые смогут воспользоваться услугами провайдера до даты, указанной на карте. Для создания карт этого типа достаточно выставить значение поля «Использовать до» позднее текущей даты.

Карты второго типа используются для регистрации пользователей в системе, которые смогут воспользоваться услугами провайдера определённое количество дней, начиная с момента активации карты. После активации карты такого типа её дата истечения срока действия устанавливается в значение даты активации плюс заданное количество дней. Для создания карт этого типа необходимо при выставлении значения поля «Использовать до» отметить в календаре галочку «Infinity date» и выставить значение поля «Дни» в величину большую нуля, эта величина регламентирует количество дней в течении которых пользователь сможет воспользоваться услугами. Если галочка «Infinity date» снята, то система игнорирует значение поля «Дни» и генерирует карты первого типа (с фиксированной датой истечения срока действия).

При достижении даты, когда срока действия карты истекает, система обнуляет баланс пользователя. Таким образом, пользователи не смогут более воспользоваться услугами провайдера.

В списке существующих карт присутствует информация о номере карты, её пин-коде (пароле), сроке действия, валюте и дате активации (если карта уже активирована).

Информацию о prepaid картах можно экспортировать в файл формата XML, который имеет следующий формат:

```
<?xml version="1.0" encoding="UTF-8" ?>
<UTM>
  <pool id="1">
    <card id="1" secret="56205393" balance="100.0"
      currency="810" expire_date="31.12.2004" />
    <card id="2" secret="95672099" balance="100.0"
      currency="810" expire_date="31.12.2004" />
  </pool>
</UTM>
```

id – идентификатор пула (карты);

secret – пароль (пин-код) карты;

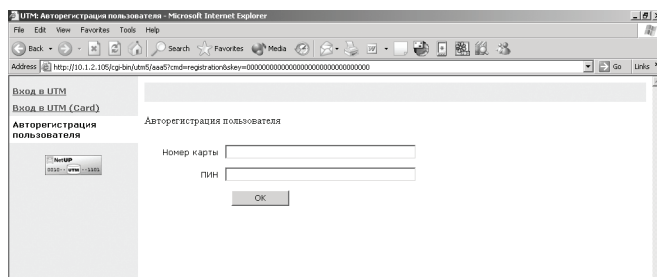
balance – номинал карты;

currency – идентификатор валюты, в которой выражен номинал карты;

expire_date – дата истечения срока действия карты в формате ДД.ММ.ГГГГ.

При создании карт имеется возможность указать (привязать к карте) тарифный план, услуги которого будут привязаны к основному лицевому счету пользователя при автоматической активации карты. При активации карты к основному лицевому счету пользователя привязываются только услуги, относящиеся к типам «Hotspot», «Коммутируемый доступ» и «Телефония», если помимо этих типов услуг тарифный план содержит услуги других типов, то такие услуги не подключаются.

Для активации карты пользователю необходимо зайти на страницу автоматической регистрации и ввести корректные данные с карты.

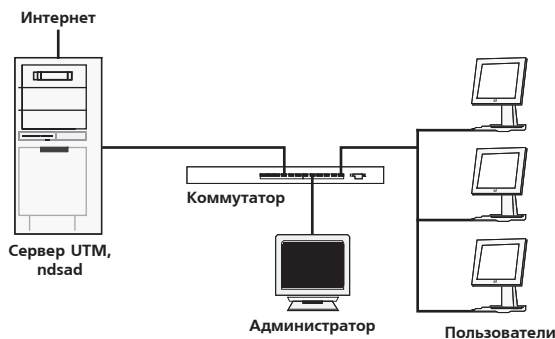


Если данные введены верно, то в системе будет создан пользователь с логином card_NUM, где вместо NUM будет указан номер карты, и паролем, равным пин-коду карты. Баланс пользователя будет равен балансу активированной карты, и при этом карта будет помечена, как активированная. Если к активируемой карте привязан тарифный план, тогда к основному лицевому счету пользователя подключаться услуги из этого тарифного плана со значениями логина и пароля такими же вновь созданный пользователь. С лицевого счета пользователя снимутся средства в размере суммы стоимостей периодических составляющих услуг, входящих в состав тарифного плана.

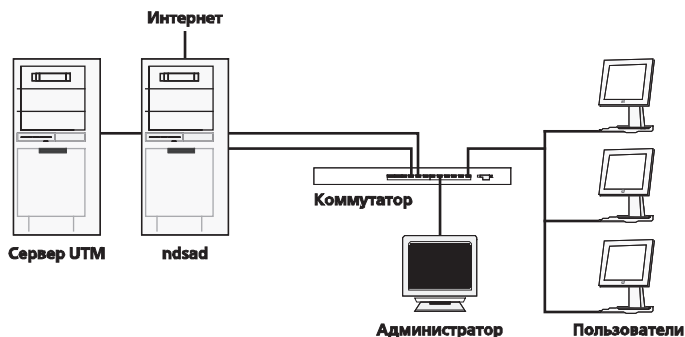
NetUP Data Stream Accounting Daemon (ndsad)

В общем случае возможны два способа включения в сеть:

- ndsad и биллинговая система UTM работают на одном сервере, служащем маршрутизатором между локальной и глобальной сетями;



- ndsad запускается на роутере, а биллинговая система – на удаленном сервере, находящемся либо внутри локальной сети, либо вне её.



В первом случае на роутере запущены демон ndsad, регистрирующий прошедший через роутер трафик, и ядро биллинговой системы, получающее и обрабатывающее полученную информацию о трафике. Для обмена данными между демоном ndsad и ядром системы используется протокол UDP, данные передаются в формате NetFlow версии 5. Для правильной ра-

боты системы в рассмотренной конфигурации необходимо направить поток UDP-пакетов, содержащих информацию о трафике, на локальную машину на порт, «прослушиваемый» ядром системы. Порт UDP и хост для принятия данных о трафике задаются в конфигурационном файле `/netup/utm5/utm5.cfg`. Если статистика собирается с локальной машины, то хостом для принятия данных следует указать `127.0.0.1`.

Для настройки демона `ndsad` необходимо внести изменения в файл `/netup/utm5/ndsad.cfg`. Если поток NetFlow необходимо направить на локальную машину, то значение параметра `ip` должно быть равным `127.0.0.1`, значение параметра `port` – `9996`.

Для правильной работы демона `ndsad` в файле конфигурации необходимо указать семейство интерфейсов, на которых нужно собирать информацию о трафике. Список интерфейсов можно узнать при помощи системной команды `ifconfig`. Интерфейсы, на которых необходимо собирать статистику, указываются с помощью параметра `force`. Нужно иметь в виду, что если вы не используете транслирование адресов (NAT) и включите сбор статистики с внешнего и внутреннего интерфейсов, то трафик на клиентов будет удваиваться, так как проходящие пакеты будут регистрироваться два раза: при входе в маршрутизатор и при выходе из него.

В ОС FreeBSD `ndsad` запускается командой:

```
/usr/local/etc/rc.d/ndsad.sh start
```

В ОС Linux `ndsad` запускается командой:

```
/etc/rc.d/init.d/ndsad start
```

В Windows NT-подобных системах `ndsad` работает в качестве системной службы. Для установки и удаления службы используются ключи командной строки `--install` и `--uninstall` соответственно. Служба устанавливается в автоматическом режиме, что обеспечит её запуск при старте компьютера.

```
C:\Program Files\NetUP\UTM5>ndsad.exe --install  
Successfully created ndsad service
```

```
C:\Program Files\NetUP\UTM5>ndsad.exe --uninstall  
Successfully deleted ndsad service
```

Если этого не наблюдается, нужно проверить настройки демона `ndsad` (файл `ndsad.cfg`). Полное описание структуры файла `ndsad.cfg` приводится ниже.

После того, как данные о трафике появятся в детальном отчете по трафику, демон ndsad в связке с биллинговой системой готов к работе.

Получить последнюю версию ndsad можно на сайте проекта в Интернете – <http://sourceforge.net/projects/ndsad> . При этом необходимо отметить, что данный коллектор так же доступен в виде исходных кодов, что позволяет при необходимости самостоятельно вносить изменения

Конфигурационный файл

В файле допустимы пустые строки. Весь остаток строки, идущий после символа # считается комментарием и игнорируется.

Синтаксис строк:

<слово> <значение>

Если пропущено значение или неправильно написано ключевое слово, демон выдаст при старте предупреждение, которое не попадет в журнал. Ошибки в конфигурационном файле не приведут к сбою в старте демона, и ndsad запустится.

«Семьей» устройств называются сетевые устройства, отличающиеся только индексом. Например, в семью eth входят устройства: eth0, eth1, eth12 и т. д.

Значением параметра может быть одно неразрывное слово (кроме параметров heap и hash). Если имеется несколько значений параметра (например, нужно обрабатывать несколько устройств), то параметр должен задаваться несколько раз:

```
force rl0
```

```
force fxp0
```

Ключевые слова

ip

Адрес назначения. По этому адресу (и порту) будет происходить отсылка статистики по трафику. Значение по умолчанию: ip 127.0.0.1.

Пример: ip 10.0.0.1.

port

Порт назначения. См также ip. Значение по умолчанию: port 9996.

Пример: port 10001.

force

Указанные здесь устройства будут обрабатываться в любом случае. Кроме тех, которые не поддерживаются. Это ключевое слово имеет больший приоритет, чем ignore и dummy. В конце главы приведён список поддерживаемых устройств.

Пример: force eth0.

ignore

Строка указывает на то, что указанное устройство не будет обрабатываться. См. также ключевое слово force.

Пример: ignore eth0.

На платформе Win32 в опциях force и ignore вместо имён интерфейсов возможно задание любого из IP-адресов, на которые это устройство настроено.

Пример для платформы Win32:

```
force \Device\NPF_{A07050FE-62B3-40AF-B6D2-658701A56089}
```

```
ignore 192.168.1.1
```

```
force 192.168.0.1
```

dummy

Строка указывает на то, что все устройства из этой семьи не будут обрабатываться. См. также force. Указание в качестве семьи ключевого слова all приведёт к тому, что все устройства, не помеченные, как force, будут игнорироваться.

Пример: `dummy eth.`

promisc

Строка указывает на то, что устройство должно быть помещено в режим прослушивания всех пакетов, проходящих по сети. Отсутствие этой строки не гарантирует, что устройство не будет находиться этом режиме.

Пример: `promisc ex0.`

filter

Фильтр для ограничения количества обрабатываемых пакетов. Формат фильтра аналогичен формату фильтров для `tcpdump` (man `tcpdump`).

Пример: `filter fxp0 not port 135`

Пример: `filter fxp0 net 10.0.0.0/24 and not port 135`

hash

Размер хеша для семьи устройств. Это значение должно быть степенью двойки. Иначе использование памяти будет очень неэффективным. Значение по умолчанию: `hash all 128.`

Пример: `hash lo 64.`

heap

Размер буфера хранения. Такой максимальный объём памяти в байтах может быть занят, но не обязательно использован. В случае необходимости память берётся из этой кучи, а не у системы. Разумные размеры увеличивают быстродействие. Значение по умолчанию: `heap 16384.`

Пример: `heap 65536.`

dump

Насколько часто будет происходить запись информации о загрузке разных частей демона в журнал. Измеряется в секун-

дах. Указание значения 0 приведёт к тому, что записи не будут происходить. Статистику можно получить, послав программе сигнал `SIGUP`. Значение по умолчанию: `dump 0`.

Пример: `dump 5`.

`log`

Файл, в который будет записываться журнал работы демона. Если значение не указано, то будет использован `stderr` (стандартный вывод для ошибок, обычно прямо на терминал). Значение по умолчанию: `/netup/utm5/log/ndsad.log`.

Пример: `log /var/log/ndsad.log`.

`config`

Изменить конфигурационный файл. Текущий файл после такой директивы не используется. Проверок на циклы нет, поэтому неправильное указание следующего файла может привести к тому, что программа зависнет. Значение по умолчанию: `config /netup/utm/ndsad.cfg`.

Пример: `config /usr/local/etc/ndsad.cfg`.

`bsd_div_port`

Порт, на который необходимо производить перенаправление (копирование) трафика из `ipfw` методом `divert (tee)`. Для использования данного функционала необходимо добавить следующее примерное правило в `ipfw`:

```
ipfw add 10 tee 21000 all from any to any
```

В данном примере используется порт 21000, соответственно запись в конфигурационном файле должна выглядеть следующим образом:

```
bsd_div_port 21000
```

Значение по умолчанию не предусмотрено. Данный функционал доступен только под ОС FreeBSD.

bsd_div_copy

В случае если правило в файрволл добавляется с использованием директивы divert вместо tee, то необходимо установить данную опцию равную значению yes. В противном случае пакеты не будут проходит.

ulog_group

Номер группы используемый при сборе статистики через интерфейс ULOG в ОС Linux при использовании файрвола iptables. Пример использования:

```
ulog_group 13
```

В этом примере указано использовать группу с номером 13. Соответственно правила в файрволл необходимо добавлять примерно следующей командой:

```
iptables -A OUTPUT -s 10.0.0.1 -d 10.0.0.2 -j  
ULOG --ulog-nlgroup 13
```

В случае если в лог-файле появляются ошибки вида “No buffer space available”, то необходимо увеличить системные сетевые буферы командой:

```
sysctl -w net/core/rmem_max=1048576
```

```
sysctl -w net/core/rmem_default=1048576
```

Значение по умолчанию для данной директивы не предусмотрено.

Список поддерживаемых семей устройств

Для ОС семейства BSD: vlan, bfe, tun, ng, nv, lo, dc, fxp, pcn, rl, sf, sis, ste, tl, tx, vr, wb, xl, de, txp, vx, bge, em, gx, lge, nge, sk, ti, wx, cx, ed, el, ep, ie, is, le, ex, lnc, my, wi, an.

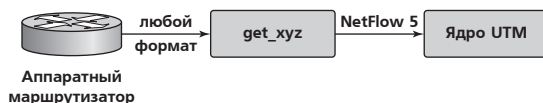
Для ОС семейства Linux: lo, eth, ppp.

На платформе Win32 в стандартной поставке поддерживаются устройства Ethernet, которые объединены в семейство eth и устройства связанные с VPN-соединениями, которые имеют имена \Device\NPF_GenericDialupAdapter либо \Device\NPF_GenericNdiswanAdapter.

Универсальные сборщики статистики

Ядро биллинговой системы NetUP UTM 5 рассчитано на сбор статистики по протоколу NetFlow v. 5. Для приведения статистики в формат NetFlow предназначен универсальный сборщик статистики NetUP `get_xyz`. Сборщик написан на языке C++ и поставляется в исходных кодах. Благодаря этому возможен сбор статистики и преобразование в NetFlow v.5 практически с любых устройств или файлов. При этом также имеется возможность запускать неограниченное число сборщиков `get_xyz` и отправлять статистику в одно ядро биллинговой системы.

Схема сбора статистики с использованием NetUP `get_xyz`



Утилита `get_xyz` в стандартной поставке имеет возможность собирать статистику по трафику с маршрутизаторов Cisco IP-Accounting, Mikrotik, NSG, Revolution и передачи ее по протоколу Cisco NetFlow v5 либо сохранения в файл. Запуск осуществляется командой:

```
/netup/utm5/bin/get_xyz
```

Ключи командной строки запуска:

- d – запустить в режиме демона
- l LOGFILE – выводить отладочную информацию в файл LOGFILE
- k – остановить запущенный процесс
- h – помощь.

Конфигурационный файл расположен по следующему пути:

```
/netup/utm5/get_xyz.conf
```

Файл состоит из строк вида

параметр=значение

Строки, начинающиеся с символа «#», считаются комментарием.

Список возможных параметров:

```
outfile=/tmp/traffic.log
```

Файл, в который будет сохраняться статистика.

```
outhost=127.0.0.1
```

IP-адрес сервера, на который передается статистика по протоколу NetFlow v. 5.

```
outport=9996
```

Порт, на который передается статистика по протоколу NetFlow v.5.

```
loop=600
```

Интервал (в секундах), через который производить снятие статистики. Если этот параметр не указан, то статистика снимается один раз, после этого выполнение программы завершается.

Раздел конфигурационного файла указания устройств, с которых снимается статистика. Настройки для каждого маршрутизатора заключаются в фигурные скобки {}.

```
host {
```

```
    type=nsg
```

Тип маршрутизатора, с которого снимается статистика. Возможные значения: cisco, revolution, mikrotik, nsg.

```
ip=192.168.0.1
```

IP-адрес маршрутизатора.

```
port=23
```

TCP-порт маршрутизатора.

```
timeout=5
```

Тайм-аут соединения.

```
login=root
```

Логин пользователя.

```
password=foo
```

Пароль пользователя.

```
}
```

Такую секцию необходимо создать для каждого маршрутизатора, с которого планируется собирать статистику.

Сбор статистики по протоколу IP-accounting с маршрутизатора Cisco

На сервере с биллинговой системой необходимо создать конфигурационный файл `/netup/utm5/get_xyz.conf` следующего содержания:

```
outhost=127.0.0.1
```

```
outport=9996
```

```
loop=30
```

```
host {
```

```
    type=cisco
```

```
    ip=10.1.2.99
```

```
    port=514
```

```
    login=root
```

```
    timeout=5
```

```
}
```

При этом на маршрутизаторе Cisco необходимо включить на нужном интерфейсе аккаунтинг командами.

```
CiscoRouter#conf t
CiscoRouter(config)# interface FastEthernet 0/0
CiscoRouter(config-if)#ip accounting
```

Разрешить машине с get_xyz забирать статистику.

```
CiscoRouter#conf t
CiscoRouter(config)#username netup privilege 8 pass-
word 0 plain_text_password
CiscoRouter(config)#ip rcmd rsh-enable
CiscoRouter(config)#no ip rcmd domain-lookup
CiscoRouter(config)#ip rcmd remote-host netup REMOTE_
IP_ADDRESS REMOTE_USER_NAME enable 8
```

REMOTE_IP_ADDRESS – IP-адрес сервера с get_xyz.

REMOTE_USER_NAME – имя пользователя на сервере с get_xyz, от которого производится запуск сборщика.

```
CiscoRouter(config)#privilege exec level 8 show ip
accounting checkpoint
CiscoRouter(config)#privilege exec level 1 show ip
CiscoRouter(config)#privilege exec level 8 clear ip
accounting
CiscoRouter(config)#ip accounting-threshold
4294967295
```

После завершения настройки маршрутизатора Cisco произведите запуск сборщика командой.

```
/netup/utm5/bin/get_xyz -d
```

Проверьте, происходит ли забор статистики с маршрутизатора Cisco командой.

```
show ip accounting
```

Проверьте, появляется ли статистика в формате NetFlow v.5 на указанном интерфейсе. Чтобы проверить это, выполните команду.

```
su# tcpdump -ni lo0 port 9996
```

При этом должно отобразиться примерно следующее:

```
12:40:51.958448 127.0.0.1.4675 > 127.0.0.1.9996: udp
1464
```

```
12:40:51.959051 127.0.0.1.4675 > 127.0.0.1.9996: udp
408
```

```
12:40:51.959074 127.0.0.1.4675 > 127.0.0.1.9996: udp
648
```

Сбор статистики по протоколу IP-accounting с коллектора ipcad

На сервере с биллинговой системой необходимо создать конфигурационный файл `/netup/utm5/get_xyz.conf` следующего содержания:

```
outhost=127.0.0.1
outport=9996
loop=30
host {
    type=cisco
    ip=10.0.0.1
# IP-адрес сервера с установленным ipcad.
    port=514
    login=root
    password=root
    timeout=5
}
```

На удаленном сервере необходимо установить пакет `ipcad` (<http://sourceforge.net/projects/ipcad/>) и создать конфигурационный файл `/usr/local/etc/ipcad.conf` примерно следующего содержания:

```
interface fxp0;
rsh enable;
rsh root@127.0.0.1 admin;
rsh root@10.0.0.2 admin;
# IP-адрес сервера с get_xyz и логин пользователя, от
которого производится запуск get_xyz
```

```
pidfile = /var/run/ipcad.pid;
memory_limit = 32m;
dumpfile = ipcad.dump;
ttl = 3;
rsh timeout = 30;
```

В результате статистика в формате Cisco IP-Accounting с ipcad будет передаваться утилите get_xyz, которая будет производить преобразование в формат Cisco NetFlow и экспортировать ее на локальный хост (127.0.0.1) порт 9996. Если всё настроено корректно, то на локальном сервере должны проходить UDP-пакеты на порт 9996. Проверить можно утилитой tcpdump:

```
su-2.05b# tcpdump -ni lo0 port 9996
tcpdump: listening on lo0
17:38:26.347689 127.0.0.1.2789 > 127.0.0.1.9996: udp
1464
17:38:26.550360 127.0.0.1.2789 > 127.0.0.1.9996: udp
1464
17:38:26.751455 127.0.0.1.2789 > 127.0.0.1.9996: udp
1464
17:38:26.952631 127.0.0.1.2789 > 127.0.0.1.9996: udp
1464
```

Сбор статистики по протоколу NetFlow с маршрутизатора Cisco

На маршрутизаторе Cisco необходимо включить на нужном интерфейсе NetFlow командами.

```
CiscoRouter# conf t
CiscoRouter(config)# interface FastEthernet 0/0
CiscoRouter(config-if)# ip route-cache flow
```

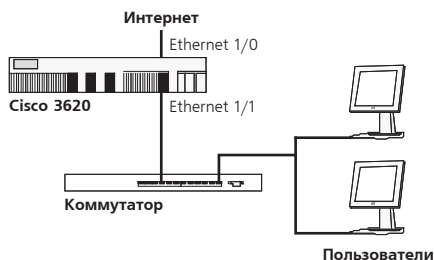
Затем указать адрес и порт сервера, на который производить отсылку пакетов Netflow:

```
CiscoRouter# conf t
CiscoRouter(config)# ip flow-export version 5
CiscoRouter(config)# ip flow-export destination
10.1.1.1 9996
```

Сбор статистики по протоколу NetFlow с маршрутизатора Cisco в случае использования NAT

Основная проблема при использовании NetFlow совместно с технологией преобразования IP-адресов NAT, заключается в том, что на внутреннем интерфейсе будет фиксироваться информация о переданном от клиента трафике, а на внешнем интерфейсе будет фиксироваться трафик переданный из интернета на внешний IP-адрес маршрутизатора. Таким образом, в NetFlow-потоке будет информация о переданном трафике от клиента, но не будет фигурировать информация о данных переданных в сторону клиента.

Например, в рассмотренном ниже конфигурационном файле внутренняя сеть имеет IP-адреса 10.11.0.0 и маску подсети 255.255.0.0, а внешний интерфейс маршрутизатора имеет IP-адрес 10.1.0.1. При этом пользователь 10.11.0.6 пытается загрузить страницу www.netup.ru с IP-адресом 195.161.112.6.



Ниже приводится работающий конфигурационный файл маршрутизатора Cisco с комментариями:

```

Current configuration : 4013 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
  
```

```
boot-start-marker
boot-end-marker
!
ip subnet-zero
!
ip cef
!
```

Интерфейс, на который производится перенаправление пакетов после обратного преобразования. Таким образом, на данном интерфейсе будет проходить трафик с IP-адреса 195.161.112.6 на IP-адрес 10.11.0.6. Чтобы данный трафик экспортировался по NetFlow, указываем опцию `ip route-cache flow`.

```
!
interface Loopback0
 ip address 192.168.0.1 255.255.255.0
 ip route-cache policy
 ip route-cache flow
!
```

Внешний интерфейс маршрутизатора. На данном интерфейсе проходит трафик с IP-адреса 195.161.112.6 на IP-адрес этого же интерфейса – 10.1.0.1. Что бы данный трафик экспортировался по NetFlow, указываем опцию `ip route-cache flow`.

Кроме того, на данном интерфейсе необходимо указать опцию `ip policy route-map NETUP_MAP`, чтобы пакеты после обратного преобразования направлялись на интерфейс `Loopback 0` согласно правилам, указанным в `route-map`.

```
!
interface Ethernet1/0
 ip address 10.1.0.1 255.255.0.0
 ip nat outside
 ip route-cache policy
 ip route-cache flow
 ip policy route-map NETUP_MAP
!
```

Внутренний интерфейс маршрутизатора. На данном интерфейсе проходит трафик с IP-адреса клиента 10.11.0.6 на IP-адрес 195.161.112.6. Чтобы данный трафик экспортировался по NetFlow, указываем опцию `ip route-cache flow`.

```
!
interface Ethernet1/1
  ip address 10.11.0.1 255.255.0.0
  ip nat inside
  ip route-cache policy
  ip route-cache flow
!
```

Опции, указывающие IP-адрес какого интерфейса использовать для преобразования, а также информация о версии NetFlow-потока и адресе сервера UTM.

```
!
ip nat inside source list 1 interface Ethernet1/0
overload
ip flow-export version 5
ip flow-export destination 10.1.0.5 9996
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.0.5
!
```

Списки доступа. Первый список доступа (номер 1) используется для указания, какую сеть необходимо преобразовывать во внешний IP-адрес при работе NAT. Второй список доступа (номер 108) используется для указания в `route-map`.

```
!
access-list 1 permit 10.11.0.0 0.0.255.255
access-list 108 permit ip any 10.11.0.0 0.0.255.255
!
```

Правила, указывающие, что если пакет направляется в сеть, указанную в списке доступа 108 (в данном случае 10.11.0.0), перенаправлять на интерфейс `Loopback 0`. Таким образом, все пакеты с внешних IP-адресов, в частности с IP-адреса 195.161.112.6, после обратного преобразования по техноло-

гии NAT, попадут на интерфейс Loopback 0, где будут зафиксированы и информация о них появится в потоке NetFlow.

```
!
route-map NETUP_MAP permit 10
  match ip address 108
  set interface Loopback0 Ethernet1/1
!
End
```

В случае если информация о трафике, переданном в сторону клиента, не появляется в NetFlow проверьте следующие пункты:

1. Работает ли route-map. Для этого выполните на маршрутизаторе команду:

```
show route-map NETUP_MAP
```

При этом счетчики переданных пакетов и байт должны увеличиваться.

