

# SMG-1016M

Приложение к руководству по эксплуатации  
Руководство по настройке транкового шлюза SMG-  
1016M для работы с Radius сервером FreeRadius

---

**Цифровой шлюз**

## СОДЕРЖАНИЕ

1. Аннотация.....	3
2. План работ.....	3
3. Настройка Radius сервера FreeRadius .....	3
3.1 Конфигурационные файлы .....	3
3.2 Утилиты.....	5
4. Настройка SMG-1016M .....	5
5. Пример настройки SMG-1016M для работы с Radius-сервером FreeRadius .....	12

## 1. АННОТАЦИЯ

В настоящем руководстве приведена методика по конфигурированию транкового шлюза SMG-1016M и программной модульной системы FreeRadius.

## 2. ПЛАН РАБОТ

- Настройка Radius-сервера FreeRadius;
- Настройка транкового шлюза SMG-1016M;
- Пример взаимодействия.

## 3. НАСТРОЙКА RADIUS СЕРВЕРА FREERADIUS

Конфигурация сервера хранится в каталоге /etc/raddb и представляет собой совокупность файлов, каждый из которых отвечает за определенные настройки сервера.

Список и описание основных файлов конфигурации:

**radiusd.conf** – общая схема файлов конфигурации FreeRadius;

**clients.conf** – описание клиентов сервера;

**proxy.conf** – описание настроек Proxy-сервера и возможных областей перенаправления запроса авторизации;

**acct\_users** – установка биллинговых данных;

**dictionary** – данные об известных AV-парах;

**sql.conf** – настройка работы FreeRadius с MySQL сервером;

**users** – описание пользователей.

### 3.1 КОНФИГУРАЦИОННЫЕ ФАЙЛЫ

#### radius.conf

Файл **radius.conf** описывает основные параметры подключения клиентской части:

- максимальное время обработки запроса сервером, по истечении которого клиенту будет послан пакет с инициализацией разрыва соединения:

```
max_request_time = 30 (возможное значение от 5-120с)
```

- максимальное количество соединений для сервера (рассчитывается умножением числа 256 на возможное число клиентов, то есть для 4-х клиентов значение атрибута 1024);

```
max_request = 1024 (возможное число клиентов ограничено 256)
```

- в разделе listen {...} данного конфигурационного файла указываются порты для авторизации и аккаунтинга клиентской части на сервере.

```
Type=auth/acct
```

```
Port=<значение> (по дефолту для авторизации 1812, для аккаунтинга 1813)
```

## clients.conf

Файл **clients.conf** описывает возможных клиентов (NAS) RADIUS-сервера.

Формат описания клиентов:

```
client <имя_или_ip_адрес> и далее список AV пар для данного клиента, заключённый в фигурные скобки{..}
```

Пример:

```
client 192.168.0.170 {
    secret = smg
}
```

## users

Файл **users** хранит данные о пользователях.

Формат файла:

```
< user_name >          <AV-пара>
                        <AV-пара>
                        ....
                        <AV-пара>
```

Указывается без отступа имя пользователя, затем с отступом в табуляцию идут AV-пары (первой парой указывается пароль). AV-пары должны описываться в файле словаря dictionary. Существует также специальный пользователь, который имеет специальное имя DEFAULT.

Примеры:

1. Пакет на авторизацию от пользователя с именем lameuser будет отброшен, в ответном пакете Access-Reject будет указана причина *«Недостаточно средств для звонка»*:

```
lameuser  Auth-Type := Reject
          Reply-Message = "Недостаточно средств для звонка"
```

2. Пакет на авторизацию от пользователя с именем jonny будет принят без пароля, в ответ будет послан пакет Access-Accept:

```
jonny  Auth-Type := Accept
```

3. Пакет на авторизацию от пользователя с именем 59113 будет принят, произведена проверка по паролю 59113, в ответе Access-Accept (в случае успешной авторизации) будут отправлены атрибуты ограничения разговорной сессии Session-Timeout=30 с и h323-credit-time=15 с., если какой-либо из данных параметров используется на RADIUS-профиле шлюза, то по истечении указанного времени шлюз разорвет разговорное соединение:

```
59113  Cleartext-Password := "59113"
       Login-IP-Host = 0.0.0.0,
       Session-Timeout := 30,
       h323-credit-time := 15
```

## 3.2 УТИЛИТЫ

### radtest

Для проверки корректности настроенных данных на FreeRadius можно воспользоваться утилитой radtest.