2. Появляются ли пакеты в кэше NetFlow. Для этого сразу после получения клиентом информации из интернета выполните на маршрутизаторе команду:

```
show ip cache flow | include 195.161.112.6
```

При этом должна появиться информация о трафике примерно следующего вида:

```
Router#show ip cache flow | include 10.1.2.2
```

SrcIf	SrcIPaddress	DstIf	DstIPaddress
Pr	SrcP	DstP	Pkts
Et1/0	195.161.112.6	Et1/1	10.11.0.6
06	0050	1093	3
Et1/1	10.11.0.6	Et1/0	195.161.112.6
06	1093	0050	5
Et1/0	195.161.112.6	Local	10.1.0.1
06	0050	1093	2

SrcIf – интерфейс, с которого пришел пакет.

DstIf – интерфейс, на который был направлен пакет. Если данное поле равно Null, то данная информация может не экспортироваться в NetFlow. Проверьте списки доступа.

Универсальный сборщик статистики utm5_unif

Если в импортируемом файле с данными по трафику не присутствуют IP-адреса, но присутствуют логины пользователей, то обработку таких данных можно осуществить при помощи программы utm5_unif.

Запуск осуществляется командой:

```
/netup/utm5/bin/utm5_unif
```

Ключи командной строки запуска:

-c – альтернативный путь к конфигурационному файлу

-s SOURCE_FILE – импортировать данные из файла SOURCE_FILE

Конфигурационный файл расположен по следующему пути:

```
/netup/utm5/utm5_unif.conf
```

Файл состоит из строк вида

параметр=значение

Строки, начинающиеся с символа «#», считаются комментарием.

Список возможных параметров:

core_host

Адрес хоста, на котором запущено ядро биллинговой системы. Значение по умолчанию: 127.0.0.1.

core_port

Порт, на котором запущено ядро биллинговой системы. Значение по умолчанию: 11758.

core_login

Логин системного пользователя в биллинговой системе.

core_password

Пароль системного пользователя в биллинговой системе.

data_source

Тип данных в импортируемом файле. Для файла с данными об IP-трафике значение должно быть равно `iptr`.

Формат импортируемого файла должен быть следующим:

```
LOGIN BYTES TCLASS IP
```

LOGIN – логин, привязанный к услуге «IP-трафик». По данному полю происходит определение сервисной связки и, соответственно, определение стоимости трафика.

BYTES - количество переданных байт.

TCLASS – класс трафика.

IP – поле, указывающее IP-адрес, использованный при передаче данных. Данное поле используется только для отчётов, поэтому возможно указание значения 0.0.0.0 без ущерба для тарификации.

Пример

```
uniftest 1048576 10 10.10.10.10
```

```
test 10485760 20 0.0.0.0
```

Первая строка указывает на то, что пользователем с логином `uniftest` было передано 1048576 байт IP-трафика. При этом класс трафика равен 10 и использовался IP-адрес 10.10.10.10.

В случае если `data_source=pbx`, то производится импорт CDR-записей. При этом можно настроить формат импортируемого файла. Для этого необходимо определить следующие параметры:

`pbx_called_sid`

Номер позиции в импортируемом файле, в которой находится запись о вызываемом номере. Значение по умолчанию 0.

`pbx_calling_sid`

Номер позиции в импортируемом файле, в которой находится запись о вызывающем номере. Значение по умолчанию 1.

`pbx_duration`

Номер позиции в импортируемом файле, в которой находится запись о длительности звонка. Значение по умолчанию 2.

`pbx_session_id`

Номер позиции в импортируемом файле, в которой находится запись о идентификаторе сессии. Значение по умолчанию 3.

`pbx_delimiter`

Символ-разделитель между полями. По умолчанию таким символом является точка с запятой - ;.

`pbx_quote`

Символ, в который заключены поля. По умолчанию таким символом является символ двойной кавычки – “.

Если сохранить указанные параметры по умолчанию, то формат файла должен быть следующим:

“9391000”, “5409652”, “100”, “0000122”

В результате разбора такой строки будут получены следующие значения:

Вызываемый номер – 9391000

Вызывающий номер -5409652

Длительность звонка -100 сек.

Идентификатор сессии – 122

Полученные в результате разбора исходного файла данные будут экспортированы в биллинговую систему по протоколу RADIUS. Для указания параметров экспорта необходимо определить следующие параметры в конфигурационном файле:

radius_dst_host

IP-адрес, на котором слушает поток `utm5_radius`. Значение по умолчанию 127.0.0.1

radius_secret

Секретное RADIUS-слово. Значение по умолчанию `secret`.

radius_nas_name

Идентификатор сервера доступа. Это значение будет передано в атрибуте `NAS-Identifier (32)`. Значение по умолчанию `utm5_unif`.

radius_port

Порт, на котором слушает поток `utm5_radius`. Значение по умолчанию 1813.

Для запуска обработки CDR-файла используйте команду:

```
utm5_unif -c utm5_unif.cfg.pbх -s export_cdr.txt
```

Вспомогательные утилиты

Генератор статистики по протоколу NetFlow

Для эмулярования работы пользователей и экспорта статистики по протоколу NetFlow v.5 используется утилита `utm5_flowgen`, которая устанавливается по следующему пути: `/net-up/utm5/bin/utm5_flowgen`. В командной строке можно передать следующие параметры:

-h

IP-адрес хоста, на который пересылать сгенерированные NetFlow-пакеты. Значение по умолчанию – `127.0.0.1`.

-p

Порт, на который пересылать сгенерированные NetFlow-пакеты. Значение по умолчанию – `9996`.

-c

Количество NetFlow-пакетов. Значение по умолчанию – `65535`.

-t

Период ожидания в микросекундах между посылками NetFlow-пакетов.

-s

IP-адрес, с которого был передан IP-трафик. Этот адрес записывается в поле `srcaddr` в генерируемых NetFlow-пакетах.

-d

IP-адрес, к которому был передан IP-трафик. Этот адрес записывается в поле `dstaddr` в генерируемых NetFlow-пакетах.

-b

Количество переданных байтов. Это значение записывается в поле `dOctet` в генерируемых NetFlow-пакетах.

Следующая команда генерирует один NetFlow-пакет с информацией о 1048576 байтах, переданных между адресами 10.0.0.1 и 10.0.0.2:

```
/netup/utm5/bin/utm5_flowgen -c 1 -s 10.0.0.1 -d 10.0.0.2 -b 1048576
```

Генератор статистики по протоколу RADIUS

Для эмуляции работы пользователей и экспорта статистики по протоколу RADIUS используется утилита `utm5_radgen`, которая устанавливается по следующему пути: `/netup/utm5/bin/utm5_radgen`. В командной строке можно передать следующие параметры:

-p

Порт, на который пересылать сгенерированные RADIUS-пакеты.

-h

IP-адрес, на который пересылать сгенерированные RADIUS-пакеты.

-s

Секретное слово для общения с RADIUS-сервером.

-c

Код RADIUS-пакета. Значение по умолчанию – 1 (`Access-Request`).

-u

Пароль пользователя в открытом виде. Данное значение будет передано с ID атрибута 2 (`Password`).

-a

Атрибуты и значения. Возможно указание нескольких атрибутов. Строка имеет следующий формат:

```
vendor_id:attr_id:is_digit:value
```

Поля разделены двоеточием. Первое поле указывает на идентификатор вендора. Значение по умолчанию – 0.

Второе поле указывает на идентификатор атрибута.

Третье поле используется для указания типа данных: цифровой либо строчный. Если значение 0, то данные передаются, как строка. Если значение 1, то данные передаются, как цифры (integer).

Четвёртое поле используется для передачи самого значения.

Примеры

1. Для отправки запроса на авторизацию (Access-request) необходимо выполнить следующую команду:

```
/netup/utm5/bin/utm5_radgen -h 127.0.0.1 -p 1812 -s secret -u password -a 0:1:0:username -a 0:32:0:localhost
```

При этом будет сгенерирован RADIUS-пакет с запросом на авторизацию для пользователя username с паролем password.

2. Для отправки запроса на аккаунтинг (Accounting-request) необходимо выполнить следующую команду:

```
/netup/utm5/bin/utm5_radgen -h 127.0.0.1 -p 1813 -s secret -a 0:1:0:username -a 0:32:0:localhost -a 0:40:1:1 -a 0:44:0:sessionid1 -c 4
```

При этом будет сгенерирован RADIUS-пакет с запросом на аккаунтинг для пользователя username. При этом будет указано, что осуществляется начало сессии (start). Идентификатор сессии sessionid1.

3. Для отправки запроса на аккаунтинг (Accounting-request) необходимо выполнить следующую команду:

```
/netup/utm5/bin/utm5_radgen -h 127.0.0.1 -p 1813 -
s secret -a 0:1:0:username -a 0:32:0:localhost -a
0:40:1:2 -a 0:44:0:sessionid1 -a 0:46:1:100 -c 4
```

При этом будет сгенерирован RADIUS-пакет с запросом на аккаунтинг для пользователя `username`. При этом будет указано, что осуществляется окончание сессии (`stop`). Идентификатор сессии `sessionid1`. Длительность сессии (`Acct-Session-Time`) – 100 секунд.

Утилита для резервного копирования базы данных

Для обеспечения сохранности данных рекомендуется периодически делать резервное архивирование SQL-базы данных. Для этого необходимо выполнить скрипт из поставки UTM:

```
/netup/utm5/bin/utm5_backup.sh
```

При этом будет создан файл `/netup/utm5/backup/UTM5.YY_MM_DD.gz`, где `YY` – год создания архива, `MM` – месяц, `DD` – день.

Для периодического выполнения процедуры резервного копирования следует добавить строку вида:

```
0      5      *      *      *      root    /netup/utm5/
bin/utm5_backup.sh
```

в файл конфигурации планировщика задач `/etc/crontab` и перезапустить планировщик задач. При этом каждый день в 5 часов утра будет выполняться резервное копирование базы данных.

Утилита для загрузки IP-сетей из файла

Утилита для загрузки IP-сетей в классы трафика из файла. Для получения справки наберите следующую команду:

```
/netup/utm5/bin/utm5_load_tc.pl -h
usage: utm5_load_tc.pl -f file -c tc_class -n our_net
-m our_mask [-r incoming]
```

В командной строке можно передать следующие параметры:

-f

Имя файла с информацией об IP-сетях следующего формата:

IP_NET/MASK

где IP_NET – адрес сети, MASK – маска подсети.

-c

Идентификатор класса трафика в UTM. Например, 10.

-n

Адрес нашей IP-сети. Например, 192.168.10.0.

-m

Маска нашей IP-сети. Например 255.255.255.0.

-r

Если указать **-r 1**, то наша IP-сеть будет рассматриваться, как сеть назначения. Если данный ключ не указан, то наша IP-сеть будет рассматриваться, как источник.

Пример содержимого файла с информацией о сетях

128.134.151.128/25

144.206.166.0/24

144.206.176.0/24

Утилита для сканирования ARP-таблицы

Данная утилита позволяет автоматизировать процесс выдачи IP-адресов и осуществления связи с MAC-адресами. Для запуска этой утилиты наберите команду

/netup/utm5/bin/utm5_arp.pl

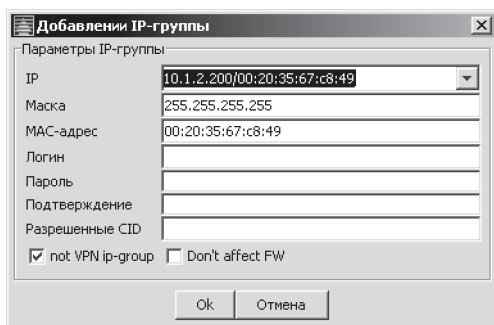
При этом на экране появятся записи, которые были обнаружены в ARP-таблице операционной системы и которые будут загружены в базу данных для дальнейшего использования. Для периодического обновления записей в базе данных реко-

мендуется установить выполнение данной утилиты по расписанию посредством системной утилиты `cron`. Для этого занесите запись в файл `/etc/crontab`:

```
*/5 * * * * root /netup/utm5/bin/utm5_arp.pl > /dev/
null 2>/dev/null
```

После этого необходимо перезапустить утилиту `cron`.

В результате при добавлении оператором IP-адресов через интерфейс администратора будут предложены на выбор все найденные пары IP-адрес/MAC-адрес.



Утилита для связки IP-адрес/MAC-адрес

Для запуска этой утилиты укажите корректные параметры для доступа к базе данных в файле `/netup/utm5/bin/arp.sh` и выполните команду:

```
/netup/utm5/bin/arp.sh
```

При этом в ARP-таблице операционной системы должны появиться неизменяемые связки IP-адрес/MAC-адрес. Они обычно помечаются как `permanent` либо `PERM`. Например:

```
(10.1.2.27) at 00:0c:29:8e:be:86 on lnc0 permanent
[ethernet]
```

Для периодического обновления записей в ARP-таблице рекомендуется установить выполнение данной утилиты по расписанию посредством системной утилиты `cron`. Для этого занесите запись в файл `/etc/crontab`:

```
*/5 * * * * root /netup/utm5/bin/arp.sh > /dev/null  
2>/dev/null
```

После этого необходимо перезапустить утилиту `cron`.

Данная технология позволяет избежать подмены IP-адресов со стороны злоумышленников, в результате чего уменьшается риск хищения IP-трафика.

Верификатор базы данных

Верификатор предназначен для проверки логической структуры базы данных UTM: тестирования на отсутствие внутренних противоречий и выявления логических ошибок. При этом не затрагивается физическое представление базы данных, т. е. целостность файлов базы контролируется средствами сервера управления базами данных и операционной системы, а не UTM.

Процедура верификации встроена в ядро системы `utm5_core` и автоматически запускается при старте системы. В том случае, если в структуре базы данных найдены несоответствия, будет создан файл с записями обо всех ошибках. Путь к нему может быть задан параметром `log_file_verificator` в конфигурационном файле `utm5.cfg`. Если значение параметра не задано, то принимается значение по умолчанию: `/netup/utm5/log/verificator.log`.

Для каждой найденной ошибки будет создана запись, содержащая краткий комментарий и набор SQL-команд. Исправления ошибок могут включать в себя работу с таблицами, содержащими данные об учётных записях абонентов, поэтому выполнение команд производится вручную и возлагается на администратора системы.

Записи, созданные верификатором, имеют следующий формат:

```
-- ERROR|WARNING <описание ошибки>
-- SQL DESC <описание SQL-запроса, который предлагает
  сделать верификатор> <SQL-запрос>
-- affected tables: <список таблиц>
```

В некоторых случаях SQL-команда будет закомментирована и в описании помечена как «NOT RECOMMENDED». Это вызвано тем, что обычно все рекомендации верификатора по исправлению ошибок сводятся к удалению сбойных услуг, IP-групп и т. п. Противоречие в базе данных будет устранено, но вместе с этим может быть потеряна информация.

Перед выполнением работ по исправлению базы данных необходимо сделать резервную копию её таблиц. Для этого существует список «affected tables», содержащий названия таблиц, которые будут затронуты в ходе выполнении SQL-команд.

Перед исполнением SQL-команд обязательно требуется остановить ядро системы `utm5_core`. Обратите внимание, что перезапуск ядра после исправления базы данных может выявить новые несоответствия, вызванные исправлением старых ошибок.

Импорт данных из других систем

Перед проведением действий по импорту в базу данных UTM необходимо остановить ядро системы. После проведения изменений нужно запустить ядро `utm5_core`. Если в процессе импорта были допущены ошибки, то появятся предупреждающие записи в файле `/netup/utm5/log/verificator.log`. В этом случае необходимо проверить все стадии ещё раз либо обратиться в службу технической поддержки Компании НетАП.

Создание учётной записи абонента

Для создания учётной записи абонента в базе данных UTM следует использовать следующий SQL-запрос:

```
INSERT INTO users (id, login, password, basic_account,
is_blocked, discount_period_id, create_date, last_
change_date, who_create, who_change, is_juridical,
full_name, juridical_address, actual_address, flat_
number, entrance, floor, passport, work_telephone,
home_telephone, mobile_telephone, web_page, icq_num-
ber, tax_number, kpp_number, email, bank_id, bank_ac-
count, comments, house_id, is_send_invoice, advance_
payment) VALUES ('ID', 'LOGIN', 'PASSWORD', 'ID',
'BLOCK', 'PERIOD_ID', unix_timestamp(), unix_time-
stamp(), '-1', '-1', '0', 'FULL_NAME', 'JUR_ADDR',
'ACT_ADDR', 'FLAT', 'ENT', 'FLOOR', '', 'PASSPORT',
'WORK_PHONE', 'HOME_PHONE', '', '', '', '', 'EMAIL',
'0', '', '', '0', '0', '0');
```

Основные параметры, использующиеся в этом запросе, описаны ниже.

ID — уникальный идентификатор абонента и лицевого счёта. Идентификатор лицевого счёта может отличаться от идентификатора абонента.

LOGIN — имя учётной записи абонента. С этим именем происходит подключение пользователя к веб-интерфейсу.

PASSWORD — пароль для учётной записи пользователя.

Создание лицевого счёта

Для создания лицевого счёта абонента в базе данных UTM следует использовать следующую последовательность SQL-запросов:

```
INSERT INTO accounts (id, balance, account_name,
credit, flags, discount_period_id, dealer_account_id,
comission_coef, default_comission_value, is_dealer,
int_status, block_recalc_abon, block_recalc_pre-
paid) VALUES ('ID', 'BALANCE', 'COMMENTS', 'CREDIT',
'PERIOD_ID', '0', '0', '0', '0', '0', '0', '0', '0');
INSERT INTO users_accounts (uid, account_id) VALUES
('ID', 'ID');
```

Основные параметры, использующиеся в этих запросах, описаны ниже.

ID — идентификатор абонента и лицевого счёта.

BALANCE — баланс лицевого счёта в условных единицах.

Создание родительской периодической услуги

Для создания записи о периодической услуге в базе данных UTM следует использовать следующую последовательность SQL-запросов:

```
INSERT INTO services_data (id, service_type, service_
name, tariff_id, link_by_default, parent_service_id)
VALUES (SERVICE_ID, SERVICE_TYPE, 'Периодическая ус-
луга', 0, 1, SERVICE_ID);
INSERT INTO periodic_services_data (id, cost, dis-
count_method) VALUES (SERVICE_ID, COST, METHOD);
```

Основные параметры, использующиеся в этих запросах, описаны ниже.

SERVICE_ID — уникальный идентификатор услуги.

COST — стоимость периодической услуги в условных единицах. Данная стоимость будет списана в течение расчётного периода.

METHOD — способ списания. Возможные значения: 1 — в начале расчётного периода, 2 — в конце расчётного периода, 3 — плавно в течение всего расчётного периода.

SERVICE_TYPE — тип услуги. Для периодической услуги данное поле равно 2. Другие возможные значения: 1 — разовая услуга, 2 — периодическая услуга, 3 — передача IP-трафика, 4 — хот-спот, 5 — коммутируемый доступ, 6 — телефония.

Создание родительской услуги передачи IP-трафика

Для создания записи об услуге IP-трафика в базе данных UTM следует использовать следующую последовательность SQL-запросов:

```
INSERT INTO services_data (id, service_type, service_name, tariff_id, link_by_default, parent_service_id)
VALUES (SERVICE_ID, SERVICE_TYPE, 'Услуга IP-трафика', 0, 1, SERVICE_ID);
```

```
INSERT INTO periodic_services_data (id, cost, discount_method) VALUES (SERVICE_ID, COST, METHOD);
```

```
INSERT INTO iptraffic_borders (borders_id, border, cost) VALUES (BORDER_ID, BORDER, BORDER_COST);
```

```
INSERT INTO traf_serv_tclasses (tst_id, tclass_id, borders_id) VALUES (TST_ID, TCLASS_ID, BORDER_ID);
```

```
INSERT INTO iptraffic_services_data (id, tst_id)
VALUES (SERVICE_ID, TST_ID);
```

Основные параметры, используемые в этих запросах, описаны ниже.

SERVICE_ID — уникальный идентификатор услуги.

BORDER_ID — уникальный идентификатор стоимостных границ для IP-трафика.

BORDER — граница в байтах.

BORDER_COST — стоимость трафика за 1 МБ при достижении указанной границы. Данная стоимость будет действовать до

следующей границы либо до бесконечности, если границ больше нет.

TST_ID — уникальный идентификатор для связки стоимостных границ, классов трафика и услуг передачи IP-трафика.

TCLASS_ID — идентификатор класса трафика. По умолчанию, в базе данных UTM создаётся три класса трафика с идентификаторами 10, 20 и 1000.

COST — стоимость периодической услуги в условных единицах. Данная стоимость будет списана в течение расчётного периода.

METHOD — способ списания. Возможные значения: 1 — в начале расчётного периода, 2 — в конце расчётного периода, 3 — плавно в течение всего расчётного периода.

SERVICE_TYPE — тип услуги. Для услуги передачи IP-трафика данное поле равно 3. Другие возможные значения: 1 — разовая услуга, 2 — периодическая услуга, 3 — передача IP-трафика, 4 — хотспот, 5 — коммутируемый доступ, 6 — телефония.

Создание тарифного плана с включёнными в него услугами

На базе созданных родительских услуг можно создать дочерние услуги и включить их в тарифный план.

Для создания записи о тарифном плане в базе данных UTM следует использовать следующий SQL-запрос:

```
INSERT INTO tariffs (id, name) VALUES (TID, 'Тарифный план');
```

Для создания записи о дочерней периодической услуге в базе данных UTM следует использовать следующую последовательность SQL-запросов:

```
INSERT INTO services_data (id, service_type, service_name, tariff_id, link_by_default, parent_service_id) VALUES (PERIODIC_SERVICE_ID, SERVICE_TYPE, 'Периодическая услуга', TID, 1, PARENT_SERVICE_ID);
```

```
INSERT INTO periodic_services_data (id, cost, discount_method) VALUES (PERIODIC_SERVICE_ID, COST, METHOD);
```

```
INSERT INTO tariffs_services_link (tariff_id, service_id) VALUES (TID, PERIODIC_SERVICE_ID);
```

Для создания записи о дочерней услуге IP-трафика в базе данных UTM следует использовать следующую последовательность SQL-запросов:

```
INSERT INTO services_data (id, service_type, service_name, tariff_id, link_by_default, parent_service_id) VALUES (IP_SERVICE_ID, SERVICE_TYPE, 'Услуга IP-трафика', TID, 1, PARENT_SERVICE_ID);
```

```
INSERT INTO periodic_services_data (id, cost, discount_method) VALUES (IP_SERVICE_ID, COST, METHOD);
```

```
INSERT INTO iptraffic_borders (borders_id, border, cost) VALUES (BORDER_ID, BORDER, BORDER_COST);
```

```
INSERT INTO traf_serv_tclasses (tst_id, tclass_id, borders_id) VALUES (TST_ID, TCLASS_ID, BORDER_ID);
```

```
INSERT INTO iptraffic_services_data (id, tst_id) VALUES (SERVICE_ID, TST_ID);
```

```
INSERT INTO tariffs_services_link (tariff_id, service_id) VALUES (TID, IP_SERVICE_ID);
```

Основные параметры, использующиеся в этих запросах, описаны ниже.

TID — идентификатор тарифного плана.

PERIODIC_SERVICE_ID — уникальный идентификатор дочерней периодической услуги. Значение идентификатора дочерней услуги должно отличаться от значения идентификатора родительской услуги.

IP_SERVICE_ID — уникальный идентификатор дочерней услуги передачи IP-трафика. Значение идентификатора дочерней услуги должно отличаться от значения идентификатора родительской услуги.

PARENT_SERVICE_ID — идентификатор родительской услуги.

Все остальные параметры заполняются аналогично параметрам базовых услуг, рассмотренным выше.

Создание расчётного периода

Для создания записи о расчётном периоде в базе данных UTM следует использовать следующую последовательность SQL-запросов:

```
INSERT INTO discount_periods (id, start_date, end_date, periodic_type) VALUES (PERIOD_ID, unix_timestamp('2004-12-01'), unix_timestamp('2005-01-01'), PERIOD_TYPE);
```

```
UPDATE discount_periods SET canonical_len=end_date-start_date WHERE id='PERIOD_ID';
```

Основные параметры, использующиеся в этих запросах, описаны ниже.

PERIOD_ID — уникальный идентификатор расчётного периода.

PERIOD_TYPE — тип расчётного периода. Возможные значения: 1 — ежедневный, 2 — еженедельный, 3 — ежемесячный, 4 — ежеквартальный, 5 — ежегодный.