Формат:

```
radtest user_name password radius_server nas_port secret
```

Пример:

```
root@jenek# radtest test test 127.0.0.1 0 test
Sending Access-Request of id 80 to 127.0.0.1:1812
  User-Name = "test"
  User-Password = "test"
  NAS-IP-Address = 127.0.0.1
  NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=80, length=108
  Session-Timeout = 722541
  Framed-IP-Address = 192.168.0.15
  Framed-IP-Netmask = 255.255.255.0
```

Также сервер можно запускать с опцией отладки, ключ `-x`

Пример:

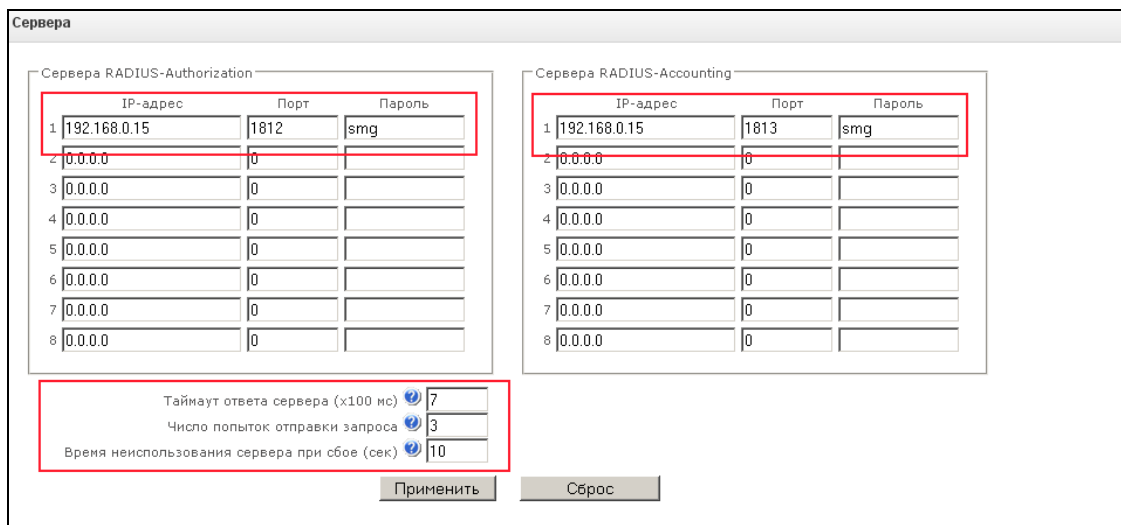
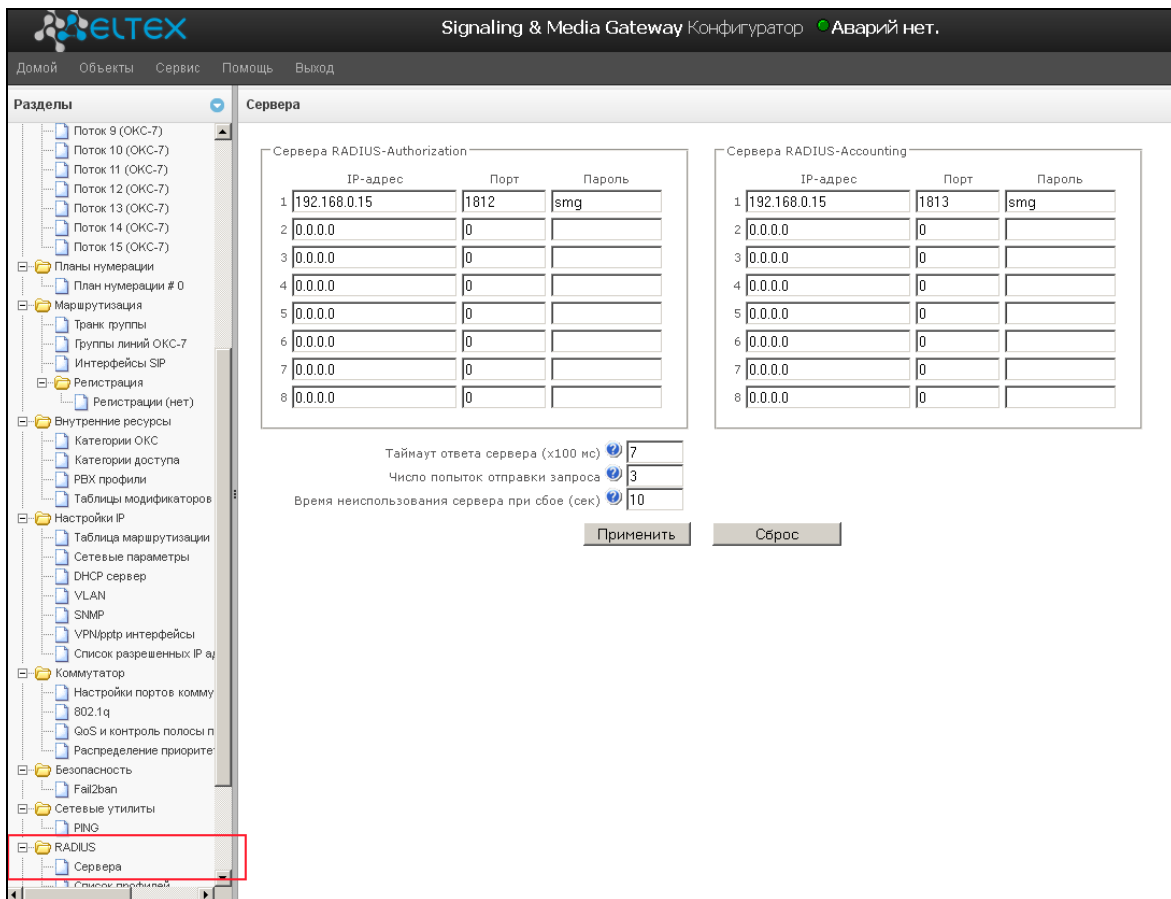
```
./radiusd -x
```

## 4. НАСТРОЙКА SMG-1016M

В разделе **«Radius/Сервера»** настраивается IP-адрес RADIUS-сервера, порты для авторизации (1812) и аккаунтинга (1813), а также пароли для доступа к RADIUS-серверу.

Параметры **«IP-адрес»** и **«Пароль»** должны совпадать с IP-адресом и паролем в настройках раздела *clients.conf* сервера FreeRadius.

В разделе **«Radius/Сервера»** помимо адреса основного RADIUS-сервера возможно задать до 7 резервных в случае отказа работы основного. Переход на адреса резервных серверов осуществляется по истечении параметров **«Таймаут ответа сервера»** и **«Число попыток отправки запроса»** при указанном таймауте.



Для конфигурирования авторизационных параметров через CLI необходимо выполнить команды:

```
SMG1016> config
Entering configuration mode.
SMG1016-[CONFIG]> radius
Entering RADIUS mode.
SMG1016-[CONFIG]-RADIUS> auth

ipaddr set auth server ipaddr
port set auth server port
secret set auth server secret key
```

Для конфигурирования параметров аккаунтинга через CLI необходимо выполнить команды:

```
SMG1016> config
Entering configuration mode.
SMG1016-[CONFIG]> radius
Entering RADIUS mode.
SMG1016-[CONFIG]-RADIUS> acct
ipaddr set acct server ipaddr
port set acct server port
secret set acct server secret
```

В разделе «*Radius/Список профилей*» создаются RADIUS-профили и производится конфигурирование параметров взаимодействия с RADIUS-сервером.

The screenshot shows the 'Signaling & Media Gateway Конфигуратор' interface. The left sidebar contains a tree view of configuration sections, with 'Список профилей' (Profiles List) highlighted in red. The main area displays the configuration for a profile named 'RADIUS\_Profile00'. The configuration includes:

- Profile name: RADIUS\_Profile00 [имя профиля]
- Use RADIUS-Authentication:
- Use RADIUS-Accounting:
- Parameters for RADIUS-Authentication:
  - Send requests:  при входящем занятии,  при конце набора
  - Limit outgoing connections:  нет ограничений,  только местная и зонавая сети,  только местная сеть,  только спецслужбы,  все запрещено (разрыв соединения)
- Parameters for RADIUS-Accounting:
  - Send requests:  accounting-start,  accounting-stop,  accounting-stop для неуспешных вызовов,  accounting-update с периодом 2 минуты,  accounting для call-origin=answer
  - Limit outgoing connections:  нет ограничений,  только местная и зонавая сети,  только местная сеть,  только спецслужбы,  все запрещено (разрыв соединения)
- Parameters for PortaBilling:
  - Use PortaBilling:
  - Use PortaRouting:
- Other fields: CgPN, password, RFC4590, Не учитывать, Async, Not used, Not used, and various modifier dropdowns (InCdPN, InCgPN, OutCdPN, OutCgPN).