Привязка тарифного плана к лицевому счёту абонента

Для создания привязки тарифного плана к лицевому счёту абонента в базе данных UTM следует использовать следующий SQL-запрос:

```
INSERT INTO account_tariff_link (id, account_id, tariff_id, next_tariff_id, discount_period_id) VALUES (ATL_ID, ACCOUNT_ID, TARIFF_ID, TARIFF_ID_NEXT, PERIOD_ID);
```

Основные параметры, использующиеся в этом запросе, описаны ниже.

ATL_ID — уникальный идентификатор данной связки «лицевой счёт–тарифный план».

ACCOUNT_ID — идентификатор лицевого счёта.

TARIFF_ID — идентификатор тарифного плана.

TARIFF_ID_NEXT — идентификатор тарифного плана следующего расчётного периода. Если на следующий расчётный период тарифный план не меняется, то значение в данном поле равно TARIFF_ID.

PERIOD_ID — идентификатор расчётного периода.

Для привязки периодической услуги из тарифного плана к лицевому счёту необходимо выполнить следующую последовательность SQL-запросов:

```
INSERT INTO service_links (id, user_id, account_id,
service_id, tariff_link_id) VALUES (SLINK_ID, USER_
ID, ACCOUNT_ID, SERVICE_ID, ATL_ID);
```

```
INSERT INTO periodic_service_links (id, discount_pe-
riod_id, discounted_in_curr_period, need_del, unpre-
pay_period, unabon_period) VALUES (SLINK_ID, PERIOD_
ID, 0, 0, 0, 0);
```

Основные параметры, использующиеся в этих запросах, описаны ниже.

SLINK_ID — уникальный идентификатор связки «идентификатор абонента–идентификатор лицевого счёта–идентификатор услуги».

USER_ID — уникальный идентификатор абонента.

ACCOUNT_ID — уникальный идентификатор лицевого счёта

SERVICE_ID — уникальный идентификатор периодической услуги.

PERIOD_ID — уникальный идентификатор расчётного периода.

Для привязки услуги передачи IP-трафика из тарифного плана к лицевому счёту необходимо выполнить следующую последовательность SQL-запросов:

```
INSERT INTO service_links (id, user_id, account_id,
service_id, tariff_link_id) VALUES (SLINK_ID, USER_
ID, ACCOUNT_ID, SERVICE_ID, ATL_ID);

INSERT INTO periodic_service_links (id, discount_pe-
riod_id, discounted_in_curr_period, need_del, unpre-
pay_period, unabon_period) VALUES (SLINK_ID, PERIOD_
ID, 0, 0, 0, 0);

INSERT INTO ip_groups (ip_group_id, ip, mask, uname,
upass, mac, allowed_cid, create_date, ip_type) VALUES
(IP_GROUP_ID, IP, MASK, ULOGIN, UPASS, MAC, '', unix_
timestamp(NOW()), 0);

INSERT INTO downloaded (downloaded_id, tclass_id)
VALUES (DOWNLOADED_ID, TCLASS_ID);

INSERT INTO iptraffic_service_links (id, ip_group_
id, downloaded_id) VALUES (SLINK_ID, IP_GROUP_ID,
DOWNLOADED_ID);
```

Основные параметры, использующиеся в этих запросах, опи- саны ниже.

SLINK_ID — уникальный идентификатор связки «идентифика- тор абонента–идентификатор лицевого счёта–идентифика- тор услуги».

USER_ID — уникальный идентификатор абонента.

ACCOUNT_ID — уникальный идентификатор лицевого счёта.

SERVICE_ID — уникальный идентификатор услуги передачи IP- трафика.

PERIOD_ID — уникальный идентификатор расчётного перио- да.

IP_GROUP_ID — идентификатор группы IP-адресов, привязан- ных к данному абоненту. Под этим идентификатором можно добавить несколько записей в таблицу ip_groups.

IP — IP-адрес в целочисленном виде (signed int). Например, адрес 195.161.112.6 необходимо вставлять как 1012830202.

MASK — маска подсети в целочисленном виде (signed int). На- пример, маску 255.255.255.255 необходимо вставлять как -1.

ULOGIN — логин, с которым возможно производить подключения по VPN.

UPASS — пароль для ULOGIN.

DOWNLOADED_ID — уникальный идентификатор для строки, в которую в процессе работы биллинговой системы будет записываться потреблённое количество данного класса трафика.

Предоставление услуги хотспот

Для организации услуги хотспот необходим сервер, на котором установлены операционная система FreeBSD или Linux и веб-сервер Apache, настроен кэширующий сервер DNS и установлена биллинговая система NetUP UTM.

Для полностью автоматического входа клиента в сеть нужно установить и настроить сервер DHCP, который будет выдавать компьютеру клиента IP-адрес. Наиболее распространённый и широко используемый сервер DHCP – isc-dhcpd. Его можно загрузить по адресу <ftp://ftp.isc.org/isc/dhcp/dhcp-latest.tar.gz>.

Установку произвести командами.

```
./configure  
make  
make install
```

Также isc-dhcpd можно установить из дистрибутивов, поставляющихся с операционной системой.

Конфигурация сервера DHCP

Главный конфигурационный файл – dhcpd.conf. Он должен содержать следующие строки.

```
option domain-name »yourdomain.com«;  
option domain-name-servers 10.1.2.1;  
option subnet-mask 255.255.255.0;  
default-lease-time 36000;  
max-lease-time 86400;  
authoritative;  
ddns-update-style none;  
log-facility local7;  
subnet 10.1.2.0 netmask 255.255.255.0  
{  
option routers 10.1.2.1;  
pool
```

```
{  
range 10.1.2.10 10.1.2.200 ;  
allow unknown clients;  
}  
}
```

При такой конфигурации сервер будет выдавать адреса из диапазона 10.1.2.10–10.1.2.200, как правило, начиная с конца диапазона. Сам сервер при этом должен иметь адрес 10.1.2.1. Очень важно проследить, на каком интерфейсе будет работать сервер DHCP, так как выдача адресов, например, в интернет может привести к нежелательным последствиям. Поэтому сервер DHCP должен запускаться с указанием интерфейса, на котором ему следует работать. Например, внутренний интерфейс `fxp0`. Правильная команда запуска – `dhcpcd fxp0`. Интерфейс указывается в качестве параметра командной строки. Несколько интерфейсов можно указывать через пробел, например, `dhcpcd fxp0 fxp1 ed0`

После настройки автоматического получения адресов нужно позаботиться о том, чтобы клиент мог без труда активировать свою карточку. Для этого необходимо принудительно перенаправлять на страницу активации запросы от неавторизовавшегося клиента. Такое перенаправление делается при помощи файрвола.

Настройка файрвола для FreeBSD

В ОС FreeBSD файрволом является программа `ipfw`.

Для перенаправления всех пакетов, следующих на 80 порт (как правило, просмотр веб-сайтов) от неавторизовавшихся клиентов, будем использовать `natd` с опцией `-proxu_rule`. Эта опция позволяет перенаправлять указанные пакеты на любой другой адрес, в нашем случае на страничку UTM с вводом номера и пин-кода prepaid-карты.

Предположим, наш сервер имеет локальный адрес 10.1.2.1 и локальная сеть 10.1.2.0/24, внешний IP-адрес сервера – 10.10.10.1. Запускаем `natd`.

```
# natd -p 9000 -a 10.1.2.1 -proxy_rule port 80 server  
10.1.2.1:80 -reverse
```

В соответствии с этим нужно сконфигурировать фаервол. Один из вариантов рабочей конфигурации – следующий.

```
10000 divert 9000 tcp from 10.1.2.0/24 to not  
10.1.2.1 dst-port 80 via fxp0  
10100 divert 9000 tcp from 10.1.2.1 80 to 10.1.2.0/24  
10200 allow tcp from 10.1.2.0/24 to any dst-port 80  
via fxp0  
10300 allow tcp from any 80 to 10.1.2.0/24  
10400 skipto 20000 ip from any to me  
10500 skipto 20000 ip from me to any  
15000 deny log ip from any to any  
20000 divert 8668 ip from 10.1.2.0/24 to any via fxp1  
20100 divert 8668 ip from any to 10.10.10.1 via fxp1  
65535 allow ip from any to any
```

В этом варианте конфигурации приняты следующие обозначения:

fxp0 – интерфейс с адресом 10.1.2.1;

fxp1 – внешний интерфейс маршрутизатора;

8668 – порт, на котором принимает соединения обычный natd (вида `natd -n fxp1`).

При такой конфигурации необходимо добавить в UTM правила фаервола для включения доступа пользователям.

```
/sbin/ipfw add RULE_ID skipto 20000 ip from UIP to  
any
```

```
/sbin/ipfw add RULE_ID skipto 20000 ip from any to  
UIP,
```

И для выключения.

```
/sbin/ipfw delete RULE_ID,
```

В результате получим, что после активации карточки пользователь будет попадать сразу на правила `divert 20000` и сможет

беспрепятственно загружать странички из Интернета. В случае если карточка не активирована, то все запросы пользователя будут перенаправлены на страницу авторизации.

Настройка файрвола для Linux

В ОС Linux файрволом является программа iptables.

В iptables существует действие REDIRECT, которое позволяет перенаправлять указываемые пакеты на порт локальной машины, подменяя адрес назначения. Воспользуемся этим действием для перенаправления запросов от неавторизовавшихся клиентов на страницу UTM с вводом номера и пин-кода prepaid-карты. Для этого в таблице nat в цепочку PREROUTING нужно добавить правило.

```
iptables -t nat -A PREROUTING -s 10.1.2.0/24 -p tcp
--dport 80 -j REDIRECT --to-ports 80
```

Далее, в UTM нужно добавить на каждого пользователя два правила для включения доступа.

```
/sbin/iptables -t nat -I PREROUTING 1 -s UIP/UBITS -j
ACCEPT
```

```
/sbin/iptables -A FORWARD -s UIP/UBITS -j ACCEPT
```

```
/sbin/iptables -A FORWARD -d UIP/UBITS -j ACCEPT
```

И для выключения.

```
/sbin/iptables -t nat -D PREROUTING -s UIP/UBITS -j
ACCEPT
```

```
/sbin/iptables -D FORWARD -s UIP/UBITS -j ACCEPT
```

```
/sbin/iptables -D FORWARD -d UIP/UBITS -j ACCEPT
```

При этом должна быть выставлена запрещающая политика для цепочки FORWARD (iptables -P FORWARD DROP).

Настройка веб-сервера Apache

Необходимо переопределить начальную страницу и страницу 404 в конфигурационном файле httpd.conf.

```
ErrorDocument 404 »/cgi-bin/utm5/aaa5?cmd=card_login«
```

```
DirectoryIndex »/cgi-bin/utm5/aaa5?cmd=card_login«
index.html
```

При этом на любой запрос пользователя будет выдаваться страница, с приглашением ввести номер и пин-код карты для выхода в Интернет.

После исправления конфигурационного файла необходимо перезапустить веб-сервер.

```
apachectl restart
```

В случае, если после успешной авторизации необходимо организовать автоматическое перенаправление пользователя на первоначально набранный URL, то необходимо в параметрах aaa5 передать `redirect=yes`. В этом случае параметры в конфигурации веб-сервера будут выглядеть следующим образом:

```
ErrorDocument 404 »/cgi-bin/utm5/aaa5?cmd=card_
login&redirect=yes«
```

```
DirectoryIndex "/cgi-bin/utm5/aaa5?cmd=card_
login&redirect=yes" index.html
```

Также необходимо в конфигурационном файле `web5.cfg` указать строку

```
src_redirect=yes
```

В этом случае при первом обращении к aaa5 будет сохранён адрес из переменной окружения `SERVER_HOST` и, если пользователь ввёл корректные данные для авторизации, то он будет автоматически переправлен по сохранённому адресу.

Например, пользователь после получения IP-адреса по DHCP запустил интернет-браузер и в строке адреса набрал сайт `www.netup.ru`. В результате срабатывания перенаправления пользователю будет выдано приглашение для ввода номера карты и пин-кода. После успешной авторизации автоматически будет загружена страница `www.netup.ru`.

Настройка услуги хотспот

В центре управления в разделе (Тарификация | Услуги) необходимо добавить услугу хотспот, указать временные диапазо-

ны и стоимость. Идентификатор этой услуги необходимо указать при добавлении карточек в систему.

После ввода пользователем номера и пин-кода карты в процессе активации карты страничка в браузере будет автоматически регулярно обновляться, давая тем самым серверу знак, что пользователь все ещё пользуется услугой. В случае если в течение указанного в настройках промежутка времени не было обновления страницы (пользователь закрыл эту страничку или просто выключил компьютер), либо поступил сигнал закрытия сессии (пользователь выбрал в меню пункт «Выход»), то доступ в интернет блокируется и производится списание средств за время работы. Также блокирование доступа в интернет наступает при окончании средств на карте.

Приём платежей через платёжную систему «Рапида»

Приём платежей в пользу абонентов через платёжную систему (ПС) «Рапида» реализован в АСР NetUP UTM 5 посредством отдельного модуля `utm5_rapida_check`. Помимо приёма платежей через ПС «Рапида» модуль выступает также в качестве интегратора АСР NetUP UTM 5 со сторонним ПО в части автоматизации приёма платежей из других АСР или ИС, о чём упоминается в разделе «Платежи». В качестве протокола обмена информацией между модулем `utm5_rapida_check` и сторонним ПО выступают файлы с информацией о платежах абонентов (ФИПА).

Подготовка системы

Для начала работы с ключами необходимо выполнить следующие действия.

Загрузить последнюю версию `dvc_tool` с сайта разработчика. Для ОС FreeBSD: <http://www.adam.ru/Pki/Download/FreeBSD4.6R.zip>. Для ОС Linux: <http://www.adam.ru/Pki/Download/Master2.2.zip>.

Исполняемый файл `dvc_tool` нужно установить в директорию `/sbin`.

Перейти в директорию:

```
cd /netup/utm5/dvc_home
```

Создать хранилище ключей:

```
dvc_tool -init 123  
[ OK ][ p11 ][ init ][ (null) ]
```

Импортировать сертификаты. В примере указаны имена файлов с тестовыми сертификатами:

```
dvc_tool -cmd cert -inform P7B -in testpay4.p7b  
[ OK ][ cert ][ import ][ testpay ]  
[ OK ][ cert ][ import ][ CP CSP Test CA ]
```

```
dvc_tool -cmd cert -inform DER -in CryptoproCA.cer
[ OK ][ cert ][ import ][ CryptoPro CA ]
```

Проверка подписи на сообщениях

Проверка подписи на письмах от платёжной системы осуществляется автоматически через настраиваемый интервал времени. При проверке используется программа `/netup/utm5/bin/utm5_rapida_check`, которая в свою очередь после сбора сообщения с сервера РОРЗ выполняет проверку подписи на сообщениях следующей командой (команда приведена для информации, АСР автоматически выполняет данную проверку без участия администратора.):

```
dvc_tool -home /netup/utm5/dvc_home -cmd vfy -in /
netup/utm5/pay_msg/1077049250_4032783c000000005.msg -
smime | grep »\[ OK \] \[ vfy \]< | grep »\[ 100 \]<
```

Настройки модуля `utm5_rapida_check`

Для управления проведением платежей используются следующие параметры в настройках модуля `utm5_rapida_check` АСР NetUP UTM 5. Настройки модуля хранятся в его конфигурационном файле `rapida5.cfg`.

rapida_host

IP-адрес сервера РОРЗ.

rapida_login

Логин к почтовому ящику, в который поступают сообщения о платежах.

rapida_password

Пароль к почтовому ящику, в который поступают сообщения о платежах.

core_host

Адрес хоста, на котором запущено ядро биллинговой системы. Значение по умолчанию – 127.0.0.1.

`core_port`

Порт, на котором запущено ядро биллинговой системы.

`core_login`

Логин системного пользователя в биллинговой системе

`core_password`

Пароль системного пользователя в биллинговой системе.

`rapida_check_interval`

Интервал в секундах, через который производить проверку наличия новых платежей.

`rapida_pay_path`

Путь к системной директории модуля, где сохраняется информация о платежах в виде текстовых файлов.

`rapida_log_path`

Путь к системной директории модуля, где сохраняются сообщения от ПС «Рапида», в виде текстовых файлов, полученные с сервера РОРЗ без изменений.

`rapida_ext_path`

Путь к системной директории модуля, из которой модуль читает файлы ФИПА.

`dvc_home`

Путь к системной директории модуля, в которой находятся хранилище ключей и сертификаты, посредством которых производится проверка подписи на сообщениях от ПС «Рапида».

`template_string_62`

Параметр задает шаблон идентификации абонента в уведомлениях о платеже от ПС «Рапида» и ФИПА (строка :62 уведомления о платеже, смотрите ниже). В шаблоне могут быть использованы специальные символы, указывающие на признак по которому АСР NetUP UTM5 идентифицирует абонентов для вноса платежа:

^u – означает, что в данной позиции будет указан идентификатор абонента [user id].

^a – идентификатор счета [account id].

^c – идентификатор контракта [contract id].

^l – логин абонента.

^p – семь цифр из логина абонента.

^^ – в данной позиции будет указана некоторая нефиксированная информация, не являющаяся необходимой для идентификации абонента.

Примеры шаблонов:

template_string_62=НОМер документа: ^a

template_string_62=фio: ^^, N догoвoра: ^l

Проверка работоспособности

В результате работы в директории /netup/utm5/pay_msg будут сохраняться сообщения, полученные с сервера РОРЗ без изменений. Рекомендуется их сохранять для дальнейшего анализа. В директории /netup/utm5/pay будут сохраняться файлы в открытом виде, содержащие информацию о платежах. Например:

1077049250_4032783c00000002.msg

1077049250_4032783c00000003.msg

1077049250_4032783c00000004.msg

1077049250_4032783c00000005.msg

1077049251_4032783c00000001.msg

ok_1077049252_4032783c00000005.pay

```
ok_1077049253_4032783c00000004.pay
ok_1077049255_4032783c00000003.pay
ok_1077049256_4032783c00000002.pay
ok_1077049257_4032783c00000001.pay
```

Если файл имеет префикс `err_`, следовательно, при обработке этого файла возникли ошибки. Если файл имеет префикс `ok_`, следовательно, обработка этого файла прошла успешно.

Формат файлов с информацией о платеже

Структура и содержание файлов должны соответствовать следующей лексической конструкции (поля, обязательные для заполнения, выделены жирным шрифтом):

```
RRECV
FROM: <от кого поступает платеж(абонент)>
TO: <кому поступает платеж(провайдер)>
DATE:<дата платежа(DD:MM:YY)>
:10 MessTp: 710
:21 RegRecvEssId: <Код платежных реквизитов ТСП>
:30 PaymId: <Код исполненного платежа>
:31 InvId: <Код регистрации принятого счета>
:40 PaymSum: <Сумма платежа>
:50 InvNumb: <Номер счета ТСП, по которому произошла
оплата>
:51 InvDate: <Дата выписки счета в ТСП>
:60 PaymSubjText: <Текстовое описание назначения
платежа>
:61 PaymSubjTp: <Код назначения платежа по каталогу
типов назначений платежей>
:62 PaymSubjParam: <Идентификатор абонента>
ENDRRECV
```

Поле `:10` всегда должно иметь значение 710.

В случае ФИПА, файл может содержать несколько лексических конструкций, расположенных в файле друг за другом.

Пример

```
RRECV
FROM: ООО Платежная интернет-система РАПИДА
TO: Закрытое акционерное общество »ТЕСТ« (г.Москва)
```

```

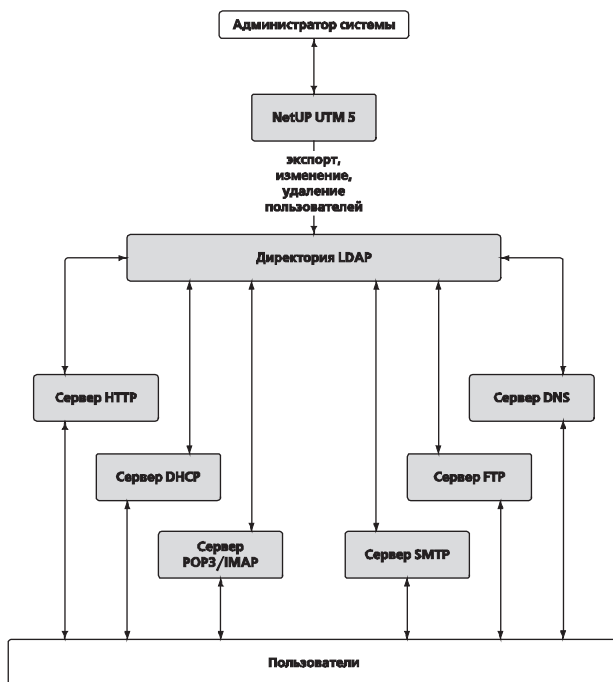
DATE: 15.02.04
:10 MessTp: 710
:21 RegRecvEssId: 412
:30 PaymId: 12404
:40 PaymSum: 3,00
:31 InvId:
:50 InvNumb:
:51 InvDate:
:60 PaymSubjText: Доступ в интернет
:61 PaymSubjTp: 584
:62 PaymSubjParam: Номер Договора: 1
ENDRRECV
    
```

Сумма указанная в поле :40 PaymSum: зачисляется на основной лицевой счёт, соответствующий абоненту с номером договора указанным в поле :62 PaymSubjParam: Номер Договора: (если в качестве значения параметра `template_string_62` используется значение `^c`).

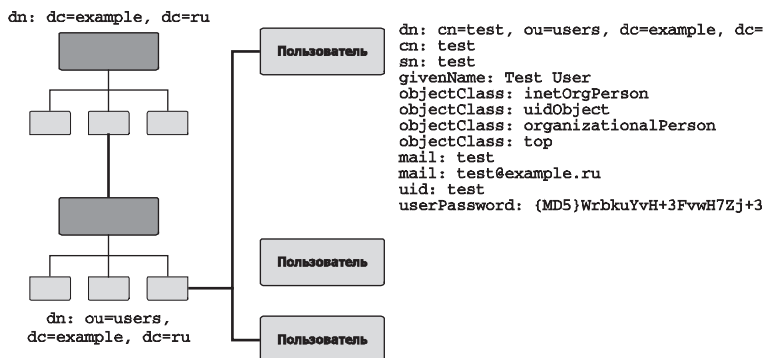
Совместная работа UTM и LDAP

Данный вопрос детально рассмотрен в статье «Настройка и использование централизованного управления сервисами сети при помощи сервера LDAP» расположенной на сайте компании НетАП в разделе «Документация».

Использование биллинговой системы NetUP UTM в связке с сервером OpenLDAP позволяет более гибко и удобно администрировать услуги, предоставляемые пользователям. В результате описанных ниже настроек сервер LDAP будет играть роль единого хранилища пользовательских данных (логин, пароль, почтовый ящик и прочее), доступ к которому может иметь любое программное обеспечение в сети, поддерживающее протокол LDAP. Таким образом, можно поддерживать актуальность данных (наличие пользователя, его пароль и т. д.) для всех серверов в сети через единое хранилище.



При этом все указанные сервисы могут работать как на одном физическом сервере, так и на разных физических серверах.



Установка программного обеспечения

Последовательность шагов по установке и конфигурирование программного обеспечения.

BerkeleyDB

Скачайте BerkeleyDB: <http://www.sleepycat.com/update/snapshot/db-4.2.52.tar.gz>.

Установите BerkeleyDB командами.

```
tar xvfz db-4.2.52.tar.gz
cd db-4.2.52
cd build_unix/
../dist/configure --prefix=/usr/ --exec-prefix=/usr/
make
make install
```

OpenLDAP

Скачайте OpenLDAP: <ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/openldap-2.1.26.tgz>.

Установите OpenLDAP командами.

```
tar xvfz openldap-2.1.26.tgz
cd openldap-2.1.26
./configure
make depend
make
make install
```

Отредактируйте конфигурационный файл `/usr/local/etc/openldap/slapd.conf`. Пример содержимого конфигурационного файла приведён ниже.

```
include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.
schema

include /usr/local/etc/openldap/schema/nis.schema
include /usr/local/etc/openldap/schema/openldap.sche-
ma

include /usr/local/etc/openldap/schema/misc.schema
include /usr/local/etc/openldap/schema/java.schema


pidfile /usr/local/var/run/slapd.pid
argsfile /usr/local/var/run/slapd.args


allow bind_v2


database bdb
suffix "dc=example,dc=ru"
rootdn "cn=Manager,dc=example,dc=ru"
rootpw secret
directory /usr/local/var/openldap-netup
index cn,sn,uid pres,eq,sub
```

Произведите запуск сервера OpenLDAP командой.

```
/usr/local/libexec/slapd
```

Создайте файл `example.ldiff` следующего содержания.

```
dn: dc=example,dc=ru
objectclass: dcObject
objectclass: organization
o: Example company
dc: example
dn: cn=Manager,dc=example,dc=ru
objectclass: organizationalRole
cn: Manager
```

Примените его командой.

```
ldapadd -D "cn=Manager,dc=example,dc=ru" -w secret <
example.ldiff
```

Почтовый сервер Cyrus

Скачайте демон авторизации, почтовый (POP3/IMAP) сервер Cyrus и патч к нему по адресам:

```
ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/cyrus-imapd-2.2.3.tar.gz;
```

```
ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/cyrus-sasl-2.1.18.tar.gz;
```

```
http://email.uoa.gr/download/cyrus/cyrus-imapd-2.2.3/cyrus-imapd-2.2.3-autocreate-0.8.6.diff.
```

Установите демон авторизации командами.

```
tar xvfz cyrus-sasl-2.1.18.tar.gz
```

```
cd cyrus-sasl-2.1.18
```

```
./configure --with-ldap --with-bdb-incdir=/usr/local/BerkeleyDB.4.2/include/
```

```
make
```

```
make install
```

Создайте файл `/usr/local/etc/saslauthd.conf`, в котором укажите строки.

```
ldap_servers: ldap://127.0.0.1/  
ldap_bind_dn: cn=Manager,dc=example,dc=ru  
ldap_password: secret  
ldap_search_base: ou=users,dc=example,dc=ru  
ldap_mech: DIGEST_MD5  
ldap_auth_method: custom
```

Произведите запуск демона командой.

```
/usr/local/sbin/saslauthd -a ldap
```

Установите почтовый сервер командами.

```
tar xvfz cyrus-imapd-2.2.3.tar.gz  
patch < cyrus-imapd-2.2.3-autocreate-0.8.6.diff  
cd cyrus-imapd-2.2.3  
./configure --with-ldap --with-sasl=/usr/local/ --  
with-bdb=/usr/local/BerkeleyDB.4.2/ --with-bdb-inc-  
dir=/usr/local/BerkeleyDB.4.2/include/  
make  
make install
```

Создайте файл `/etc/imapd.conf` и укажите в нём строки.

```
configdirectory: /var/imap  
partition-default: /var/spool/imap  
sasl_pwcheck_method: saslauthd  
admins: aospam  
mboxlist_db: flat  
autocreatequota: 1000000  
createonpost: yes
```

Добавьте в систему пользователя `cyrus` командой `adduser`.

Создайте директории.

```
/var/imap/
```

```
/var/imap/proc  
/var/imap/db  
/var/imap/socket  
/var/imap/log  
/var/imap/msg  
/var/spool/imap/
```

Важно! Укажите владельцем созданных папок пользователя `cyrus`.

Выполните команды, находясь в директории `cyrus-imapd-2.2.3`.

```
./tools/mkimap  
cp master/conf/normal.conf /etc/cyrus.conf
```

Произведите запуск почтового сервера командой.

```
/usr/cyrus/bin/master &
```

Почтовый сервер Postfix

Скачайте почтовый (SMTP) сервер postfix по адресу <ftp://ftp.easynet.be/postfix/official/postfix-2.0.19.tar.gz>

Установите его командами.

```
tar xvfz postfix-2.0.19.tar.gz  
cd postfix-2.0.19  
make tidy  
make makefiles CCARGS="-I./ -DHAS_LDAP" AUXLIBS="-lldap -llber"  
make  
make install
```

Создайте конфигурационный файл `/etc/postfix/main.cf` примерно следующего содержания.

```
mailbox_transport = lmtp:unix:/var/imap/socket/lmtp  
alias_maps = hash:/etc/aliases, ldap:ldapsource  
ldapsource_server_host = example.ru  
ldapsource_search_base = ou=users,dc=example,dc=ru  
ldapsource_version = 3
```

```
ldapsource_bind_dn = cn=Manager,dc=example,dc=ru
ldapsource_bind_pw = secret
ldapsource_result_attribute = mail
ldapsource_query_filter = (&(mail=%s))
readme_directory = no
sample_directory = /etc/postfix
sendmail_path = /usr/sbin/sendmail
setgid_group = postdrop
command_directory = /usr/sbin
manpage_directory = /usr/local/man
daemon_directory = /usr/libexec/postfix
newaliases_path = /usr/bin/newaliases
mailq_path = /usr/bin/mailq
queue_directory = /var/spool/postfix
mail_owner = postfix
unknown_local_recipient_reject_code = 450
```

Произведите запуск почтового сервера командой.

```
/usr/libexec/postfix/master &
```

Создание схемы LDAP

Создайте файл `netup.ldiff` следующего содержания.

```
dn: ou=users, dc=example, dc=ru
objectclass: organizationalUnit
ou: users

dn: cn=test, ou=users, dc=example, dc=ru
cn: test
sn: test
givenName: Test Test
objectClass: inetOrgPerson
objectClass: uidObject
objectClass: organizationalPerson
objectClass: top
mail: test
```

```
mail: test@example.ru
uid: test
userPassword: {MD5}2Fe034RYzgb7xht2pYxcpA==
```

Затем примените созданный файл командой.

```
ldapadd -D "cn=Manager,dc=example,dc=ru" -w secret <
netup.ldiff
```

В результате будет создана учётная запись почты test@example.ru. Для получения почты по протоколу POP3 (рекомендуется настроить POP3S) необходимо использовать логин test и пароль qwerty (в LDAP хранится его MD5-хеш: {MD5}2Fe034RYzgb7xht2pYxcpA==).

Сгенерировать хеши можно perl-скриптом, который можно найти по адресу http://www.netup.ru/download/pas_md5.pl,

либо использовать команду

```
slappasswd -h {MD5}
```

Просмотреть содержимое LDAP можно при помощи утилиты командной строки ldapsearch либо при помощи графической утилиты «LDAP Browser/Editor»: <http://www.iit.edu/~gawojar/ldap/>.

Установка и настройка сервера DHCP

Скачайте сервер DHCP по адресу <ftp://ftp.isc.org/isc/dhcp/dhcp-3.0pl2.tar.gz> и обновление к нему по адресу <http://www.lunytune.net/dhcp-3.0pl2.ldap.diff.gz>.

Установите командами.

```
tar xvfz dhcp-3.0pl2.tar.gz
gzip -d dhcp-3.0pl2.ldap.diff.gz
cp dhcp-3.0pl2.ldap.diff dhcp-3.0pl2
cd dhcp-3.0pl2
patch -p1 < dhcp-3.0pl2.ldap.diff
./configure
```

в файле work.freebsd/server/Makefile укажите строку

```
LIBS = -lldap
```

вместо строки

```
LIBS =
```

Выполните команды.

```
make
```

```
make install
```

Если у вас уже имеется файл конфигурации `dhcpd.conf`, то для автоматического переноса данных в LDAP следует использовать скрипт `contrib/dhcpd-conf-to-ldap.pl` (предварительно в него необходимо вписать ваши данные).

Примерный вариант LDIF-файла:

```
dn: cn=dhcpd.example.ru, dc=example, dc=ru
```

```
objectClass: top
```

```
objectClass: dhcpServer
```

```
cn: dhcpd.example.ru
```

```
dhcpServiceDN: cn=DHCP Config, dc=example, dc=ru
```

```
dn: cn=DHCP Config, dc=example, dc=ru
```

```
cn: DHCP Config
```

```
objectClass: top
```

```
objectClass: dhcpService
```

```
objectClass: dhcpOptions
```

```
dhcpPrimaryDN: cn=dhcpd.example.ru, dc=example, dc=ru
```

```
dhcpStatements: default-lease-time 600
```

```
dhcpStatements: max-lease-time 7200
```

```
dhcpStatements: log-facility local7
```

```
dhcpOption: domain-name "example.ru"
```

```
dhcpOption: domain-name-servers 10.1.2.1
```

```
dn: cn=10.1.2.0, cn=DHCP Config, dc=example, dc=ru
```

```
cn: 10.1.2.0
```

```
objectClass: top
```

```
objectClass: dhcpSubnet
```

```
objectClass: dhcpOptions
```

```
dhcpNetMask: 24
dhcpRange: 10.1.2.2 10.1.2.253
dhcpOption: domain-name-servers 10.1.2.1
dhcpOption: routers 10.1.2.1

dn: cn=test, cn=DHCP Config, dc=example, dc=ru
cn: test
objectClass: top
objectClass: dhcpHost
objectClass: dhcpOptions
dhcpHWAddress: ethernet 00:00:e2:58:ac:a6
dhcpStatements: fixed-address 10.1.2.45
```

Создайте конфигурационный файл `/etc/dhcpd.conf` примерно следующего содержания:

```
ldap-server "localhost";
ldap-port 389;
ldap-username "cn=Manager, dc=example, dc=ru";
ldap-password "secret";
ldap-base-dn "dc=example, dc=ru";
ldap-method dynamic;
ddns-update-style ad-hoc;
```

Запуск сервера DHCP произведите командой (вместо `fxp0` укажите ваш интерфейс).

```
/usr/sbin/dhcpd fxp0
```

В результате поиск данных для выдачи IP-адресов по DHCP будет производиться в LDAP.

Установка и настройка сервера FTP

Скачайте FTP-сервер - <ftp://ftp.proftpd.org/distrib/source/proftpd-1.2.9.tar.bz2>

Установите сервер командами.

```
tar xvfj proftpd-1.2.9.tar.bz2
cd proftpd-1.2.9
```

```
./configure --with-modules=mod_ldap  
make  
make install
```

В конфигурационном файле /usr/local/etc/proftpd.conf укажите строки.

```
LDAPServer localhost  
LDAPDNInfo cn=Manager,dc=example,dc=ru secret  
LDAPDoAuth on "ou=users,dc=example,dc=ru"
```

Файл LDIFF для добавления тестового пользователя выглядит следующим образом.

```
dn: cn=test, ou=users, dc=netup, dc=ru  
cn: test  
sn: test  
givenName: Test  
objectClass: inetOrgPerson  
objectClass: uidObject  
objectClass: organizationalPerson  
objectClass: posixAccount  
objectClass: top  
uid: test  
userPassword: {MD5}2Fe034RYzgb7xht2pYxcpA==  
uidNumber: 10001  
gidNumber: 10001  
homeDirectory: /home/test
```

Применить файл можно командой.

```
ldapadd -D "cn=Manager,dc=example,dc=ru" -w secret <  
netup.ldiff
```

В результате будет создана учётная запись FTP test с паролем qwerty (в LDAP хранится MD5-хеш {MD5}2Fe034RYzgb7xht2pYxcpA==). Домашняя директория пользователя – /home/test.

Запуск сервера FTP можно осуществить командой.

```
/usr/local/sbin/proftpd
```

Установка и настройка сервера DNS

Скачайте сервер DNS по адресу <ftp://ftp.isc.org/isc/bind9/9.2.3/bind-9.2.3.tar.gz>.

Разархивируйте командами.

```
tar xvfz bind-9.2.3.tar.gz
cd bind-9.2.3
```

Скопируйте файлы командами:

```
cp contrib/sdb/ldap/ldapdb.c bin/named/
cp contrib/sdb/ldap/ldapdb.h bin/named/include/
```

Отредактируйте файл `bin/named/Makefile.in`. Необходимо указать строки вместо тех, что есть.

```
DBDRIVER_OBJS = ldapdb.@O@
DBDRIVER_SRCS = ldapdb.c
DBDRIVER_INCLUDES = -I/usr/local/include
DBDRIVER_LIBS = -L/usr/local/lib -lldap -llber
```

Отредактируйте файл `bin/named/main.c`. Необходимо указать строки.

```
include <ldapdb.h>
```

после строки

```
#include "xxdb.h
```

```
ldapdb_init();
```

после строки

```
xxdb_init();
```

```
ldapdb_clear();
```

после строки

```
xxdb_clear();
```

После этого можно произвести сборку и установку командой.

```
./configure  
make  
make install
```

Сервер DNS будет установлен по пути `/usr/local/sbin/named`.

Конфигурационный файл `/etc/named.conf`.

Пример конфигурации домена, данные для которого хранятся в LDAP.

```
zone "hosting.example.ru" {  
    type master;  
    database "ldap ldap://127.0.0.1/dc=hosting,dc=example,dc=ru 172800";  
};
```

Примерный вариант LDIF-файла для создания зоны с одной записью.

```
dn: dc=hosting,dc=example,dc=ru  
dc: hosting  
objectClass: dcObject  
objectClass: Organization  
o: DNS
```

```
dn: relativeDomainName=zzz,dc=hosting,dc=example,dc=ru  
objectClass: top  
objectClass: dNSZone  
relativeDomainName: zzz  
aRecord: 10.1.2.105  
dNSTTL: 3600  
zoneName: hosting.example.ru
```

```
dn: dNSTTL=3600+relativeDomainName=@,dc=hosting,dc=example,dc=ru
```

```
objectClass: top
objectClass: dNSZone
relativeDomainName: @
sOARRecord: hosting.example.ru. root.example.ru.
2004040304 86400 900 3600000 360
0
dNSTTL: 3600
zoneName: hosting.example.ru
mXRecord: 10 mail.example.ru.
nSRecord: ns.example.ru.
nSRecord: ns2.example.ru.
aRecord: 10.0.0.1
```

Настройка биллинговой системы

Настройки доступа к серверу LDAP из UTM указываются в конфигурационном файле `/netup/utm5/utm5.cfg`. Для этого используются следующие параметры:

`ldap_enable`

Включить ли поддержку LDAP. Значение по умолчанию – `no`. Для включения необходимо указать `yes`.

`ldap_host`

IP-адрес сервера LDAP. Значение по умолчанию – `127.0.0.1`.

`ldap_login`

Логин для доступа к серверу LDAP. Значение по умолчанию не предусмотрено. Пример: `cn=Manager,dc=example,dc=ru`.

`ldap_password`

Пароль для доступа к серверу LDAP. Значения по умолчанию не предусмотрено.

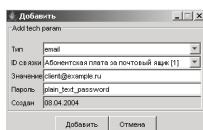
`ldap_ping_timeout`

Периодичность проверки соединения с сервером LDAP в секундах. Значение по умолчанию – 60 секунд.

`ldap_base_dn`

Верхняя часть вашего дерева LDAP. Эта строка добавляется к запросам на сервер LDAP. Пример: ou=users, dc=example, dc=ru. В этом случае запрос на добавление почтового ящика будет выглядеть как cn=user@example.ru, ou=users, dc=example, dc=ru.

Для добавления почтового ящика пользователю через биллинговую систему необходимо задать новый технический параметр на подключённую услугу. Обычно это периодическая услуга, стоимость которой равна абонентской плате за пользование почтовым ящиком.



При добавлении технического параметра произойдет автоматическое создание новой записи на сервере LDAP, и почтовый ящик будет доступен пользователю.

Для добавления связи адресов MAC- IP через биллинговую систему необходимо подключить пользователю услугу типа «Передача IP-трафика» и указать IP-адрес и MAC-адрес. При этом будет автоматически добавлена запись на сервере LDAP в раздел cn=DHCP Config. Например,

```
dn: cn=10.1.2.45, cn=DHCP Config, dc=example, dc=ru
cn: 10.1.2.45
objectClass: top
objectClass: dhcpHost
objectClass: dhcpOptions
dhcpHWAddress: ethernet 00:00:e2:58:ac:a6
dhcpStatements: fixed-address 10.1.2.45
```

Ссылки

RFC-2251 по протоколу LDAP – <http://www.rfc-editor.org/rfc/rfc2251.txt>.

Проект OpenLDAP – <http://www.openldap.org/>.

Проект BerkeleyDB – <http://www.sleepycat.com/>.

Контрольный пример

Контрольный пример предназначен для проверки корректности функционирования биллинговой системы NetUP UTM на вашем сервере. Суть проверки заключается в загрузке в базу данных параметров пяти клиентов и эмулирования работы этих пользователей в течение трёх месяцев. Необходимые данные для запуска контрольного примера находятся на CD-ROM с биллинговой системой NetUP UTM.

Внимание. Остановите сервисы критичные к изменению даты на сервере.

Остановите ядро биллинговой системы `utm5_core`.

Установите дату на сервере на 00 часов 00 минут 1 апреля 2003 года.

Для FreeBSD:

```
date 0304010000
```

Для Linux:

```
date 0401000003
```

Для загрузки данных в базу выполните команды.

```
mysqladmin drop UTM5
mysqladmin create UTM5
mysql UTM5 < UTM5_MYSQL_kp.sql
mysql -f UTM5 < UTM5_MYSQL_update.sql
```

Произведите корректировку данных в файле `kp.pl` о том, на каком порту принимает NetFlow-пакеты ядро биллинговой системы, а также путь к программе-генератору NetFlow-пакетов – `utm5_flowgen` (обычно `/netup/utm5/bin/utm5_flowgen`).

Запустите ядро биллинговой системы `utm5_core`.

Запустите программу kp.pl командой.

```
perl kp.pl
```

В процессе работы программы дата на сервере будет меняться с 1 апреля 2003 г. до 1 июля 2003 г. Таким образом, будет эмулирована работа тестовых пользователей в течение трёх месяцев: апреля, мая, июня 2003 г.

Первый месяц (апрель 2003 г.)

	cli1	cli2	cli3	cli4	cli5
Объем в день, МБ	0,5	2	4	10	40
Количество дней	30	30	30	30	30
Объем за месяц, МБ	15	60	120	300	1200
Стоимость единицы превышения	0,2	0,2	0,2	0,15	0,15
Предоплачено, МБ	50	50	50	500	500
Стоимость превышения	0	2	14	0	105
Абонплата	3	3	3	100	100
Остаток	-3	-5	-17	-100	-205

Второй месяц (май 2003 г.)

	cli1	cli2	cli3	cli4	cli5
Объем в день, МБ	1	2,5	5	20	50
Количество дней	31	31	31	31	31
Объем за месяц, МБ	31	77,5	155	620	1550
Стоимость единицы превышения	0,2	0,2	0,2	0,15	0,15
Предоплачено, МБ	50	50	50	500	500
Стоимость превышения	0	5,5	21	18	157,5
Абонплата	3	3	3	100	100
Остаток	-6	-13,5	-41	-218	-462,5

Третий месяц (июнь 2003 г.)

	cli1	cli2	cli3	cli4	cli5
Объем в день, МБ	1,5	3	6	30	60
Количество дней	30	30	30	30	30
Объем за месяц, МБ	45	90	180	900	1800
Стоимость единицы превышения	0,2	0,2	0,2	0,15	0,15
Предоплачено, МБ	50	50	50	500	500

Стоимость превышения	0	8	26	60	195
Абонплата	3	3	3	100	100
Остаток	-3	-11	-29	-160	-295
Итого остаток	-9	-24,5	-70	-378	-757,5

В случае корректной работы биллинговой системы, полученные вами цифры после отработки `кр.pl` должны совпадать с указанными в таблице.

После проведения работ установите корректную дату на сервере.

Руководство пользователя

Личный кабинет

Для входа в личный кабинет пользователя необходимо запустить любой интернет-браузер (Internet Explorer, Opera, Mozilla, Konqueror, lynx и др.) и набрать в адресной строке:

```
https://SERVER/cgi-bin/utm5/aaa5
```

где SERVER замените на IP-адрес либо доменное имя сервера провайдера. При этом префикс `https://` указывает на то, что необходимо использовать шифрование SSL. В случае если веб-сервер не поддерживает SSL, то интернет-браузером будет выдана ошибка. В этом случае можно использовать префикс `http://`, но при этом возникает опасность перехвата логина и пароля злоумышленниками.

В личном кабинете доступна информация по лицезовому счёту абонента, отчёты по потребленным услугам, возможность управлять доступом, пополнение счёта, отсылка сообщения администратору и др.

Вкл/Выкл интернета

Здесь можно включить или выключить Интернет. Если не удастся включить Интернет, то это означает, что аккаунт заблокирован. Заблокирован он может быть по двум причинам: либо закончились деньги на счёту, либо администратор заблокировал аккаунт.

Отчёты

В этом разделе можно узнать информацию, которая известна о вас системе. Здесь есть данные о состоянии счёта, используемом тарифном плане, логин (для тех, кто забыл). Можно узнать дату начала и дату окончания учётного периода, а также посмотреть статистику по использованному трафику, разделённую по разным классам трафика и за указанный период. Также здесь содержится информация и времени предыдущей сессии в рабочем кабинете и размер установленной абонент-

ской платы. Здесь же доступны графики загрузки за текущий день и месяц.

История платежей

Здесь можно посмотреть даты и суммы всех платежей, которые осуществлялись на вашем счету.

Пополнение счёта

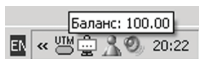
Можно пополнить свой счёт самостоятельно, если есть предоплаченная Интернет-карточка. Карточка содержит номер и пин-код. Если ввести их в соответствующие поля, ваш счёт пополнится на номинал карточки. Также можно выписать квитанцию на оплату через банк.

Настройки

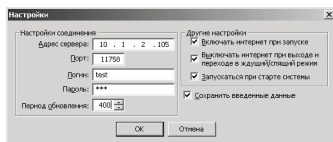
В этом разделе можно поменять пароль на вход в рабочий кабинет.

Утилита utm5 wintray

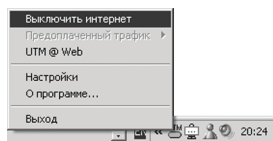
Для оперативного и удобного доступа к балансу лицевого счета рекомендуется использовать утилиту utm5_wintray.



Данная программа запускается на компьютере пользователя и с настраиваемым периодом обновляет информацию о текущем состоянии баланса и количестве оставшегося предоплаченного трафика. При запуске необходимо указать где находится ядро биллинговой системы и логин/пароль для доступа.



Также при помощи этой утилиты можно производить включение и выключение Интернета.



Модуль коммутируемых и VPN-соединений

Модуль коммутируемых соединений

Модуль коммутируемых соединений представляет собой сервер NetUP RADIUS и предназначен для обработки запросов на авторизацию и учёт потребленных услуг.

Сервер NetUP RADIUS представляет собой приложение, которое в реальном времени обрабатывает поступающие к нему запросы по протоколу Remote Authentication Dial In User Service (RADIUS) – RFC 2138 и RFC 2139.

При обработке запросов сервер NetUP RADIUS обращается к ядру системы по протоколу URFA.

Описание протокола RADIUS

Протокол Remote Authentication Dial In User Service (RADIUS) описан в документах RFC 2138 и RFC 2139 и предназначен для обеспечения авторизации, аутентификации и аккаунтинга между сервером доступа и сервером авторизации.

Протоколу RADIUS официально присвоен порт UDP 1812.

Данный протокол был разработан для облегчения управления большим количеством модемных пулов. Например, когда в сети имеются несколько устройств, к которым должны иметь доступ пользователи, и на каждом устройстве содержится информация обо всех пользователях, то администрирование такой системы значительно усложняется, превращаясь в головную боль администратора. Проблема может быть решена установкой одного центрального сервера авторизации, а все сетевые устройства производили бы запросы к нему по стандартному протоколу RADIUS. При этом в качестве серверов доступа могут выступать устройства любых производителей, поддерживающие протокол RADIUS.

В общем виде формат RADIUS-пакета выглядит, как показано на рисунке.



Поле «Код» размером один байт и может принимать следующие значения: 1 – запрос на проверку доступа (Access-Request), 2 – доступ разрешён (Access-Accept), 3 – в доступе отказано (Access-Reject), 4 – запрос на учёт (Accounting-Request), 5 – ответ на запрос на учёт (Accounting-Response), 255 – зарезервированное значение (Reserved).

Поле «Длина» размером два байта указывает на полный размер всего пакета RADIUS.

Поле «Аутентификатор» размером 16 байтов содержит информацию для проверки подлинности пересылаемых пакетов.

Поле «Атрибуты» RADIUS переменной длины содержит полезные данные. Данное поле состоит из последовательности атрибутов и соответствующих присвоенных значений. Каждый атрибут имеет своё числовое обозначение (идентификатор). Например, атрибут User-Name имеет числовое значение 1 и содержит в себе имя пользователя, а атрибут User-Password имеет значение 2 и содержит в себе пароль пользователя в открытом виде.

При подключении пользователя сначала происходит его аутентификация, т. е. проверка подлинности. Для этого сервер доступа предлагает пользователю ввести логин (имя учётной записи) и пароль. После ввода этих данных сервер доступа формирует пакет Access-Request и отправляет его серверу RADIUS.

В данном пакете содержатся введённые пользователем данные. Следует учесть, что есть несколько методов аутентификации и содержимое пакета с запросом на аутентификацию будет содержать разные данные в зависимости от того, какой метод используется. Наиболее распространенные методы – PAP и CHAP.

PAP (Password Authentication Protocol) – простейший протокол аутентификации. Он не предусматривает использования шифрования паролей. При аутентификации по этому методу сервер доступа заполняет атрибуты «Имя пользователя» (User-Name) и «Пароль пользователя» (User-Password) и отправляет запрос серверу RADIUS.

CHAP (Challenge Handshake Authentication Protocol) – более сложный и защищённый протокол, описанных в документе RFC 1994. Он использует зашифрованные пароли. При аутентификации по этому протоколу сервер доступа генерирует случайное 16-байтное значение (CHAP challenge) и отправляет его на компьютер пользователя. После этого компьютер поль-

зователя отправляет обратно в незашифрованном виде логин пользователя, и зашифрованное значение (хэш), полученное из строки вызова, идентификатора сеанса и пароля пользователя с применением алгоритма MD5. Протокол MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) очень похож на CHAP.

После получения данных аутентификации сервер RADIUS проводит их проверку и, если они корректны, то отправляет обратно пакет «Доступ разрешен» (Access-Accept). В противном случае посылается пакет «В доступе отказано» (Access-Reject).