Buttons for 'Применить' (Apply) and 'Сброс данных' (Reset) are visible at the bottom.

**Список профилей**

RADIUS\_Profile00 [имя профиля]

Использовать RADIUS-Authorization  
 Использовать RADIUS-Accounting

**Параметры RADIUS-Authorization**

Отправлять запросы

при входящем занятии  
 при конце набора

Ограничения исходящей связи при сбое сервера

нет ограничений  
 только местная и зонавая сети  
 только местная сеть  
 только спецслужбы  
 все запрещено (разрыв соединения)

CgPN  Поле User-name  
password  Поле User-password

Индивидуальные пароли для SIP-абонентов  
RFC4590  DIGEST авторизация  
 Не учитывать  Вреня сессии

Разрешить доступ к спецслужбам при получении отказа в соединении от сервера

Async  NAS-Port-Type  
Not used  Service-Type  
Not used  Framed-protocol

Модификаторы InCdPN  
 Модификаторы InCgPN  
 Модификаторы OutCdPN  
 Модификаторы OutCgPN

**Параметры RADIUS-Accounting**

Отправлять запросы

accounting-start  
 accounting-stop  
 accounting-stop для неуспешных вызовов  
 accounting-update с периодом  минуты  
 accounting для call-origin=answer

Ограничения исходящей связи при сбое сервера

нет ограничений  
 только местная и зонавая сети  
 только местная сеть  
 только спецслужбы  
 все запрещено (разрыв соединения)

CgPN  Поле User-name  
CdPN-in  Поле CdPN  
CgPN-in  Поле CgPN

**Параметры PortaBilling**

Использовать PortaBilling  
 Использовать PortaRouting

Описание и назначение всех параметров приведено в руководстве по эксплуатации шлюза (<http://www.eltex.nsk.ru/download?sgrp=563&grp=211&id=434>).

Для конфигурирования параметров RADIUS-профиля через CLI необходимо выполнить следующие команды:

```
SMG1016> config
Entering configuration mode.
SMG1016-[CONFIG]> radius
Entering RADIUS mode.
SMG1016-[CONFIG]-RADIUS> profile 0
Entering RADIUS-Profile-mode.
SMG1016-[CONFIG]-RADIUS-PROFILE[0]>

acct    set acct parameters
auth    set auth parameters
config  Back to configuration mode
exit    Go back to Config-view
modifiers Set modifiers table for RADIUS
quit    Exit this CLI session
show    show RADIUS Profile info
use     set auth/acct usage flag
```



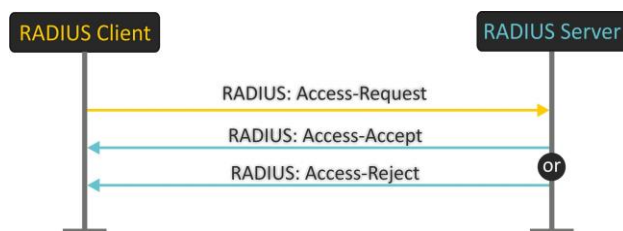
Стоит учесть, что использование RADIUS-профиля назначается на транковой группе для входящей связи. Возможные варианты взаимодействия:

### 1. Входящая связь от TDM-абонентов

Необходимо создать Radius-профиль, выбрать «Использовать *Radius-authorization* в настройках профиля, заполнить поле “user-password” паролем, указанным в настройках пользователей (файл *user* в FreeRadius).

Созданный профиль с настроенными параметрами необходимо присвоить входящей транковой группе на потоке, с которого поступают вызова на SMG-1016M.

При входящем вызове по потоку на указанный адрес RADIUS-сервера будет послан запрос Access-Request, где в качестве имени пользователя *User-Name* будет указан номер А (calling) входящего вызова, в качестве пароля *Password* – настроенное значение пароля в конфигурации Radius-профиля.