В пакете «Доступ разрешен» (Access-Accept) также в поле атрибутов могут передаваться параметры для установки сеанса, например, IP-адрес пользователя (Framed-IP-Address), тип протокола (Framed-Protocol), максимальное количество времени, отведённое на сессию (Session-Timeout).

Сервер доступа, получив пакет «Доступ разрешен» (Access-Accept), устанавливает соединение с пользователем. Если данный пакет не получен либо получен пакет «В доступе отказано» (Access-Reject), то соединение разрывается.

После успешного установления соединения сервер доступа отправляет на сервер RADIUS пакет «Запрос на учёт» (Accounting-Request), в котором содержится информация о начале предоставления услуги и параметрах сеанса: порт на который подключился пользователь (NAS-Port), идентификатор сессии (Acct-Session-Id). Это так называемая стартовая запись.

При окончании сеанса отправляется пакет со стоп-записью. В этом пакете содержится информация об окончании предоставления услуги. Также в этом пакете содержится информация о том, сколько времени предоставлялась услуга (Acct-Session-Time), сколько принято или передано байт в ходе работы.

Настройка сервера RADIUS

Сервер NetUP RADIUS устанавливается по следующему пути `/netup/utm5/bin/utm5_radius`. Для его работы необходима загрузка в ядро биллинговой системы модуля `/netup/utm5/lib/utm5_radius/liburfa-radius.so`. Чтобы сделать это, необходимо указать путь к файлу модуля в конфигурационном файле `utm5.cfg`, либо произвести загрузку этого модуля в интерфейсе администратора.

При запуске сервера RADIUS без параметров, он загружает настройки из файла `/netup/utm5/radius5.cfg`. Для указания альтернативного файла конфигурации можно пользоваться параметром командной строки `-c`, например,

```
utm5_radius -c /etc/radius5.cfg
```

Файл конфигурации сервера RADIUS

Файл состоит из строк вида

параметр=значение

Строки, начинающиеся с символа «#», считаются комментарием.

Возможные параметры:

core_host

Адрес хоста, на котором запущено ядро биллинговой системы. Значение по умолчанию – `127.0.0.1`.

core_port

Порт, на котором запущено ядро биллинговой системы. Значение по умолчанию – `11758`. В случае, если `core_host` не указан или пуст, данный параметр неактивен.

radius_login

Логин системного пользователя в биллинговой системе. Значение по умолчанию – radius.

radius_password

Пароль системного пользователя в биллинговой системе. Значение по умолчанию – radius.

radius_ssl_type

Тип безопасного соединения SSL. Возможные варианты: tls1, ssl3, none. В случае если указано значение none, будет использоваться нешифрованное соединение.

radius_acct_port

Порт для приема пакетов Accounting. Значение по умолчанию – 1813.

radius_auth_port

Порт для приема пакетов Access. Значение по умолчанию – 1812.

radius_acct_host

IP-адрес узла для приёма пакетов Accounting. Значение по умолчанию – 0.0.0.0 (все интерфейсы).

radius_auth_host

IP-адрес узла для приема пакетов Access. Значение по умолчанию – 0.0.0.0 (все интерфейсы).

log_file_main

Путь к файлу, куда будет записываться журнал событий. Например, /netup/utm5/log/radius_main.log.

log_file_debug

Путь к файлу, куда будет записываться журнал событий. Например, /netup/utm5/log/radius_debug.log.

`radius_auth_mppe`

Разрешить MPPE 128 бит при авторизации по протоколу MS-CHAP-v2. Значение по умолчанию не предусмотрено. Для включения необходимо указать значение `enable`.

`radius_auth_vap`

Запретить авторизоваться заблокированным пользователям. Для включения необходимо указать значение 1. Значение по умолчанию — 0, т. е. заблокированные пользователи по умолчанию могут авторизоваться.

`radius_ippool_acct_timeout`

Время в секундах, на которое происходит блокирование IP-адресов в пуле после отправки пакета `Access-Accept`. Значение по умолчанию — 30 секунд, т. е. если в течение этого времени не пришел пакет `Accounting-Start`, то IP-адрес снова считается свободным и может быть выдан при следующей успешной авторизации.

`radius_ippool_timeout`

Время в секундах, на которое происходит блокирование IP-адресов в пуле после прихода пакета `Accounting-Start`. Значение по умолчанию не предусмотрено (адреса блокируются до прихода пакета `Accounting-Stop`).

`radius_auth_null`

При включении этой опции (значение `yes` или `enable`) сервер RADIUS будет принимать и успешно авторизовать запросы без пароля в случае, если пароль пользователя пуст. Имеются в виду запросы без атрибута CHAP, PAP или MSCHAP авторизации. По умолчанию, опция выключена.

`radius_auth_h323_remote_address`

При включении данной опции есть возможность авторизоваться не по атрибуту `user-name`, а по значению VSA атрибута от Cisco: `h323-remote-address`, которое содержит в себе IP-адрес клиента, инициировавшего сессию. При приеме запро-

са с данным атрибутом сервер RADIUS использует его значение (IP-адрес в формате x.x.x.x) в качестве логина, т. е. для успешной авторизации должна присутствовать связка услуги IP-телефонии, в которой в поле логина указан IP-адрес клиента (в формате x.x.x.x, например, 192.168.1.56).

radius_nas_port_vpn

Указанный в данном поле тип порта будет использоваться при подключении по VPN. В случае если при авторизации по услуге VPN будет передан другой тип порта, то радиус-сервер откажет в авторизации. Данная опция применяется для предотвращения подключения пользователей коммутируемого доступа по VPN. Обычно значение равно 5 (Virtual).

radius_nas_port_dialup

Аналогично для коммутируемого доступа. Данную директиву можно указать несколько раз. Например,

```
radius_nas_port_dialup=0
```

```
radius_nas_port_dialup=1
```

В данном примере для подключения по услуге «Коммутируемый доступ» необходимо подключаться к порту типа 0 (Async) либо 1 (Sync). В противном случае сервер RADIUS откажет в авторизации и на сервер доступа будет выслан пакет Access-Reject.

radius_nas_port_tel

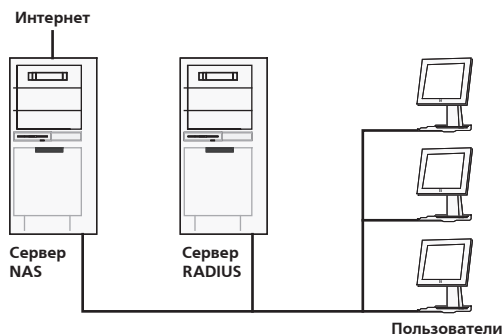
Аналогично для услуги «Телефония».

radius_card_autoadd

При задании значения yes, эта опция разрешает проводить автоматическую регистрацию пользователей через сервер RADIUS по предоплаченной интернет-карте. При этом пользователь в поле «Логин» указывает номер карты, а в поле «Пароль» – пин-код карты.

Настройка VPN

Схема сетевого комплекса для работы с виртуальными частными сетями (VPN) с авторизацией по протоколу RADIUS. В приведённой модели сервер доступа (NAS) и сервер авторизации RADIUS являются разными машинами, однако, довольно часто встречаются варианты, когда они являются одним физическим сервером.



При этом предоставляться будет услуга типа «IP-трафик» со статическим IP-адресом. Для добавления этой услуги в интерфейсе администратора нужно выбрать раздел «Тарификация, Услуги, Добавить».

Редактировать...
Параметры услуги IP-трафика

Название услуги: [Интернет - ТП канал]
Комментарий:
Периодическая стоимость: 1000.0
Тип периода: ежедневно
Метод снятия денег: в начале учётного периода
Дата начала: 01.01.2004 0:00:00 [Выбрать]
Срок завершения действия: 01.01.2005 0:00:00 [Выбрать]
Reset regular traffic: [X]

Тарифы: [Добавить] [Удалить] [Редактировать]

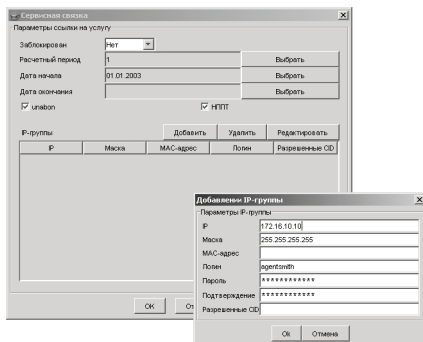
Класс трафика	Количество	Стоимость
Incoming	0	0.0

Предоплаченные единицы: [Добавить] [Удалить] [Редактировать]

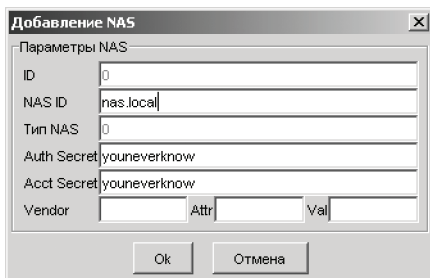
Класс трафика	Количество
Incoming	100
Outgoing	10

[Ok] [Отмена]

Указывается стоимость трафика. Затем данную услугу можно подключить клиенту. При этом необходимо указать IP-адрес, который будет автоматически выдаваться клиенту при подключении по VPN.



Также необходимо добавить в систему сервер доступа, к которому будет осуществляться подключение. Для этого перейдите в раздел «Настройки, Список NAS, Добавить».



Если всё настроено корректно, то при старте `utm5_radius` на экране должна появиться надпись.

```

    Fetched: 2 IP from 3Group
    
```

При успешной авторизации пользователя радиус-сервер должен отобразить текст.

```

    Packet from vpn.test.ru
    
```

```

'a' connecting
    
```

```

    CHAP
    
```

```

    CHAP Challenge size: 16
    
```

```

Authorized
IP claimed: 0xac12bd13
Reply:
RPacket:
Code: 2; ID: 50
<Vendor: 0; Attr: 6>[4]
<Vendor: 0; Attr: 7>[4]
<Vendor: 0; Attr: 8>[4]
<Vendor: 0; Attr: 10>[4]
<Vendor: 0; Attr: 12>[4]
<Vendor: 0; Attr: 13>[4]
<Vendor: 0; Attr: 27>[4]
Size send: 62
Next...
Size: 104; HDR.Size: 104
Acct: Recv...
RPacket:
Code: 4; ID: 112
<Vendor: 0; Attr: 1>[1]
<Vendor: 0; Attr: 6>[4]
<Vendor: 0; Attr: 7>[4]
<Vendor: 0; Attr: 8>[4]
<Vendor: 0; Attr: 9>[4]
<Vendor: 0; Attr: 32>[16]
<Vendor: 0; Attr: 40>[4]
<Vendor: 0; Attr: 41>[4]
<Vendor: 0; Attr: 44>[17]
<Vendor: 0; Attr: 50>[0]
<Vendor: 0; Attr: 61>[4]

Acct: Packet from vpn.test.ru
Session ID: 23028-a1079623271
Acct: START
Acct: IP: 0xac12bd13

```

```
Acct: For user a
Bind: 0xac12bd13: 0xac12bd13
Acct: Reply:
RPacket:
Code: 5; ID: 112
Size send: 20
Acct: Next...
```

Настройка сервера доступа (NAS)

Настройка в среде FreeBSD

Установите сервер VPN (пакет PoPToP). Его можно установить из поставляемых с дистрибутивом FreeBSD портов.

Создайте файл конфигурации `/etc/pptpd.conf`. Он имеет следующий формат.

```
option /etc/ppp/ppp.conf
localip 172.16.0.1
pidfile /var/run/pptpd.pid
```

Создайте файл конфигурации `/etc/ppp/ppp.conf`. Он имеет такой формат.

```
loop:
    set timeout 0
    set device /dev/ppp

local

# Server (local) IP address, Range for Clients, and
# Netmask
set ifaddr 172.16.0.1 172.16.0.2-254 255.255.255.255
set server /tmp/loop "" 0177

pptp:
load loop
enable chap
#enable mschapv2
#enable pap
```

```
set radius /etc/radius.conf
```

В данном случае включена авторизация CHAP. Строки, включающие авторизацию PAP, MSCHAP-v2 закомментированы.

Создайте файл конфигурации `/etc/radius.conf`. Он имеет следующий формат.

```
auth 127.0.0.1:1812 mysecret
acct 127.0.0.1:1813 mysecret
```

В данном случае указывается, что сервер NetUP RADIUS принимает соединения на адрес 127.0.0.1 (на локальной машине) на портах 1812 и 1813. Секретное слово для общения с сервером RADIUS – mysecret

Запустите сервер VPN

```
pptpd
```

На этом конфигурация сервера доступа на базе FreeBSD закончена. Клиенты могут начать беспрепятственно авторизоваться.

Настройка в среде Linux (на примере RedHat 9.0)

Для обновления пакета `ppp` необходимо выполнить команды.

```
cvs -d :pserver:cvs@pserver.samba.org:/cvsroot login
cvs
cvs -z5 -d :pserver:cvs@pserver.samba.org:/cvsroot co
ppp
cd ppp/
./configure
make
make install
```

Если сервер CVS недоступен, то можно скачать исходный код программы по следующей ссылке <ftp://ftp.samba.org/pub/ppp/ppp-2.4.2.tar.gz>.

Далее необходимо выполнить команды.

```
tar xvfz ppp-2.4.2.tar.gz
```

```
cd ppp-2.4.2
./configure
make
make install
```

Установите сервер VPN (пакет PoPToP). Его можно взять из дистрибутива RedHat, либо загрузить с сервера <http://www.porttop.org/>.

Создайте файл конфигурации `/etc/pptpd.conf`. Он имеет следующий формат.

```
option /etc/ppp/options
localip 172.16.0.1
```

Создайте файл конфигурации `/etc/ppp/options`. Он имеет такой формат.

```
auth
#require-pap
require-chap
#require-mschap-v2
local
172.16.0.1:
plugin radius.so
```

В данном случае включена авторизация CHAP. Строки, включающие авторизацию PAP, MSCHAP-v2 закомментированы.

Внесите корректировки в файл конфигурации `/etc/radius-client/radiusclient.conf`. Необходимо внести информацию о вашем сервере RADIUS.

```
authserver localhost:1812
acctserver localhost:1813
```

В данном случае указывается, что сервер NetUP RADIUS находится по адресу 127.0.0.1 (на локальной машине) на портах 1812 и 1813. Секретное слово для общения с сервером RADIUS – `mysecret` указывается в другом конфигурационном файле `/etc/radiusclient/servers`.

```
localhost mysecret
```

Запустите сервер VPN.

```
pptpd
```

На этом конфигурация сервера доступа на базе Linux Red Hat 9.0 закончена. Если всё выполнено без ошибок, то клиенты должны беспрепятственно авторизоваться.

Настройка в среде Windows

Для настройки VPN в среде Windows (Windows 2000 и Windows 2003) используется служба RRAS (Routing and Remote Access Service).

Для ее настройки используется пункт меню (Control Panel | Administrative Tools | Routing and Remote Access service). Выбрав этот пункт, вы попадаете в консоль MMC администрирования данной службы. Вам необходимо нажать правой кнопкой на имя компьютера и выбрать “Configure and Enable Routing and Remote Access” и следовать шагам помощника.

После окончания работы помощника будет настроена базовая конфигурация службы RRAS. Для настройки адреса Radius-сервера надо нажать правой кнопкой на имя компьютера, вызвать свойства объекта. На вкладке Security в поле Authentication provider выбрать RADIUS Authentication и нажать кнопку Configure. Далее внести адрес radius-сервера в список и нажать ОК. То же самое повторить с полем Radius Accounting.

На этом базовая конфигурация сервера доступа закончена. Для получения более подробной информации пользуйтесь справочной системой консоли RRAS и документацией на сайте <http://www.microsoft.com>.

Настройка на Cisco

Примерный вариант конфигурационного файла на маршрутизаторе Cisco, версия IOS - IOS (tm) 3600 Software (C3620-IS-M), Version 12.3(3a), RELEASE SOFTWARE (fc2):

```
!  
vpdn enable  
!
```

```

vpdn-group 1
! Default PPTP VPDN group
accept-dialin
    protocol pptp
    virtual-template 1
!
!
interface Virtual-Template1
    ip address 192.168.20.1 255.255.255.0
    ip tcp header-compression
    ip mroute-cache
    no peer default ip address
    ppp authentication ms-chap-v2 chap
!
radius-server host 10.0.0.1 auth-port 1812 acct-port
1813
radius-server key secret
!

```

При этом маршрутизатор будет принимать подключения от клиентов с авторизацией по MS CHAP версии 2 либо CHAP и авторизацией на сервере RADIUS 10.0.0.1.

Активные сессии на маршрутизаторе можно просмотреть, выполнив команду

```

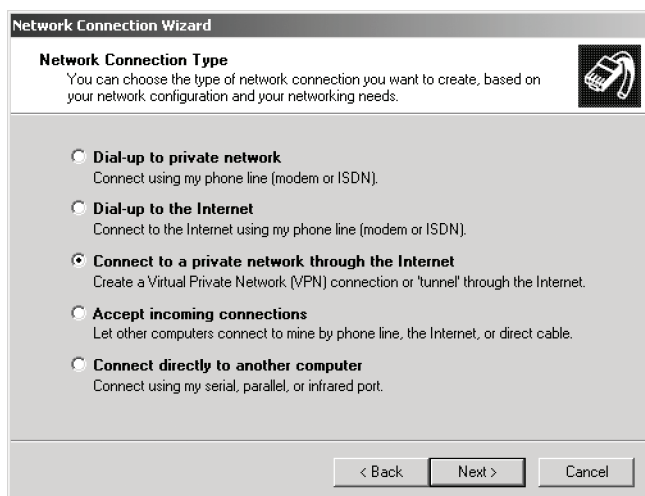
Router#show vpdn session
%No active L2TP tunnels
%No active L2F tunnels
PPTP Session Information Total tunnels 1 sessions 1
LocID RemID TunID Intf      Username      State      Last
Chg Uniq ID
10      32768 11      Vi3      vpn_netup     establd
00:00:23 9

```

Настройка компьютера клиента на работу с VPN

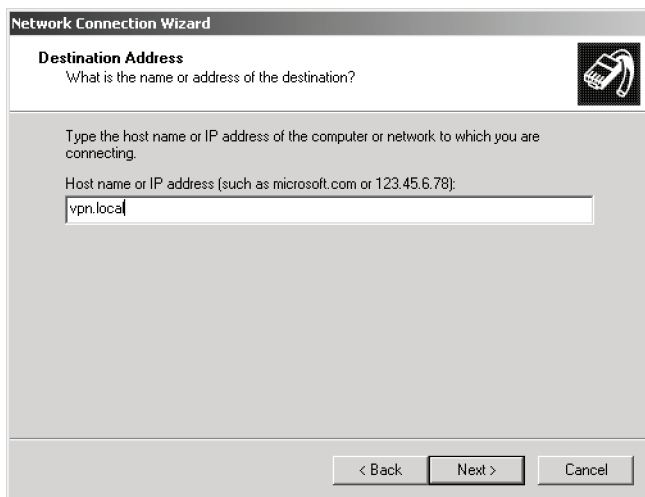
Пример приведён для установленной ОС Windows 2000.

Откройте раздел «Сетевые соединения» («Network Connections»). Выберите создание нового соединения: «Добавить новое соединение» («Create a new connection»).



Выберите тип подключения: VPN.

Укажите IP-адрес или имя сервера VPN. Например, vpn.local.



Network Connection Wizard

Destination Address
What is the name or address of the destination?

Type the host name or IP address of the computer or network to which you are connecting.

Host name or IP address (such as microsoft.com or 123.45.6.78):

vpn.local

< Back Next > Cancel

Выберите, для кого будет создано соединение: для всех пользователей компьютера или только для текущего пользователя.



Network Connection Wizard

Connection Availability
You may make the new connection available to all users, or just yourself.

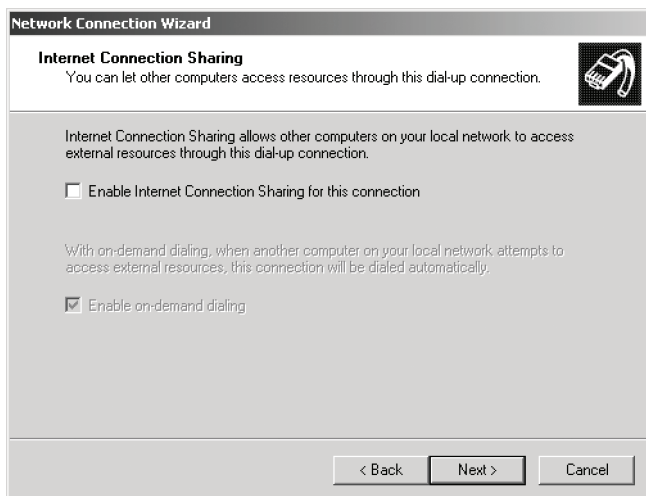
You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.

Create this connection:

☒ For all users
☐ Only for myself

< Back Next > Cancel

Выберите, будет ли соединение общим для всех пользователей локальной сети (если соединение устанавливается на сервере локальной сети).

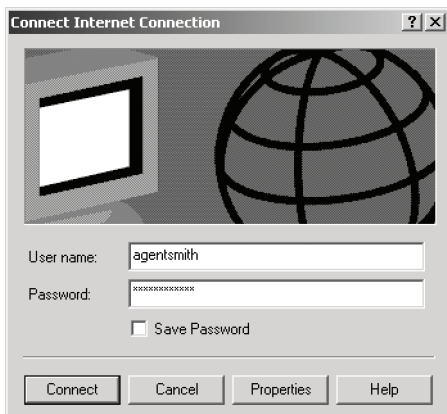


Введите название соединения и нажмите кнопку «Finish» для завершения работы мастера.



После окончания работы мастера будет создано новое соединение VPN. Для того, чтобы его установить нужно в разделе

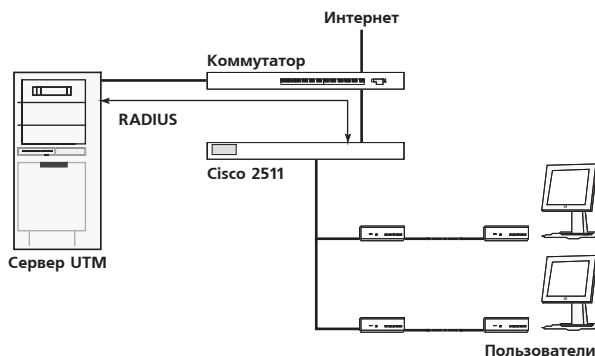
«Сетевые соединения» дважды кликнуть на него мышкой, затем ввести корректные логин и пароль.



Настройка коммутлируемого доступа

Сервер NetUP RADIUS устанавливается по следующему пути: `/netup/utm5/bin/utm5_radius`. Для его работы необходима загрузка в ядро биллинговой системы модуля `/netup/utm5/lib/utm5_radius/liburfa-radius.so`. Чтобы сделать это, необходимо указать путь к файлу модуля в конфигурационном файле `utm5.cfg`, либо произвести загрузку этого модуля в интерфейсе администратора.

Схема сетевого комплекса для предоставления коммутлируемого доступа с авторизацией по протоколу RADIUS.



При этом предоставляться будет услуга типа «Коммутлируемый доступ» с динамическим IP-адресом. Для добавления этой услуги в интерфейсе администратора выберите меню (Тарификация | Услуги | Добавить). Укажите стоимость 1 часа соединения для разных времени суток и дней недели, а также название IP-пула, из которого будут выдаваться IP-адреса клиентам. Пул IP при этом должен быть сконфигурирован на сервере доступа.

В случае если устройство не поддерживает IP-пулы (например, программный сервер доступа), необходимо сконфигурировать пул в разделе (Настройки | IP-пулы).

Добавление услуги Dial-up

Параметры услуги Dial-up:

Название услуги: ТП Псковской

Комментарий:

Тип периода: ежемесячно

Метод снятия денег: в течение всего учётного периода

Периодическая составляющая стоимости: 0

Название плана: None

Максимальный таймаут: 72000

Дата начала: 01.01.2003

Срок завершения действия: 01.01.2006

Обслуживать предоплаченные единицы: ☒

Vendor: AB VM

Временные диапазоны:

Название временного диапазона	Стоимость
All day (1)	20.0

Добавление услуги Dial-up

Параметры услуги Dial-up:

Название услуги: ТП Псковской

Комментарий:

Тип периода: ежемесячно

Метод снятия денег: в течение всего учётного периода

Периодическая составляющая стоимости: 0

Название плана: None

Максимальный таймаут: 72000

Дата начала: 01.01.2003

Срок завершения действия: 01.01.2006

Обслуживать предоплаченные единицы: ☒

Vendor: AB VM

Временные диапазоны:

Название временного диапазона	Стоимость
All day (1)	20.0

В разделе «Установка радиус-параметров» можно указать дополнительные атрибуты RADIUS, которые будут передаваться в пакете Access-Accept при успешной авторизации пользователя. Можно указать в числовом виде:

- код вендора;
- код атрибута;
- значение атрибута;
- признак строки либо числового значения.

Таким образом, можно организовать специфичные параметры соединения (ограничение скорости, протокол, адреса и др.) для каждой услуги либо NAS. Обычно требуется поддержка этих атрибутов сервером доступа.

После этого услугу можно подключать клиентам. При этом необходимо указывать логин и пароль, которые необходимо будет указывать клиенту при подключении.

В случае если указано поле «Разрешённые CID», то при подключении пользователя по VPN либо Dial-up это значение будет сравниваться с радиус атрибутом Calling-Station-Id (31). Обычно в этом атрибуте содержится адрес вызывающей станции (компьютера клиента). В случае VPN это может быть IP-адрес, в случае PPPoE это может быть MAC-адрес, в случае Dial-up это может быть телефонный номер вызывающего абонента. Ответственность за заполнение этого поля полностью лежит на сервере доступа. Если не будет найдено совпадения между значением указанным в поле «Разрешённые CID» и тем, что указано в радиус атрибуте Calling-Station-Id, то авторизация не пройдет и пользователь не сможет воспользоваться услугой. При сравнении данное поле рассматривается как регулярное выражение. Регулярные выражения строятся по следующим основным правилам: ^ – начало строки; \$ – конец строки; [0-9] – цифры от 0 до 9; {n} означает, что предыдущее объявление должно повторяться ровно n раз; (x|y) означает, что в этом месте может находиться либо x, либо y.

Для примера разберём шаблон ^5409652\$. Данный шаблон указывает, что номер вызывающей станции (радиус атрибут Calling-Station-Id) должен быть полностью равен значению «5409652». Владелец номера 5409652 сможет воспользоваться данной услугой, а владелец номера 70955409652 – нет.

В качестве другого примера разберем шаблон 5409652. В этом примере не указаны открывающий символ ^ и закрывающий символ \$, поэтому номер вызывающей станции может содержать значение «5409652». Такие номера, как 70955409652 или 78125409652 будут подходить под этот шаблон, и владельцы этих номеров смогут воспользоваться данной услугой.

В случае если необходимо задать несколько разрешённых номеров, то можно задать шаблон в виде `^(5409652|5409653)$`. В этом случае при сравнении будет проверяться совпадение с номером 5409652 либо номером 5409653.

В случае если указано поле «Разрешённые CSID», то при подключении пользователя по VPN либо коммутируемому соединению это значение будет сравниваться с атрибутом RADIUS Called-Station-Id (30). Обычно в этом атрибуте содержится адрес вызываемой станции (адрес сервера доступа). В случае Dial-up это может быть телефонный номер провайдера, который клиенты набирают при подключении. Данное поле рассматривается, как регулярное выражение, по тем же правилам, что и для поля «Разрешённые CID».

Также необходимо добавить в систему сервер доступа, к которому будет осуществляться подключение. Это можно сделать в разделе «Настройки, Список NAS, Добавить».

Если всё настроено корректно, то при старте `utm5_radius` на экране должна появиться надпись.

DLink: 2 dialup

При успешной авторизации пользователя сервер RADIUS должен отобразить текст:

Size: 83; HDR.Size: 83

Recv...

RPacket:

Code: 1; ID: 86

<Vendor: 0; Attr: 1>[6]

<Vendor: 0; Attr: 2>[16]

<Vendor: 0; Attr: 4>[4]

<Vendor: 0; Attr: 5>[4]

<Vendor: 0; Attr: 6>[4]

<Vendor: 0; Attr: 7>[4]

<Vendor: 0; Attr: 31>[5]

<Vendor: 0; Attr: 61>[4]

Packet from 10.1.2.95

'dialup' connecting

PAP

Passwords: 123 and 123

TR<1 TRDET:1 SIZE:1> fits...

Tmp Balance: 0 for 35721 seconds

BEFORE:10:13:1

AFTER:20:8:22

Calculated maximum session time: 35721

Reply:

RPacket:

Code: 2; ID: 86

<Vendor: 0; Attr: 6>[4]

<Vendor: 0; Attr: 7>[4]

<Vendor: 0; Attr: 10>[4]

<Vendor: 0; Attr: 12>[4]

<Vendor: 0; Attr: 13>[4]

<Vendor: 0; Attr: 27>[4]

<Vendor: 9; Attr: 1>[17]

Size send: 81

Next...

```

Size: 99; HDR.Size: 99
Acct: Recv...
RPacket:
Code: 4; ID: 87
<Vendor: 0; Attr: 1>[6]
<Vendor: 0; Attr: 4>[4]
<Vendor: 0; Attr: 5>[4]
<Vendor: 0; Attr: 6>[4]
<Vendor: 0; Attr: 7>[4]
<Vendor: 0; Attr: 8>[4]
<Vendor: 0; Attr: 31>[5]
<Vendor: 0; Attr: 40>[4]
<Vendor: 0; Attr: 41>[4]
<Vendor: 0; Attr: 44>[8]
<Vendor: 0; Attr: 45>[4]
<Vendor: 0; Attr: 61>[4]

```

```

Acct: Packet from 10.1.2.95
Session ID: 00000059
Acct: START
Acct: IP: 0xac10100c
Acct: For user dialup
Acct: Reply:
RPacket:
Code: 5; ID: 87
Size send: 20
Acct: Next...

```

После отключения пользователя сервер RADIUS должен отобразить текст.

```

Size: 135; HDR.Size: 135
Acct: Recv...
RPacket:
Code: 4; ID: 94
<Vendor: 0; Attr: 1>[6]

```

```
<Vendor: 0; Attr: 4>[4]
<Vendor: 0; Attr: 5>[4]
<Vendor: 0; Attr: 6>[4]
<Vendor: 0; Attr: 7>[4]
<Vendor: 0; Attr: 8>[4]
<Vendor: 0; Attr: 31>[5]
<Vendor: 0; Attr: 40>[4]
<Vendor: 0; Attr: 41>[4]
<Vendor: 0; Attr: 42>[4]
<Vendor: 0; Attr: 43>[4]
<Vendor: 0; Attr: 44>[8]
<Vendor: 0; Attr: 45>[4]
<Vendor: 0; Attr: 46>[4]
<Vendor: 0; Attr: 47>[4]
<Vendor: 0; Attr: 48>[4]
<Vendor: 0; Attr: 49>[4]
<Vendor: 0; Attr: 61>[4]
```

```
Acct: Packet from 10.1.2.95
Session ID: 0000005B
Acct: STOP
Discount: 1 0.00305556 for 11
```

Настройка сервера доступа (NAS)

Настройка оборудования Cisco

Пример конфигурационного файла маршрутизатора фирмы Cisco для работы по коммутлируемым соединениям. Пример приведен для Cisco 2511 с 16 модемами. Версия IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(3).

```
aaa new-model
aaa authentication password-prompt password:
aaa authentication username-prompt login:
aaa authentication login default local
aaa authentication ppp default group radius
```

```

aaa authorization exec default local
aaa authorization network default group radius
aaa accounting delay-start
aaa accounting network default start-stop group ra-
dus

!
interface Group-Async0
    ip unnumbered Ethernet0
    encapsulation ppp
    async mode interactive
    peer default ip address pool TEST
    ppp authentication pap
    group-range 1 16
!
interface Ethernet0
    ip address 192.168.0.2 255.255.255.0
    no ip mroute-cache
!
ip local pool TEST 172.16.0.2 172.16.0.254
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
async-bootp dns-server 195.161.112.6
!
radius-server host 192.168.0.3 auth-port 1812 acct-
port 1813
radius-server retransmit 3
radius-server key mysecret
!
line 1 16
    script modem-off-hook offhook
    script callback callback
    modem InOut
    modem autoconfigure type usr_sportster
    
```

```
transport input all
autoselect during-login
autoselect ppp
speed 115200
!
end
```

Дополнительная информация

RFC-2138: <ftp://ftp.rfc-editor.org/in-notes/rfc2138.txt>.

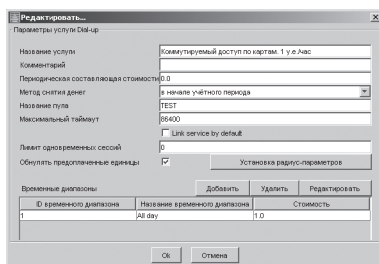
RFC-2139: <ftp://ftp.rfc-editor.org/in-notes/rfc2139.txt>.

Пакет PoPToP: <http://www.poptop.org/>.

Автоматическая регистрация пользователей

В UTM предусмотрены два варианта активации предоплаченных интернет-карт для получения услуги коммутируемого доступа: через гостевой доступ и через обычный доступ с автоматической регистрацией пользователя. В первом случае пользователь, соединяясь впервые, использует известный ему гостевой логин и пароль и регистрируется в системе. После регистрации он заходит в систему, используя свои собственные параметры доступа. Во втором случае пользователь вводит номер и пин-код своей карточки в качестве логина и пароля для коммутируемого соединения, его регистрация производится автоматически, и пользователь сразу же получает доступ в интернет.

Для реализации автоматической регистрации пользователей этими двумя способами необходимо создать тарифный план и подключить к нему услугу коммутируемого доступа с соответствующей стоимостью соединений по коммутируемым линиям.



После создания тарифного плана необходимо сгенерировать пул предоплаченных интернет-карт и привязать их к созданному тарифному плану.

Гостевой доступ

В случае реализации гостевого доступа необходимо создать пользователя, логин и пароль которого будут известны всем перед регистрацией. Например, логин guest и пароль guest.

Добавление карты

Параметры карты

Идентификатор пула: 0

Количество: 1000

Баланс: 10

Валюта: USD

Длина ПИН-кода: 8

Random number: ☐

Использовать до: 27.01.2005 Days: 30

ID тарифа: dialup (1) Выбрать

Progress: 22%

Гость должен быть настроен таким образом, чтобы иметь возможность только получать доступ с сайта для активации интернет-карт. Время соединения также может быть ограничено, например, 600 секундами.

Необходимо создать услугу «Коммутируемый доступ» со следующими параметрами: пул – GUEST, максимальный таймаут соединения – 600 сек., стоимость соединения – 0 у. е. в час.

Настроить...

Параметры услуги Dial-up

Название услуги: Сайт - гостевой доступ

Комментарий:

Периодическая составляющая стоимости: 0.0

Метод снятия денег: в начале учётного периода

Название пула: GUEST

Максимальный таймаут: 600

Дата начала: Oct 27, 2004 Выбрать

Срок завершения действия: Выбрать

☒ Линия одноразовых сессий

Обслуживать предоплаченные единицы: ☒ Установка-radius-параметров

Временные диапазоны

ID временного диапазона	Название временного диапазона	Стоимость
1	All day	0.0

Добавить Удалить Редактировать

OK Отмена

При этом на маршрутизаторе, либо в UTM, необходимо создать пул IP-адресов с именем GUEST и адресами из определённого диапазона, например, 172.16.0.0/16. Маршрутизатор необходимо настроить таким образом, чтобы клиенты из этого диапазона адресов могли получать доступ только к веб-серверу, на котором производится активация карт, и серверу DNS. В целях безопасности рекомендуется организовать отдельный сервер DNS, который не связан с интернетом, и содержит только записи, необходимые клиенту для доступа к веб-серверу регистрации.

При входе на веб-сервер регистрации интернет-карт абонент выбирает пункт меню «Авторегистрация пользователя» и вводит данные, указанные на интернет-карте. Если все данные введены корректно, и карта не была активирована прежде либо заблокирована, то в UTM автоматически будет создан новый карточный пользователь, и абонент получит информацию о логине и пароле для подключения по коммутируемым линиям. Выбирая пункт меню «Вход в UTM» на странице регистрации и указав логин и пароль, выданные системой после регистрации, абонент может получить доступ к своему личному кабинету, где для него доступна статистика его лицевого счёта.

Доступ с автоматической регистрацией

Для реализации моментального доступа по интернет-картам требуется дополнительная настройка сервера RADIUS. В конфигурационном файле сервера RADIUS /netup/utm5/radius5.cfg необходимо указать опцию

```
radius_card_autoadd=yes
```

После перезапуска сервер RADIUS будет автоматически регистрировать пользователя в UTM при первой попытке доступа по предоплаченной карте.

Для получения доступа, абонент должен указать номер интернет-карты в качестве логина и её пин-код в качестве пароля. Если пользователь подключается по этой карте впервые, то сервер RADIUS произведёт автоматическую регистрацию, и абонент моментально получит доступ в интернет. Каждый раз при подключении пользователь указывает номер карты, как логин, и пин-код – как пароль. После того, как баланс карты истечёт, пользователь должен активировать новую карту.

Следует отметить, что подобная автоматическая регистрация возможна только в случае использования авторизации по протоколу PAP. Этот способ по умолчанию используется Windows для авторизации при подключении с помощью модемного доступа, поэтому в большинстве случаев дополнительных настроек не требуется. Однако следует иметь в виду, что иногда

необходимо менять конфигурацию клиентов, прежде чем они смогут автоматически зарегистрировать таким образом.

При правильно настроенном доступе с автоматической регистрации пользователя при первом входе в журнале сервера RADIUS должны появиться следующие записи:

```
?Debug : Oct 27 12:08:00 RADIUS Auth: Packet from
<example.org>

?Debug : Oct 27 12:08:00 RADIUS Auth: User <5> con-
necting

  ERROR : Oct 27 12:08:00 RADIUS DBA: Can't find login
<5>

  ERROR : Oct 27 12:08:00 RADIUS DBA: Can't find card
login <000000005>

?Debug : Oct 27 12:08:00 RADIUS Auth: Attempt to add
new Card user: <5>

?Debug : Oct 27 12:08:00 RADIUS DBA: Sending Auto-Add
Request for Card-ID: 5

?Debug : Oct 27 12:08:00 RADIUS URFA[plugin]: DLink:
SLID/SID/AID: 14/6/14

?Debug : Oct 27 12:08:00 RADIUS URFA[plugin]: Account
<14> with balance <10.000>

?Debug : Oct 27 12:08:00 RADIUS Auth: Got AutoAdd 14
UID from core.

  ERROR : Oct 27 12:08:00 RADIUS DBA: Can't find login
<5>

?Debug : Oct 27 12:08:00 RADIUS DBA: login_store
iter->second.dialup.session_count:0

  Info : Oct 27 12:08:00 RADIUS Auth: User <5> added.

?Debug : Oct 27 12:08:00 RADIUS Auth: Auth scheme:
PAP

?Debug : Oct 27 12:08:00 RADIUS Auth: PAP: <51154755>
vs <51154755>

?Debug : Oct 27 12:08:00 RADIUS Auth: PAP: Authorized
user <5>

?Debug : Oct 27 12:08:00 RADIUS Auth: Dialup session
limit:0 session count:0 for user:5

?Debug : Oct 27 12:08:00 RADIUS Auth: Calculated max-
imum session time: 36000
```

?Debug : Oct 27 12:08:00 RADIUS DBA: dialup_link_update called for slink:14

?Debug : Oct 27 12:08:00 RADIUS DBA: soft dialup_link_update for slink:14 session_count:1

Контрольный пример

Контрольный пример предназначен для проверки корректности функционирования биллинговой системы NetUP UTM на вашем сервере. Суть проверки заключается в загрузке в базу данных параметров трех клиентов и эмулирования работы этих пользователей в течение трёх месяцев. Необходимые данные для запуска контрольного примера находятся на CD-ROM с биллинговой системой NetUP UTM.

Внимание. Остановите сервисы критичные к изменению даты на сервере.

Остановите ядро биллинговой системы `utm5_core`.

Установите дату на сервере на 00 часов 00 минут 1 апреля 2003 года.

Для FreeBSD:

```
date 0304010000
```

Для Linux:

```
date 0401000003
```

Для загрузки данных в базу выполните команды.

```
mysqladmin drop UTM5  
mysqladmin create UTM5  
mysql UTM5 < UTM5_MYSQL_kp_dialup.sql  
mysql -f UTM5 < UTM5_MYSQL_update.sql
```

Произведите корректировку данных в файле `kp_dialup.pl` о том, на каком порту принимает Radius Accounting-пакеты процесс `utm5_radius`, а также путь к программе-генератору RADIUS-пакетов – `utm5_radgen` (обычно `/netup/utm5/bin/utm5_radgen`).

Запустите ядро биллинговой системы `utm5_core` и сервер RADIUS `utm5_radius`.

Запустите программу `kp.pl` командой.

```
perl kp_dialup.pl
```

В процессе работы программы дата на сервере будет меняться с 1 апреля 2003 г. до 1 июля 2003 г. Таким образом, будет эмулирована работа тестовых пользователей в течение трёх месяцев: апреля, мая, июня 2003 г.

В случае корректной работы биллинговой системы, полученные вами цифры после отработки `kp_dialup.pl` должны совпадать с указанными в таблицах.

После проведения работ установите корректную дату на сервере.

Первый месяц (апрель 2003 г.). Количество дней – 30.

	dialup1		dialup2		dialup3	
	8.00-19.59	20.00-7.59	8.00-19.59	20.00-7.59	8.00-19.59	20.00-7.59
Длительность в день, час	0,1	0,1	0,2	0,2	0,3	0,3
Объем за месяц, час	3	3	6	6	9	9
Стоимость, у.е./час	1	2	1	2	1	2
Стоимость, у.е.	3	6	6	12	9	18
Абонплата	10		10		10	
Остаток	-19		-28		-37	

Второй месяц (май 2003 г.). Количество дней – 31.

	dialup1		dialup2		dialup3	
	8.00-19.59	20.00-7.59	8.00-19.59	20.00-7.59	8.00-19.59	20.00-7.59
Длительность в день, час	0,1	0,1	0,2	0,2	0,3	0,3
Объем за месяц, час	3,1	3,1	6,2	6,2	9,3	9,3
Стоимость, у.е./час	1	2	1	2	1	2
Стоимость, у.е.	3,1	6,2	6,2	12,4	9,3	18,6
Абонплата	10		10		10	
Остаток	-19,3		-28,6		-37,9	

Третий месяц (июнь 2003 г.). Количество дней – 30.

	dialup1		dialup2		dialup3	
	8.00- 19.59	20.00- 7.59	8.00- 19.59	20.00- 7.59	8.00- 19.59	20.00- 7.59
Длительность в день, час	0,1	0,1	0,2	0,2	0,3	0,3
Объем за ме- сяц, час	3	3	6	6	9	9
Стоимость, у.е./час	1	2	1	2	1	2
Стоимость, у.е.	3	6	6	12	9	18
Абонплата	10		10		10	
Остаток	-19		-28		-37	
Итого оста- ток	-57,3		-84,6		-111,9	

В случае корректной работы биллинговой системы, полученные вами цифры после отработки `cr.pl` должны совпадать с указанными в таблице.

После проведения работ установите корректную дату на сервере.

Модуль телефонии

Модуль IP-телефонии

Модуль IP-телефонии представляет собой сервер NetUP RADIUS и предназначен для обработки запросов на авторизацию и учёт потребленных услуг от голосовых шлюзов, гейткиперов (gatekeepers), голосовых прокси-серверов.

Сервер NetUP RADIUS – это приложение, которое в реальном времени обрабатывает поступающие к нему запросы по протоколу Remote Authentication Dial In User Service (RADIUS) – RFC 2138 и RFC 2139.

При обработке запросов сервер NetUP RADIUS обращается к ядру системы по протоколу URFA.

Более подробное описание протокола RADIUS можно найти в разделе «Модуль коммутируемых и VPN-соединений».

Терминология

IP-телефония (IP telephony)

Общий термин, означающий передачу речи по сетям с использованием протокола IP. Так же для обозначения этой технологии используются термины: Voice over IP (VoIP), Internet Telephony.

ТфОП (PSTN)

Сокращение от словосочетания «телефонная сеть общего пользования». В это понятие включены городские и национальные сети обычной телефонии. Также используется термин PSTN – сокращение от «Public Switched Telephony Network».

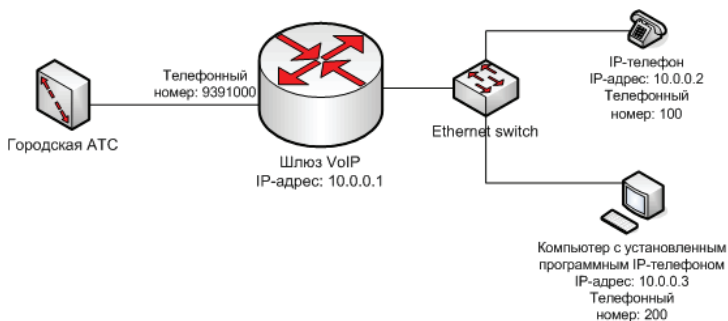
АОН (Caller ID)

Номер вызывающего абонента. Также используется термин ANI – сокращение от «Automatic Number Identification». Часто услуга определения номера вызывающего абонента называется АОН.

Шлюз IP-телефонии (VoIP gateway)

Устройство, имеющее порт для подключения к сети на базе протокола IP, а также по необходимости порты для подключения к ТфОП. Обычно данное устройство служит для стыковки ТфОП и IP-сети.

Примером устройства данного типа может служить маршрутизатор Cisco 3620 с модулем NM-2V + VIC2FXO.



При таком подключении шлюз организует преобразование голосового трафика из сети на базе протокола IP в ТфОП. Таким образом, пользователь с IP-телефоном либо компьютером с установленным программным телефоном (Microsoft NetMeeting, OpenPhone и др.) может вызывать абонента городской телефонной сети (ТфОП).

Аналогично и в обратную сторону: абонент городской телефонной сети (ТфОП) может вызывать абонента в сети с протоколом IP. Для этого необходимо набрать номер шлюза в сети ТфОП (на схеме это 9391000) и затем после авторизации (если этот механизм включен на шлюзе) набрать внутренний номер абонента в сети с протоколом IP (на схеме это номера 100 и 200).

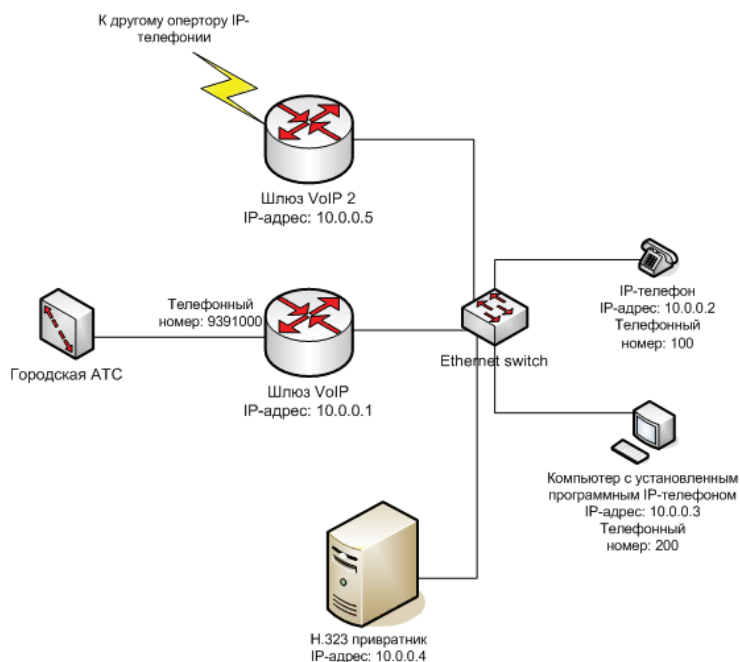
Н.323

Стандарт, предложенный Международным союзом электросвязи (ITU-T), описывающий построение сетей IP-телефонии. Стандарт описывает протоколы, связанные с регистрацией оборудования IP-телефонии (RAS – Registration, Admission

and Status), установления соединения (H.225.0, H.245), передачи речи, авторизации пользователей и др.

Н.323 привратник (Н.323 гейткипер, Н.323 gatekeeper)

Привратник отвечает за регистрацию оконечного оборудования (шлюзов, клиентских устройств), контроль прав доступа, номерной план. Практически все привратники имеют возможность проводить авторизацию и передачу статистики по состоявшимся звонкам по протоколу RADIUS.



В такой схеме все устройства сети должны зарегистрироваться на привратнике. При этом авторизация может проводиться по протоколу RADIUS с использованием стандартной схемы Access-Request.

В итоге у привратника находится таблица IP-адресов и номеров всех устройств в сети. Соответственно, все вызовы начинаются с обращения к привратнику для преобразования набранного номера в IP-адрес. При этом привратник может запросить у сервера RADIUS авторизацию данного звонка

и передать заполненные атрибуты Called-Station-Id (набранный номер) и Calling-Station-Id (номер вызывающего абонента). При этом сервер RADIUS проверяет баланс пользователя, тарифный план на вызываемое направление, и если все вычисления прошли успешно, то передает пакет Access-Accept, в котором может указать максимальное время соединения для данного пользователя по данному направлению. Обычно эта информация указывается в атрибуте h323-credit-time, vendor 9 (Cisco).

В случае, если авторизация прошла успешно, после согласования всех параметров устанавливается соединение между вызываемым и вызывающим терминалами. При этом привратник передает на сервер RADIUS пакет о начале соединения (Accounting-Start), в котором указывает параметры установленного соединения.

В случае, если терминалы находятся в одной сети, то общение между ними производится напрямую. Если вызываемый терминал находится в другой сети, то общение между терминалами производится через один из шлюзов. Также возможен вариант, когда общение клиента производится только с привратником. В этом случае привратник выполняет функции прокси, и реальные IP-адреса терминалов скрываются. Такая схема работы применяется, если канал напрямую между терминалами по качеству хуже (например, большие потери IP-пакетов либо задержки) чем между привратником и каждым терминалом.