Пример:

```
----- RADIUS. Accs-Request [000] -----
User-Name           = '55555'
Password            = 'Eltex777'
Calling-Station-Id = '55555'
Called-Station-Id  = '123456789'
NAS-Port-Id        = '67109376'
NAS-Port-Type      = 'Async'
Acct-Session-Id    = '04000200 3a844407 04000200 3a844407'
h323-conf-id       = '04000200 3a844407 04000200 3a844407'
Cisco-AVPair       = 'xpgk-request-type=number'
Cisco-AVPair       = 'xpgk-src-number-in=55555'
Cisco-AVPair       = 'xpgk-dst-number-in=123456789'
NAS-IP-Address     = '192.168.0.10'
Cisco-AVPair       = 'h323-gw-address=192.168.0.10'
h323-gw-id         = '192.168.0.10'
```

## 2. Входящая связь от SIP-интерфейса

Аналогично вызову от TDM-абонента, создается RADIUS-профиль, который назначается на входящую транковую группу. В качестве «*User Name*» используется номер из параметра *from* входящего запроса INVITE, в качестве пароля «*Password*» настроенное значение пароля в конфигурации RADIUS-профиля:

```
----- RADIUS. Accs-Request [002] -----
User-Name           = '001'
Password            = 'password'
Calling-Station-Id = '001'
NAS-Port-Id        = '285213694'
NAS-Port-Type      = 'Async'
Acct-Session-Id    = '110003fe 38704d10 110003fe 38704d10'
h323-conf-id       = '110003fe 38704d10 110003fe 38704d10'
Cisco-AVPair       = 'xpgk-request-type=number'
Cisco-AVPair       = 'xpgk-src-number-in=001'
NAS-IP-Address     = '192.168.0.10'
Cisco-AVPair       = 'h323-gw-address=192.168.0.10'
h323-gw-id         = '192.168.0.10'
```

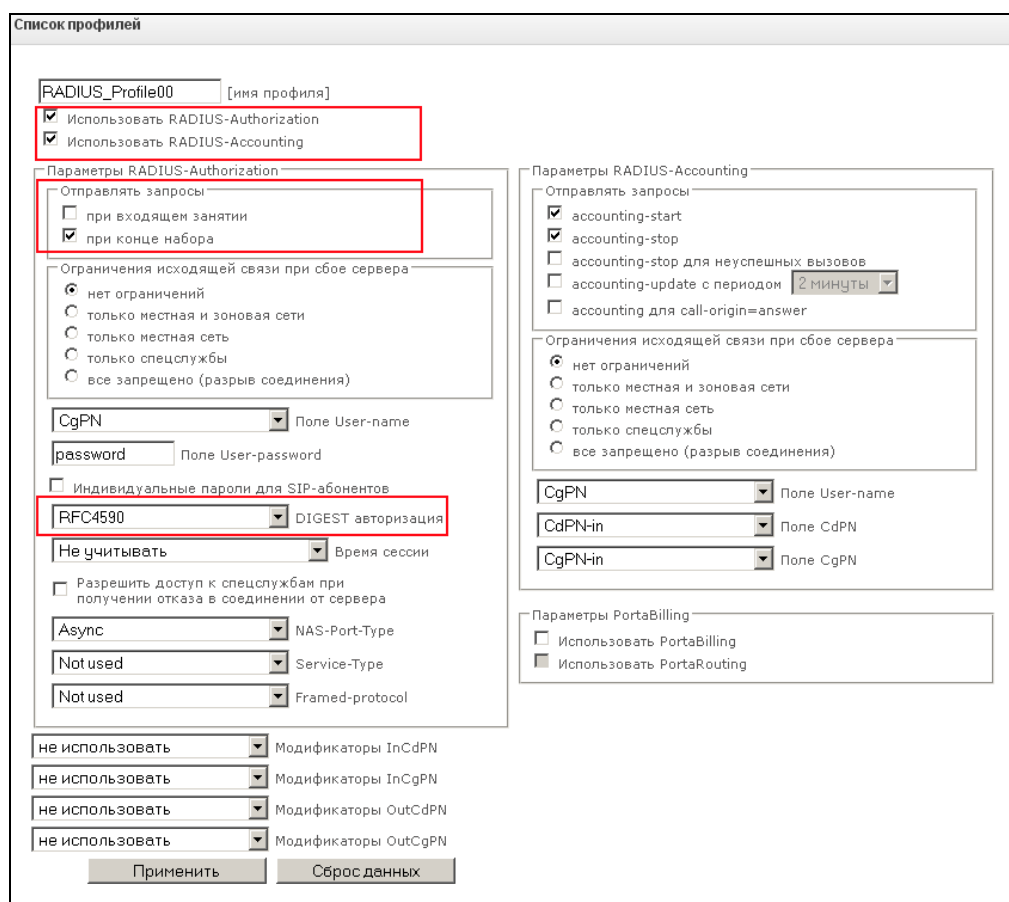
### 3. Входящая связь от SIP-абонента

На SMG-1016M возможно использование двух типов SIP абонентов – статического и динамического.