По окончании соединения привратник пересылает на сервер RADIUS пакет с информацией о завершившемся звонке. В пакете указываются время соединения, причина завершения соединения и другие параметры. По этим данным сервер RADIUS проводит тарификацию сессии, списание средств и запись в журнал событий.

Кодеки

Алгоритмы сжатия звука на передающей стороне и декодирования на принимающей стороне. В основном это используется для минимизации трафика, поэтому кодеки в основном характеризуются полосой пропускания необходимой для передачи

речи с использованием этого кодека. При передаче голоса без сжатия потребуются полоса пропускания в 64 Кбит/сек.

Кодеки с высокой степенью сжатия требуют больших вычислительных ресурсов, поэтому для кодирования большого количества голосовых потоков используются специальные микросхемы, так называемые DSP-процессоры.

Название кодека	Поток, Кбит/сек	Качество
G.711	64	Высокое
G.723.1	5.3 – 6.4	Среднее
G.729	8	Среднее

IVR

Сокращение от «Interactive Voice Response». Представляет собой технологию голосовых меню и часто используется для авторизации пользователей ТфОП для звонков по IP-телефонии. При этом используется следующая последовательность шагов.

1. Абонент ТфОП набирает городской номер доступа оператора IP-телефонии. При этом трубку поднимает шлюз IP-телефонии (например, Cisco 3640 с платой E1), подключенный к этой линии.

2. Шлюз загружает звуковой файл (обычно расширение у файлов .au) с записанным приглашением и проигрывает его абоненту. При этом обычно предлагается ввести номер и пин-код предоплаченной телефонной карты.

3. После ввода определённого количества цифр производится авторизация с введенными данными на сервере RADIUS. При этом номер карты обычно записывается в атрибут 1 (UserName), а пин-код – в атрибут 2 (Password).

4. В случае успешной авторизации сервер RADIUS присылает пакет Access-Accept, в котором указывает количество оставшихся средств на счету. Для этого используются атрибуты h323-credit-amount и h323-currency с vendor=9 (Cisco). Шлюз IP-телефонии загружает соответствующие голосовые файлы и проигрывает абоненту остаток средств на счету и предлагает ввести номер, по которому необходимо выпол-

нить вызов. Следует заметить, что в основном IP-телефония выгодна для звонков на большие расстояния (междугородние и международные звонки).

5. После ввода номера производится повторная авторизация на сервере RADIUS, при этом дополнительно передается атрибут `Called-Station-Id`, в котором записывается набранный номер. В зависимости от остатка средств на счету и стоимости минуты соединения по этому направлению сервер RADIUS вычисляет максимальное время сессии и передает вычисленное время в пакете `Access-Accept` в атрибуте `h323-credit-time`.

6. После получения положительного ответа от сервера RADIUS шлюз IP-телефонии устанавливает соединение с вызываемым абонентом. Соединение будет разорвано, если длительность сессии составит количество секунд, вычисленное на предыдущем шаге.

7. При установлении соединения на сервер RADIUS отсылается пакет `Accounting-Start`, при разрыве – пакет `Accounting-Stop`.

Настройка сервера

Установка и запуск H323 гейткипера

Для установки загрузите установочный пакет с <http://www.gnu.org/h323download.html> для вашей операционной системы (доступны версии под FreeBSD, Linux, Windows, Solaris) и установите согласно инструкциям.

Гейткипер можно также установить из исходных кодов. Для этого необходимо загрузить библиотеку PWLib, доступную по адресу http://www.openh323.org/bin/pwlib_1.5.2.tar.gz и установить её командами:

```
tar xvfz pwlib_1_5_2.tgz
cd pwlib
./configure
gmake
gmake install
```

Загрузить пакет Openh323 можно по адресу http://www.openh323.org/bin/openh323_1.12.2.tar.gz.

Он устанавливается командами:

```
tar xvfz openh323_1_12_3.tgz
cd openh323
./configure
gmake
gmake install
```

Загрузить пакет openh323gk можно по адресу <http://www.gnu.org/download/gnugk-2.2beta2.tgz>.

Он устанавливается командами:

```
tar xvfz gnugk-2.2beta2.tgz
cd openh323gk
export HAS_ACCT=1
./configure
gmake
```

```
gmake install
```

Конфигурационный файл /etc/opensk.ini

Подробное описание опций можно найти в документе <http://www.gnugk.org/h323manual.html>.

Ниже приведён пример конфигурационного файла /etc/opensk.ini с кратким описанием.

```
[Gatekeeper::Main]
```

```
Fourtytwo=42
```

```
TimeToLive=600
```

```
Name=localhost
```

```
[RoutedMode]
```

```
GKRouted=1
```

```
[RasSrv::GWPrefixes]
```

```
cisco=5,8,9
```

Префиксы телефонных номеров (E.164), которые будут перенаправляться на шлюз, зарегистрированный под именем cisco. В данном примере номера, начинающиеся на 5, 8 и 9 будут перенаправляться на шлюз. При этом шлюз должен сам зарегистрироваться на гейткипере.

```
[RasSrv::PermanentEndpoints]
```

```
212.1.1.1=voip;1,2,3
```

Префиксы телефонных номеров (E.164), которые будут перенаправляться на шлюз с адресом 212.1.1.1. В данном примере номера, начинающиеся на 1, 2 и 3 будут перенаправляться на этот шлюз. При этом шлюз не должен сам регистрироваться на гейткипере.

```
[GkStatus::Auth]
```

```
rule=allow
```

```
[Gatekeeper::Acct]
```

```
RadAcct=required;start,stop
```

```
default=allow
```

```
[RadAcct]
```

```
Servers=127.0.0.1:1813;
```

IP-адрес и порт, на котором принимает соединения сервер NetUP RADIUS.

```
LocalInterface=
```

```
RadiusPortRange=10000-11000
```

```
DefaultAcctPort=1813
```

```
SharedSecret=secret
```

```
RequestTimeout=3500
```

```
IdCacheTimeout=9000
```

```
SocketDeleteTimeout=60000
```

```
RequestRetransmissions=4
```

```
RoundRobinServers=1
```

```
AppendCiscoAttributes=1
```

```
IncludeEndpointIP=1
```

```
FixedUsername=
```

```
[Gatekeeper::Auth]
```

```
RadAliasAuth=required;RRQ,ARQ
```

```
default=allow
```

```
[RadAliasAuth]
```

```
Servers=127.0.0.1:1812;
```

IP-адрес и порт, на котором принимает соединения сервер NetUP RADIUS.

```
LocalInterface=
```

```
RadiusPortRange=10000-11000
```

```
DefaultAuthPort=1812
```

```
SharedSecret=secret
```

```
RequestTimeout=2000
```

```
IdCacheTimeout=9000
```

```
SocketDeleteTimeout=60000
```

```
RequestRetransmissions=2
RoundRobinServers=1
AppendCiscoAttributes=1
IncludeTerminalAliases=1
IncludeEndpointIP=1
FixedUsername=
FixedPassword=

[CallTable]
DefaultCallDurationLimit=3600

[Proxy]
Enable=1
```

Включить режим прокси. В этом режиме пакеты от ATA-186 идут только до и от гейткипера. Если не указывать эту опцию, то пакеты от ATA-186 будут направляться на шлюз, минуя гейткипер.

При таких настройках гейткипер будет проводить авторизацию при каждом звонке через сервер RADIUS (порт 1812). Статистика звонков будет передаваться на сервер RADIUS (порт 1813).

Запуск гейткипера

Запуск гейткипера осуществляется командой:

```
/usr/local/bin/gnugk -c /etc/opengk.ini -o /var/log/gnugk.log -ttttt &
```

Протоколирование работы гейткипера будет вестись в файл /var/log/gnugk.log. За работой гейткипера можно наблюдать, подключившись по протоколу telnet на порт состояния командой

```
telnet 127.0.0.1 7000
```

Настройка Cisco ATA-186

В настройках ATA-186 необходимо указать следующие параметры

`UID0: 100`

Первый телефонный номер.

`UID1: 200`

Второй телефонный номер.

`GkOrProxy: 10.1.2.105`

Адрес гейткипера.

`LoginID0: test1`

Логин, который будет использоваться для авторизации звонков первого телефонного номера. При этом на гейткипер будет отсылаться пароль такой же, как логин.

`LoginID1: test2`

`LBRCCodec:3`

`RxCodec:3`

`TxCodec: 3`

`ConnectMode: 0x00060403`

`UseSIP: 0`

Настройка шлюза VoIP на базе Cisco 26xx, 36xx, 53xx

Пример приведен для Cisco 3640 IOS 12.2(11)T8 с контроллером E1.

```
aaa accounting connection h323 start-stop group radius
```

```

!
controller E1 1/0
    pri-group timeslots 1-31
!
!
voice class codec 1
    codec preference 1 g729r8
    codec preference 2 g711ulaw
    codec preference 3 g723r63
!
!
gw-accounting aaa
    acct-template callhistory-detail
!
!
interface Ethernet0/1
    ip address 21.1.1.1 255.255.255.252
    no ip mroute-cache
    full-duplex
    no cdp enable
    h323-gateway voip interface
    h323-gateway voip id GK ipaddr 21.1.1.2 1718
    h323-gateway voip h323-id cisco
!
!
interface Serial1/0:15
    no ip address

```

```

no logging event link-status
isdn switch-type primary-net5
isdn protocol-emulate network
isdn incoming-voice voice
isdn map address .* plan isdn type subscriber
isdn calling-number xxxxxx
no isdn outgoing display-ie
no cdp enable

```

!

!

```

dial-peer voice 2 pots
destination-pattern T
direct-inward-dial
port 1/0:15
prefix 96

```

!

gateway

!

```

dial-peer voice 4 voip
destination-pattern 100
voice-class codec 1
session target ras

```

!

Для звонков через Microsoft NetMeeting также следует указать следующие команды:

!

```

voice service voip
h323
h245 tunnel disable
h245 caps mode restricted

```

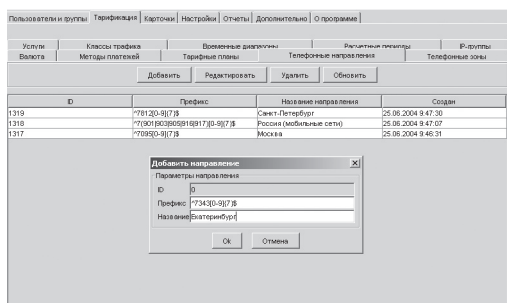
!

В настройках аудио программы NetMeeting необходимо выбрать кодек CCITT u-Law, 8,000 KHz; 8Bit; Mono.

Настройка UTM

Создание направлений и зон

Для определения направления звонка используются регулярные выражения. Строка (префикс) задает шаблон, по которому определяется, в какой город либо страну производится вызов. Направления и префиксы можно задать в интерфейсе администратора в разделе (Тарификация | Телефонные направления).



Шаблоны строятся по следующим основным правилам:

^ – начало строки.

\$ – конец строки.

[0-9] – цифры от 0 до 9.

{n} означает, что предыдущее объявление должно повторяться ровно n раз.

(x|y) означает, что в этом месте может находиться либо x, либо y.

Для примера разберем шаблон ^7095[0-9]{7}\$, который определяет направление «Москва». Он означает, что телефонный номер должен начинаться с четырёх цифр 7095, за которыми следуют ровно семь любых цифр, после чего номер

должен заканчиваться. Например, под этот шаблон попадают номера 70955409652 и 70959391000.

Аналогично для шаблона ^7(901|903|905|916|917)[0-9]{7}\$, который определяет направление «Россия (мобильные сети)». Он означает, что телефонный номер должен начинаться с цифры 7, затем следует одна из следующих комбинаций цифр: 901, 903, 905, 916, либо 917. Затем следуют ровно семь любых цифр, после чего номер должен заканчиваться. Например, под этот шаблон попадают номера 79167772233 и 79161112233.

В дальнейшем при проведении поиска UTM сортирует все направления в порядке уменьшения длины шаблона, т. е. в самом начале списка окажутся направления с наиболее длинными шаблонами. Поиск производится до первого совпадения.

Пример

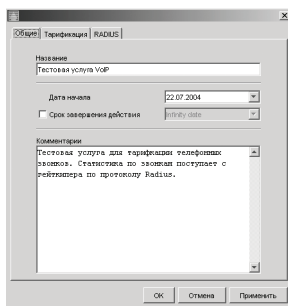
Созданы следующие направления:

Идентификатор направления	Название направления	Шаблон
1	Россия	^7
2	Москва	^7095
3	МТС (моб.)	^7916

При этом осуществляется два тестовых звонка по номеру 7-916-7777777 и номеру 7-812-8888888. Для первого звонка будет определено направление 3 – МТС (моб.). Для второго звонка будет определено направление 1 – Россия.

Создание услуги IP-телефонии

Необходимо создать услугу с типом «Телефония» и указать дату начала предоставления услуги и дату окончания.



В разделе «Тарификация» можно указать следующие параметры:

Размер абонентской платы

Периодическая составляющая услуги. Указанная в этом поле сумма спишется с лицевого счета абонента за один расчетный период.

Параметры списания абонентской платы

Определяет характер списания периодической составляющей стоимости услуги. При плавном списании сумма спишется плавно в течение расчетного периода.

Весплатное время

Не тарифицируемое время в начале каждого звонка. Размерность – секунды.

Длительность начального периода

Период в начале звонка, в течение которого действует округление до значения указанного в поле «Шаг начального периода». Размерность – секунды.

Шаг начального периода

Шаг округления в начальном периоде. Размерность – секунды.

Шаг последующего периода

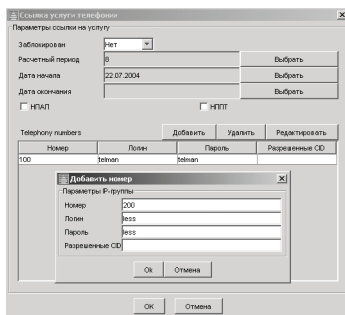
Шаг округления, действующий после завершения начального периода. Размерность – секунды.

Размер единицы тарификации

Данное поле указывает количество секунд в единице тарификации. Стоимость в списке цен указывается для единицы тарификации. Обычно единицей тарификации служит минута и, следовательно, в данном поле необходимо указывать значение 60 секунд.

В разделе «Редактор цен» можно указать стоимость звонков с учётом времени суток и направления.

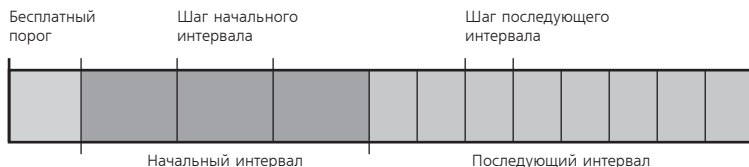
После этого можно добавлять в систему пользователей и подключать им созданную услугу «Телефония». При подключении необходимо указать, какие телефонные номера будут использоваться данным пользователем, а также логин и пароль для авторизации на гейткипере.



Механизм тарификации

Последовательность шагов при проведении тарификации телефонного звонка:

1. Определение направления/зоны.
2. Определение временного диапазона и стоимости единицы тарификации (обычно это минута и она равна 60 секундам).
3. Отсечение бесплатного времени от звонка. Как правило, это 5 секунд в начале разговора. Затем определение шага округления. Стоимость будет вычисляться за вызов с учётом округления.



4. Определение стоимости звонка с учетом данных полученных на предыдущих шагах, а так же с учетом предоплаченных единиц.

Предоплаченные единицы задаются в разделе «Редактирование стоимости» -> «Границы». В поле «Граница» задается количество секунд, после которых начинает действовать указан

ный коэффициент. Количество секунд вычисляется как сумма потребленных услуг с начала расчетного периода по данному направлению. Стоимость вычисляется как значение, указанное в поле «Стоимость» умноженное на «Коэффициент».

5. Проведение списания с лицевого счета за звонок и запись в базу данных информации о звонке (длительность, стоимость, номера вызываемого и вызывающего абонента, идентификатор сессии и др.)

Пример 1

Длительность начального периода 60 секунд, шаг округления начального периода 5 секунд, шаг округления последующего периода 1 секунда. Бесплатное время 5 секунд. Размер единицы тарификации равен 60 секундам.

Длительность звонка составляет 42 секунды при стоимости 0.1 условных единиц за единицу тарификации в данное время суток по данному направлению.

Стоимость звонка будет вычислена по следующему алгоритму

1. Вычитание бесплатного порога в 5 секунд. Для тарификации остается $42 - 5 = 37$ секунд.

2. Определение шага округления. В данном случае 37 секунд попадают в начальный шаг, поэтому округление ведется до полных 5 секунд. Следовательно, после округления стоимость будет вычисляться для 40 секунд.

3. Вычисление стоимости звонка по формуле $0.1 * 40 / 60 = 0,0667$ условных единиц.

Пример 2

Длительность начального периода 60 секунд, шаг округления начального периода 60 секунд, шаг округления последующего периода 1 секунда. Бесплатное время 0 секунд. Размер единицы тарификации равен 60 секундам.

Длительность звонка составляет 42 секунды при стоимости 0.1 условных единиц за единицу тарификации в данное время суток по данному направлению.

Стоимость звонка будет вычислена по следующему алгоритму

1. Вычитание бесплатного порога в 0 секунд. Для тарификации остается $42 - 0 = 42$ секунд.
2. Определение шага округления. В данном случае 42 секунд попадают в начальный шаг, поэтому округление ведется до полных 60 секунд. Следовательно, после округления стоимость будет вычисляться для 60 секунд.
3. Вычисление стоимости звонка по формуле $0.1 * 60 / 60 = 0,1$ условных единиц.

Настройка сервера RADIUS

Необходимо запустить сервер NetUP RADIUS. Затем указать корректные параметры для сервера доступа (NAS), в качестве которого выступает гейткипер на localhost (если UTM и гейткипер находятся на одном сервере).

Пример

Идентификатор сервера доступа (NAS ID): localhost

Секретное слово для авторизации (Auth secret): secret

Секретное слово для учета (Acct secret): secret

В результате сервер RADIUS будет авторизовать пользователей при звонках в обе стороны.

Настройка сервера tftp

Загрузить сервер tftp можно по адресу `ftp://ftp.kernel.org/pub/software/network/tftp/tftp-hpa-0.34.tar.bz2`.

Далее необходимо его установить командами:

```
tar xvfj tftp-hpa-0.34.tar.bz2
cd tftp-hpa-0.34
./configure
gmake
gmake install
```

Создайте директорию, где будут находиться файлы, доступные по tftp.

```
mkdir /netup/tftp
```

Произведите запуск сервера tftp командой

```
/usr/sbin/in.tftpd -l -s /netup/tftp
```

Для автоматического запуска сервера tftp при загрузке операционной системы нужно добавить данную команду в файл `/etc/rc.local`.

Настройка шлюза VOIP при дебетной (карточной) системе оплаты

Необходимо указать, расположение TCL-скрипта для обработки системы голосовых сообщений (IVR), расположение голосовых файлов и длину номера и пин-кода карты.

```
!
call application voice debit tftp://10.1.2.2/
debitcard.1.1.3.tcl
call application voice debit uid-len 4
call application voice debit pin-len 6
call application voice debit language 1 en
call application voice debit set-location en 0
tftp://10.1.2.2/prompts/en/
!
```

Введённые пользователем при авторизации первые четыре цифры (`uid-len`) будут использоваться, как логин, а последующие шесть цифр (`pin-len`) – как пароль.

Если скрипт загрузился успешно, то по команде

```
sh call application voice debit
```

можно увидеть содержание файла скрипта.

В настройках `dial-peer` нужно указать использование этого скрипта:

```
!
dial-peer voice 2 voip
    application debit
!
```

Необходимо задать параметры `aaa`:

```
!
aaa authentication login h323 group radius
```

```

aaa authorization exec h323 group radius
aaa accounting connection h323 start-stop group ra-
dus
!
!
gw-accounting aaa
!
radius-server vsa send accounting
radius-server vsa send authentication
!

```

В результате таких настроек шлюз VoIP будет запрашивать номер (номер и пин-код) карты, затем проводить авторизацию по протоколу RADIUS. При успешной авторизации сервер RADIUS в VSA-атрибутах (h323-credit-amount/h323-currency) отправляет текущий баланс пользователя и код валюты. Затем шлюз запрашивает направление звонка и после ввода заново проводит авторизацию через сервер RADIUS. При этом сервер отправляет количество секунд (атрибут h323-credit-time), доступных для разговора по данному направлению. Если всё прошло успешно, то производится попытка установить соединение согласно настройкам.

По окончании разговора шлюз отправляет серверу RADIUS пакет Accounting STOP с указанием времени разговора.

Совместная работа Alterteks ProxySoftSwitch и UTM

Выдержка с сайта <http://www.alterteks.ru>:

«Alterteks Proxy SoftSwitch (AlterPSS) - это программный переключатель (или коммутатор), позволяющий направлять сигналы и голосовой трафик с одного шлюза IP-телефонии на другой, или пропускать данные через себя (проксировать). При этом управляющие сигналы могут исправляться или полностью изменяться софт-свичом. Таким образом, появляется возможность установки соединения между оборудованием, использующим несовместимые протоколы...»

Настройка ProxySoftSwitch

Предполагается компьютер с операционной системой Windows 2000 или Windows Server 2003 и установленный ProxySoftSwitch.

1. Скопируйте приведённый ниже конфигурационный файл `monitor.ini` в каталог PSS (обычно `C:\Program Files\Alterteks\Proxy Softswitch`). Обратите внимание на переводы строк, строки с русскими комментариями должны начинаться с символа «;».

; Данный файл содержит дополнительные настройки,

; наличие этих настроек позволяет включать вспомогательные сервисы,

; а отсутствие этих настроек не приведет к потере работоспособности AlterPSS

[IVR]

; Префикс телефонных номеров для работы с интерактивным голосовым меню,

; может принимать значения: 'no', 'all' или строка цифр.

; PhoneNumber=no

PhoneNumber=000

[MONITOR]

; Через этот порт с помощью telnet можно просматривать H323 обмен между AlterPss и удаленным шлюзом

Port=5099

; Список AccessIPAddrN позволит ограничить доступ к этому сервису,

; при отсутствии хотя бы одной записи доступ неограничен

AccessIPAddr1=127.0.0.1

[WEB]

; Через этот порт доступна WEB-страница с информацией о текущих соединениях

Port=801

; Список AccessIPAddrN позволит ограничить доступ к этому сервису,

; при отсутствии хотя бы одной записи доступ неограничен

;AccessIPAddr1=127.0.0.1

; Доступ к WEB-странице ограничен по логину/паролю

Login=user

Password=123

; Время автоматической перезагрузки WEB-страницы,

; если на изображении WEB-страницы находится указатель »мышки«, то перезагрузка блокируется.

ReloadTime=3000

[RADIUS]

; Настройки NAS для работы по RADIUS

Server=127.0.0.1

Secret=secret

AuthorizationPort=1812

AuthorizationNasPort=1812

AccountingPort=1813

AccountingNasPort=1813

SessionID=34

Setup=0

Access=0

Connect=1

Stop=1

; Получить таблицу маршрутизации от RADIUS сервера.

RouteMode=0

GatewayID=Pss

; при установке этого параметра в "1" при переходе на следующий маршрут

; будет отправляться STOP пакет для оригиналирующего соединения, а затем вновь посылается ложный START.

ReAccountingReroute=0

; Настройки встроенного конференц сервера.

[CONFERENCE]

;Prefix=00

;Amount=2

;MaxChannels=4

;NewMemberWav=gong.wav

;WaitWav=wait.wav

[GATEWAY]

; Включение/выключение режима преобразования кодеков

CodecConversion=1

; В режиме транскодинга использовать для терминирующего шлюза информацию из таблицы шлюзов.

GetCodecFromTable=1

; Правила преобразования номера к формату E.164 в режиме IVR.

;InternationalAccessCode=810

;AreaAccessCode=8

```
;CountryCode=7
```

```
;AreaCode=095
```

```
[DYNDNS]
```

```
; Время обновления ip-адресов шлюзов согласно их DNS  
(в миллисекундах).
```

```
PollingTime=1000
```

```
[ROUTE]
```

```
; Список кодов завершения, по которым прекращается  
перебор маршрутов.
```

```
CauseStop1=17
```

```
[CAUSE]
```

```
; Подмена кодов завершения.
```

```
;3=17
```

Параметр `Server` определяет IP-адрес компьютера, на котором запущен сервер RADIUS `utm5_radius`. Через этот сервер будут проходить все запросы авторизации (authorization) и учёта (accounting) голосовых звонков. Соответственно, необходимо настроить параметры `AuthorizationPort`, `AccountingPort`.

Параметры `Setup`, `Access`, `Connect` и `Stop` определяют, когда необходимо посылать серверу RADIUS пакеты `Accounting`. Правильные значения для биллинговой системы UTM:

```
Setup=0
```

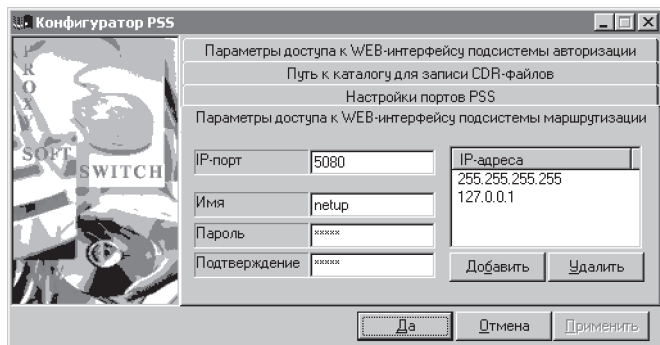
```
Access=0
```

```
Connect=1
```

```
Stop=1
```

Параметр `RouteMode=0` выключает динамическую маршрутизацию и инструктирует ProxySoftSwitch использовать жёстко заданную таблицу маршрутизации (см. ниже).

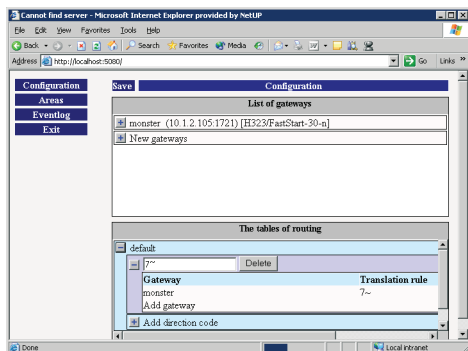
- Запустите конфигуратор PSS (Пуск | Программы | AlterTeks | Proxy Soft Switch | Конфигуратор PSS). Во вкладке «Параметры доступа к web-интерфейсу подсистемы маршрутизации» установите порт, логин и пароль для доступа. Убедитесь, что в правой части окна в списке IP-адресов есть ваш адрес.



- Скачайте модуль авторизации RADIUS по адресу http://netup.ru/dkalinin/pss_utm5_dlls.zip. Необходимо скопировать файлы `PssControl.dll` и `ivr.dll` в каталог PSS (`c:\program files\alterteks\ProxySoftSwitch`).

- Перезапустите службу ProxySoftSwitch. Убедитесь в успешном старте службы.

- Зайдите в систему администрирования подсистемы маршрутизации по адресу <http://localhost:5080>, введите указанный выше пароль.



Настройте один или более шлюзов (gateways). Создайте таблицу маршрутизации (table of routing) с именем default, настройте правила трансляции при различных префиксах.

В примере указано, что все звонки с префиксом «7» (Россия) будут направляться на маршрутизатор с именем monster.

Более подробно процесс конфигурации маршрутизаторов и таблиц роутинга описан в документации по Altermeks ProxySoft-Switch.

Настройка UTM

Необходима версия UTM 5 (любая поддерживаемая платформа) не младше 5.1.9-004.

1. Внесите изменения в конфигурационный файл radius5.cfg (/netup/utm5/radius5.cfg или c:\program files\netup\utm5\radius5.cfg). Добавьте следующие строки:

```
radius_auth_h323_remote_address=enable  
radius_auth_null=enable  
radius_acct_rewrite_login_originate=enable
```

Включенный параметр radius_auth_null дает возможность авторизоваться пользователям, имеющим пустой пароль (при этом не происходит авторизации по одной из схем PAP, CHAP, MSCHAP).

При включении параметра radius_auth_h323_remote_address utm5_radius ведёт себя следующим образом: при приеме от PSS auth-пакета с логином «ip_address» в качестве логина используется значение Cisco Vendor-Specific атрибута h323_remote_address. В итоге авторизация абонентов может производиться по IP-адресу.

При включении параметра radius_acct_rewrite_login_originate сервер RADIUS использует в качестве логина значение h323_remote_address в том случае, если в принятом пакете значение атрибута h323_call_origin равно «originate».

2. Настройте направления и зоны, подключите услугу IP-телефонии.

Настройка Cisco ATA-186

Зайдите браузером на web-интерфейс устройства и установите параметр `GkOrProxy` равным IP-адресу компьютера с PSS. Также укажите номер телефона, логин и пароль для каждого из голосовых портов. Перезагрузите устройство.

Тестовый звонок

Теперь можно пробовать звонить. Наберите номер, начиная с префикса 7 и заканчивая символом «решетка», например, 70955409652#.

Контролируйте лог-файл сервера RADIUS и вывод в web-интерфейсе PSS (ссылка `eventlog`).

После успешного звонка информация о нем появится в отчете по телефонии.

UTM5 Admin Interface int@com.netup.sate://localhost

File Help

Users & Groups | Tarification | Prepared cards | Options | Reports | Additional features | About

General report | Detailed traffic report | Services report | Dialup report | Telephony report | Reseller report | Traffic crash report | Backlogs report | Payments report

Report time range: From 08.10.04 17:00:00 to 08.10.04 23:59:59

Generate Export

Sess.	Acco.	Start	End d.	Call.	Calln.	NAS-	NAS-	User	NAS IP	Status	Inet	Outo	Zone	Direct	Sess.	Total
329	0	08.10.	08.10.	73962	400	0	00000	80.237	2	15520	15880	Unino.	Unino.	11	0	0
331	0	08.10.	08.10.	73962	400	0	00000	80.237	2	14840	14880	Unino.	Unino.	11	0	0
332	0	08.10.	08.10.	73962	400	0	00000	80.237	2	34620	34780	Unino.	Unino.	0	0	0
333	0	08.10.	08.10.	73962	400	0	00000	80.237	2	34880	34880	Unino.	Unino.	0	0	0
334	0	08.10.	08.10.	73962	400	0	00000	80.237	2	67560	67780	Unino.	Unino.	85	0	0
335	0	08.10.	08.10.	73962	400	0	00000	80.237	2	67800	67880	Unino.	Unino.	85	0	0
336	0	08.10.	08.10.	73962	400	0	00000	80.237	2	39500	39740	Unino.	Unino.	0	0	0
337	0	08.10.	08.10.	73962	400	0	00000	80.237	2	39880	39880	Unino.	Unino.	0	0	0

Контрольный пример

Подготовка сервера

Для загрузки базы данных с данными для контрольного примера выполните команды:

```
mysql UTM5 < /netup/utm5/UTM5_tel_kp_clean.sql  
  
mysql -f UTM5 < /netup/utm5/UTM5_MYSQL_update.  
sql > /dev/null 2>&1
```

Запустите RADIUS-сервер и ядро биллинговой системы. Для загрузки тестовых данных из CDR-файла выполните команду:

```
/netup/utm5/bin/utm5_unif -c /netup/utm5/utm5_  
unif_kp.cfg -s /netup/utm5/src.cdr
```

При этом в базу данных будут загружены и протарифицированы телефонные звонки по двум тестовым абонентам в июле месяце 2005 г.

Произведите подключение к ядру интерфейсом администратора.

Контрольные данные

В системе должны присутствовать два тестовых абонента.

Настройки Абонента 1

Закрепленный телефонный номер 5409652

Тарифный план – Тариф1

Настройки Абонента 2

Закрепленный телефонный номер 5409653

Тарифный план – Тариф2

В системе также должны присутствовать телефонные направления и тарифные планы согласно времени суток и дням недели.

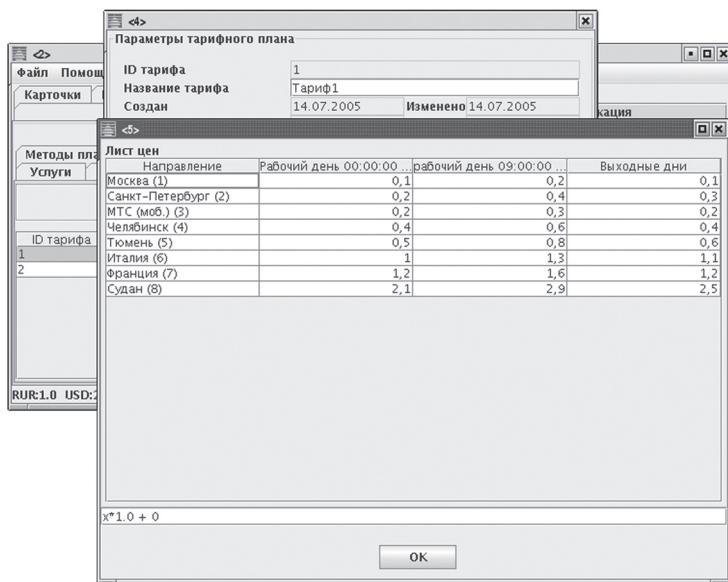


Рис. 1 Тарифный план 1

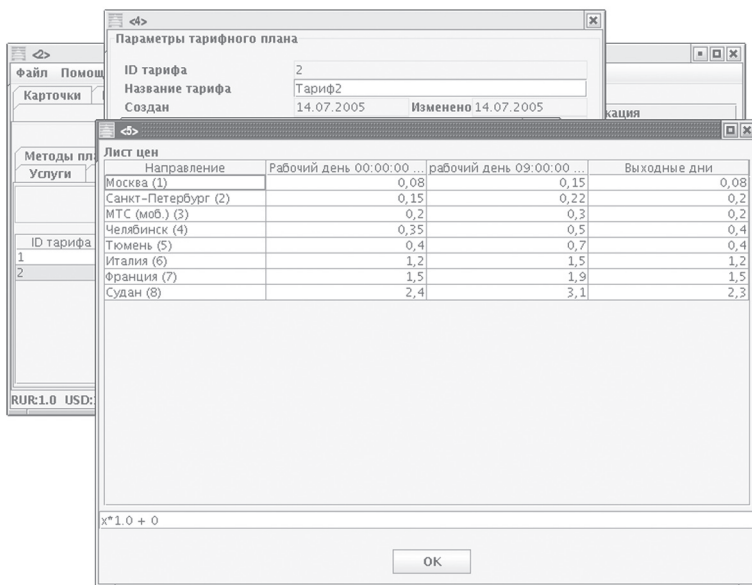


Рис. 2 Тарифный план 2

Табл. 1 Телефонные направления

Зона	Префикс (код)
Москва(1)	7095
Санкт-Петербург (2)	7812
МТС (моб.) (3)	7910, 7915, 7916, 7917
Челябинск (4)	7351
Тюмень (5)	7345
Италия (6)	81039
Франция (7)	81033
Судан (8)	810249

Настройки тарифного плана 1

Бесплатный порог – 5 сек.

Длительность начального периода – 60 сек.

Шаг тарификации начального периода - 10 сек.

Шаг тарификации следующего периода – 1 сек.

Размер единицы тарификацияЯ – 60 сек.

Абонентская плата – 10 у.е.

Стоимость указана в условных единицах

Табл. 2 Стоимость звонков по тарифному плану 1

Зона	Рабочие дни		Выходные дни
	00:00 – 9:00	9:00 – 23:59:59	
Москва(1)	0,1	0,2	0,1
Санкт-Петербург (2)	0,2	0,4	0,3
МТС (моб.) (3)	0,2	0,3	0,2
Челябинск (4)	0,4	0,6	0,4
Тюмень (5)	0,5	0,8	0,6
Италия (6)	1	1,3	1,1
Франция (7)	1,2	1,6	1,2
Судан (8)	2,1	2,9	2,5

Настройки тарифного плана 2

Бесплатный порог – 0 сек.

Длительность начального периода – 60 сек.

Шаг тарификации начального периода - 10 сек.

Шаг тарификации следующего периода – 1 сек.

Абонентская плата – 5 у.е.

Размер единицы тарификации – 60 сек.

Стоимость указана в условных единицах

Табл. 3 Стоимость звонков по тарифному плану 2

Зона	Рабочие дни		Выходные дни
	00:00 – 9:00	9:00 – 23:59:59	
Москва(1)	0,08	0,15	0,08
Санкт-Петербург (2)	0,15	0,22	0,2
МТС (моб.) (3)	0,2	0,3	0,2
Челябинск (4)	0,35	0,5	0,4
Тюмень (5)	0,4	0,7	0,4
Италия (6)	1,2	1,5	1,2
Франция (7)	1,5	1,9	1,5
Судан (8)	2,4	3,1	2,3

Табл. 4 Тестовые телефонные звонки абонента 1

Дата	Зона	Длительность	Длительность, сек	Стоимость за минуту	Стоимость
01.07.05 11:20:00	Санкт-Петербург (2)	00:12:10	730	0,4	4,833
01.07.05 15:55:40	МТС (моб.) (3)	01:10:00	4200	0,3	20,975
01.07.05 21:05:00	Челябинск (4)	00:02:54	174	0,6	1,690
02.07.05 01:25:00	Тюмень (5)	00:12:04	724	0,6	7,190

03.07.05 11:15:00	Италия (6)	00:10:01	601	1,1	10,927
04.07.05 21:53:00	Франция (7)	01:01:54	3714	1,6	98,907
05.07.05 12:13:00	Судан (8)	00:00:24	24	2,9	1,208
06.07.05 01:25:00	Москва(1)	00:01:04	64	0,1	0,098
07.07.05 11:05:20	Франция (7)	02:00:01	7201	1,6	191,893
08.07.05 21:25:00	МТС (моб.) (3)	00:32:05	1925	0,3	9,600
09.07.05 09:55:00	Челябинск (4)	00:12:01	721	0,4	4,773
10.07.05 08:05:00	Челябинск (4)	00:00:09	9	0,4	0,027
11.07.05 04:35:00	Италия (6)	00:22:52	1372	1	22,783
12.07.05 13:10:00	Челябинск (4)	00:01:24	84	0,6	0,790
13.07.05 01:05:00	Судан (8)	00:03:13	193	2,1	6,580
14.07.05 16:03:00	Франция (7)	00:07:00	420	1,6	11,067
15.07.05 18:04:00	Челябинск (4)	00:39:12	2352	0,6	23,470
16.07.05 19:15:00	Италия (6)	00:00:54	54	1,1	1,008
17.07.05 16:35:00	Москва(1)	00:00:23	23	0,1	0,042
18.07.05 14:10:00	Москва(1)	00:22:05	1325	0,2	4,400
19.07.05 23:01:00	Тюмень (5)	00:21:11	1271	0,8	16,880
20.07.05 00:35:00	Санкт-Петер- бург (2)	00:12:01	721	0,2	2,387
21.07.05 00:35:00	Италия (6)	00:00:13	13	1	0,250
22.07.05 10:22:00	Москва(1)	00:01:22	82	0,2	0,257
23.07.05 06:16:00	Санкт-Петер- бург (2)	00:00:03	3	0	0,000
24.07.05 01:14:00	Судан (8)	00:52:05	3125	2,5	130,000
25.07.05 12:19:00	Судан (8)	00:18:19	1099	2,9	52,877

26.07.05 13:45:00	Санкт-Петербург (2)	00:20:21	1221	0,4	8,107
27.07.05 11:05:00	Москва(1)	00:01:10	70	0,2	0,217
28.07.05 15:17:00	Санкт-Петербург (2)	00:02:12	132	0,4	0,847
29.07.05 12:25:00	Москва(1)	00:32:05	1925	0,2	6,400
30.07.05 21:25:00	Италия (6)	00:02:14	134	1,1	2,365
31.07.05 02:00:10	Москва(1)	00:01:25	85	0,1	0,133
				Итого:	642,98

Табл. 4 Тестовые телефонные звонки абонента 2

Дата	Зона	Длительность	Длительность, сек	Стоимость за минуту	Стоимость
01.07.05 04:15:10	Москва(1)	00:00:19	19	0,08	0,019
02.07.05 14:25:30	Франция (7)	00:01:11	71	1,5	1,650
03.07.05 18:11:24	Москва(1)	00:20:34	1234	0,08	1,639
04.07.05 01:21:10	Италия (6)	00:15:39	939	1,2	18,680
05.07.05 07:12:23	Москва(1)	00:00:15	15	0,08	0,020
06.07.05 17:22:13	Санкт-Петербург (2)	00:00:43	43	0,22	0,139
07.07.05 22:45:52	Судан (8)	00:00:18	18	3,1	0,775
08.07.05 09:10:15	Санкт-Петербург (2)	00:00:20	20	0,22	0,055
09.07.05 12:32:16	Москва(1)	00:01:21	81	0,08	0,101
10.07.05 19:11:25	Тюмень (5)	00:05:45	345	0,4	2,267
11.07.05 02:50:38	Италия (6)	00:10:07	607	1,2	12,040
12.07.05 06:00:20	Челябинск (4)	01:15:21	4521	0,35	26,343
13.07.05 13:11:45	Санкт-Петербург (2)	00:01:32	92	0,22	0,319

14.07.05 10:12:28	МТС (моб.) (3)	00:02:45	165	0,3	0,800
15.07.05 15:27:13	Москва(1)	00:00:13	13	0,15	0,038
16.07.05 11:58:22	Москва(1)	00:07:21	441	0,08	0,581
17.07.05 14:17:23	Санкт-Петер- бург (2)	00:16:42	1002	0,2	3,323
18.07.05 20:34:31	Италия (6)	00:32:15	1935	1,5	48,250
19.07.05 11:15:53	Москва(1)	03:15:41	11741	0,15	29,340
20.07.05 17:52:33	Москва(1)	01:10:32	4232	0,15	10,568
21.07.05 19:20:41	Челябинск (4)	00:04:21	261	0,5	2,133
22.07.05 02:16:14	Тюмень (5)	00:09:54	594	0,4	3,927
23.07.05 15:47:22	Италия (6)	00:05:34	334	1,2	6,580
24.07.05 11:17:27	Франция (7)	00:15:55	955	1,5	23,750
25.07.05 22:34:51	Тюмень (5)	00:20:45	1245	0,7	14,467
26.07.05 10:37:21	Москва(1)	01:56:17	6977	0,15	17,430
27.07.05 14:47:29	Москва(1)	00:21:56	1316	0,15	3,278
28.07.05 08:45:23	Санкт-Петер- бург (2)	00:48:12	2892		9,570
29.07.05 11:04:03	Италия (6)	00:12:55	775	1,5	19,250
30.07.05 18:05:11	МТС (моб.) (3)	00:03:51	231	0,2	0,753
31.07.05 23:14:43	Москва(1)	00:08:12	492	0,08	0,649
				Итого:	258,76

ФайлПомощь

Пользователи и группыТарификацияКарточкиНастройкиОтчетыДополнительноО программе

Отчет DialupТелефонияОтчет по дилеруБлокировкиПлатежиОтчет по сгорающим платежамСчета

Основной отчетОтчеты по трафикуГрафические отчетыДетальный отчет по трафикуОтчет по услугам

Отчет за период:

С

S

S

От 01.01.05 0:00 до 31.12.05 23:59

СформироватьЭкспортГрафик

ID	С	О	Дата начала	Д	Вызываемый	Вызвал	ID	Л	NAS IP	Ст	Вх	Исх	Зона	Длительно	Длито	Цена за	Стоимость	П
1	1	01.07.2005	1	0	78127113	5409652	0	17	5	127.0	2	0	О.Санкт-Петербург	720	725.0	4	4.833	0.
1	1	01.07.2005	1	0	78127113	5409652	0	17	5	127.0	2	0	О.Санкт-Петербург	720	725.0	4	4.833	0.
2	1	01.07.2005	1	0	79108122	5409652	0	21	5	127.0	2	0	О.МТС (моб.) (3)	4200	5.0	0	0.0	0.
2	1	01.07.2005	1	0	79108122	5409652	0	21	5	127.0	2	0	О.МТС (моб.) (3)	4200	4195.0	3	20.975	0.
3	1	01.07.2005	2	0	73518294	5409652	0	33	5	127.0	2	0	О.Челябинск (4)	174	5.0	0	0.0	0.
3	1	01.07.2005	2	0	73518294	5409652	0	33	5	127.0	2	0	О.Челябинск (4)	174	1690.6	1	1.690	0.
4	1	02.07.2005	1	0	73456966	5409652	0	1	5	127.0	2	0	О.Тюмень (5)	724	5.0	0	0.0	0.
4	1	02.07.2005	1	0	73456966	5409652	0	1	5	127.0	2	0	О.Тюмень (5)	724	7190.6	7	7.190	0.
5	1	03.07.2005	1	0	81039917	5409652	0	17	5	127.0	2	0	О.Италия (6)	601	5.0	0	0.0	0.
5	1	03.07.2005	1	0	81039917	5409652	0	17	5	127.0	2	0	О.Италия (6)	601	596.1	1	10.927	0.
6	1	04.07.2005	2	0	81033131	5409652	0	33	5	127.0	2	0	О.Франция (7)	3714	5.0	0	0.0	0.
6	1	04.07.2005	2	0	81033131	5409652	0	33	5	127.0	2	0	О.Франция (7)	3714	3709.1	6	98.907	0.
7	1	05.07.2005	1	0	81024925	5409652	0	18	5	127.0	2	0	О.Судан (8)	24	5.0	0	0.0	0.
7	1	05.07.2005	1	0	81024925	5409652	0	18	5	127.0	2	0	О.Судан (8)	24	252.9	1	1.208	0.
8	1	06.07.2005	1	0	70958927	5409652	0	1	5	127.0	2	0	О.Москва (1)	64	5.0	0	0.0	0.
8	1	06.07.2005	1	0	70958927	5409652	0	1	5	127.0	2	0	О.Москва (1)	64	590.1	0	0.098	0.
9	1	07.07.2005	1	0	81033247	5409652	0	17	5	127.0	2	0	О.Франция (7)	7201	5.0	0	0.0	0.
9	1	07.07.2005	1	0	81033247	5409652	0	17	5	127.0	2	0	О.Франция (7)	7201	7196.1	6	191.893	0.
10	1	08.07.2005	2	0	79108839	5409652	0	33	5	127.0	2	0	О.МТС (моб.) (3)	1925	5.0	0	0.0	0.
10	1	08.07.2005	2	0	79108839	5409652	0	33	5	127.0	2	0	О.МТС (моб.) (3)	1925	1920.3	7	9.60	0.
11	1	09.07.2005	9	0	73513115	5409652	0	9	5	127.0	2	0	О.Челябинск (4)	721	5.0	0	0.0	0.
11	1	09.07.2005	9	0	73513115	5409652	0	9	5	127.0	2	0	О.Челябинск (4)	721	716.4	4	4.773	0.
12	1	10.07.2005	8	0	73512759	5409652	0	8	5	127.0	2	0	О.Челябинск (4)	9	5.0	0	0.0	0.
12	1	10.07.2005	8	0	73512759	5409652	0	8	5	127.0	2	0	О.Челябинск (4)	9	5.4	0	0.033	0.
13	1	11.07.2005	4	0	81039993	5409652	0	4	5	127.0	2	0	О.Италия (6)	1372	5.0	0	0.0	0.
13	1	11.07.2005	4	0	81039993	5409652	0	4	5	127.0	2	0	О.Италия (6)	1372	1367.1	0	22.783	0.
14	1	12.07.2005	1	0	73511266	5409652	0	19	5	127.0	2	0	О.Челябинск (4)	84	5.0	0	0.0	0.
14	1	12.07.2005	1	0	73511266	5409652	0	19	5	127.0	2	0	О.Челябинск (4)	84	780.6	0	0.790	0.
15	1	13.07.2005	1	0	81024968	5409652	0	1	5	127.0	2	0	О.Судан (8)	193	5.0	0	0.0	0.
15	1	13.07.2005	1	0	81024968	5409652	0	1	5	127.0	2	0	О.Судан (8)	193	1882.1	6	6.580	0.
16	1	14.07.2005	1	0	81033972	5409652	0	22	5	127.0	2	0	О.Франция (7)	420	5.0	0	0.0	0.
16	1	14.07.2005	1	0	81033972	5409652	0	22	5	127.0	2	0	О.Франция (7)	420	415.1	6	11.067	0.
17	1	15.07.2005	1	0	73516869	5409652	0	24	5	127.0	2	0	О.Челябинск (4)	2352	5.0	0	0.0	0.
17	1	15.07.2005	1	0	73516869	5409652	0	24	5	127.0	2	0	О.Челябинск (4)	2352	2347.6	6	23.470	0.
18	1	16.07.2005	1	0	81039662	5409652	0	25	5	127.0	2	0	О.Италия (6)	54	5.0	0	0.0	0.
18	1	16.07.2005	1	0	81039662	5409652	0	25	5	127.0	2	0	О.Италия (6)	54	55.1	1	1.008	0.
19	1	17.07.2005	1	0	70956812	5409652	0	22	5	127.0	2	0	О.Москва (1)	23	5.0	0	0.0	0.

RURL=0 USD=29.9441 EUR=34.6813Обновить

Время на сервере: 01.08.2005 10:18:50 MS

RUR1.0 USD:29.9441 EUR:34.6813

Обновить

Время на сервере: 01.08.2005 10:18:50 MSD

Рис. 3 Отчет по телефонным звонкам

Акт

Поставщик: ЗАО "Нет"

117419, Москва, Ленинский пр. 2, В2/7

Образец заполнения платежного поручения

Получатель	Сч. #	1654136496
ИНН: 7722165; Net; КПП: 7722001	БИК	044545545
Банк получателя	Сч. #	30101845435435435435
ЗАО "Банк" Москва		

Счет # 1

От 01.08.2005

Платательщик: Абонент1, ИНН

Валюта: 810(RUR) – Russia Rouble, Курс 1.0000

#	Наименование	Цена	Кол-во	Ед.Изм.	Всего
1	Абонентская плата	10.00	1.000		10.00
2	Базовая услуга телефонии	0.00	596.960		642.99

Сумма

652.99

Сумма налогов

0.00

Итого

652.99

Руководитель _____ / И. Иванов

Бухгалтер _____ / С. Сергеев

Действие

OK

Сохранить

Просмотр

Печать

Рис. 4 Счет на оплату для Абонента 1

Рис. 5 Счет на оплату для Абонента 2