Для статического абонента указывается номер и по необходимости –IP адреса источника (для ограничения несанкционированного доступа к SMG-1016M).

Для динамического абонента создается только запись, зарегистрироваться под этой записью может любой пользователь, прошедший аутентификацию на RADIUS-сервере.

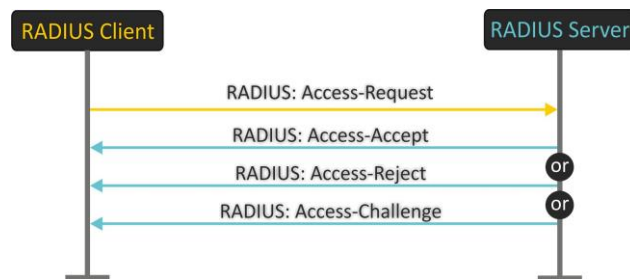
При аутентификации на RADIUS-сервере возможно использование двух основных методов (настройка производится в Radius профиле в разделе “ **DIGEST авторизация** ”) – По рекомендации RFC4590 и по варианту без ожидания пакета challenge от Radius сервера.



При использовании варианта RFC4590 на запрос регистрации/установления соединения шлюз SMG-1016M передает пакет Access-Request в сторону RADIUS-сервера, ожидая в ответ пакет Access-Challenge/Access-Accept/Access-Reject. При получении пакета Access-Challenge, то есть запроса авторизации со стороны Radius сервера, транковый шлюз SMG-1016M запрашивает параметры авторизации у абонента (ответ SIP 401 Unauthorized) и, получив необходимые данные, повторяет авторизованный запрос на сервер, включая в пакет Access-Request пароль.

Используя алгоритм RFC4590-no-challenge при попытке регистрации/установления соединения, шлюз SMG-1016M предварительно (ответ SIP 401 Unauthorized) запросит параметры

авторизации у абонента и после их получения отправит на RADIUS сервер авторизованный запрос Access-Request.



## 5. ПРИМЕР НАСТРОЙКИ SMG-1016M ДЛЯ РАБОТЫ С RADIUS-СЕРВЕРОМ FREERADIUS

### Условия задачи

Необходимо зарегистрировать на SMG-1016M (IP-адрес 192.168.0.10) абонента с номером 22222, логин и пароль для абонента: login – 22222, password – 22222 с аутентификацией на сервере FreeRadius (IP-адрес 192.168.0.175). Помимо этого совершить успешный вызов на абонента с номером 33333, аутентификационные данные второго абонента: login – 33333 , password – 33333, ограничить время разговорной сессии между абонентами через атрибут Session-time в 30 с. Для взаимодействия с RADIUS-сервером использовать пароль – password.

### Решение

1. Создать в настройках RADIUS-сервера описание клиента SMG-1016M с IP = **192.168.0.10** и паролем **smg**. Для этого в файле **clients.conf** добавить запись следующего вида:

```
client 192.168.0.10 {
  secret = smg
}
```

2. Настроить RADIUS- серверы на SMG-1016M: установить IP-адреса, порты для аутентификации и аккаунтинга, пароль как показано на рисунке ниже:

Сервера RADIUS-Authorization			
№	IP-адрес	Порт	Пароль
1	192.168.0.175	1812	smg
2	0.0.0.0	0	
3	0.0.0.0	0	
4	0.0.0.0	0	
5	0.0.0.0	0	
6	0.0.0.0	0	
7	0.0.0.0	0	
8	0.0.0.0	0	

Сервера RADIUS-Accounting			
№	IP-адрес	Порт	Пароль
1	192.168.0.175	1813	smg
2	0.0.0.0	0	
3	0.0.0.0	0	
4	0.0.0.0	0	
5	0.0.0.0	0	
6	0.0.0.0	0	
7	0.0.0.0	0	
8	0.0.0.0	0	

Таймаут ответа сервера (x100 мс)

Число попыток отправки запроса

Время неиспользования сервера при сбое (сек)

3. Создать на RADIUS-сервере описание пользователей с номерами 22222 и 33333. Для этого в файл **users** добавить следующие записи:

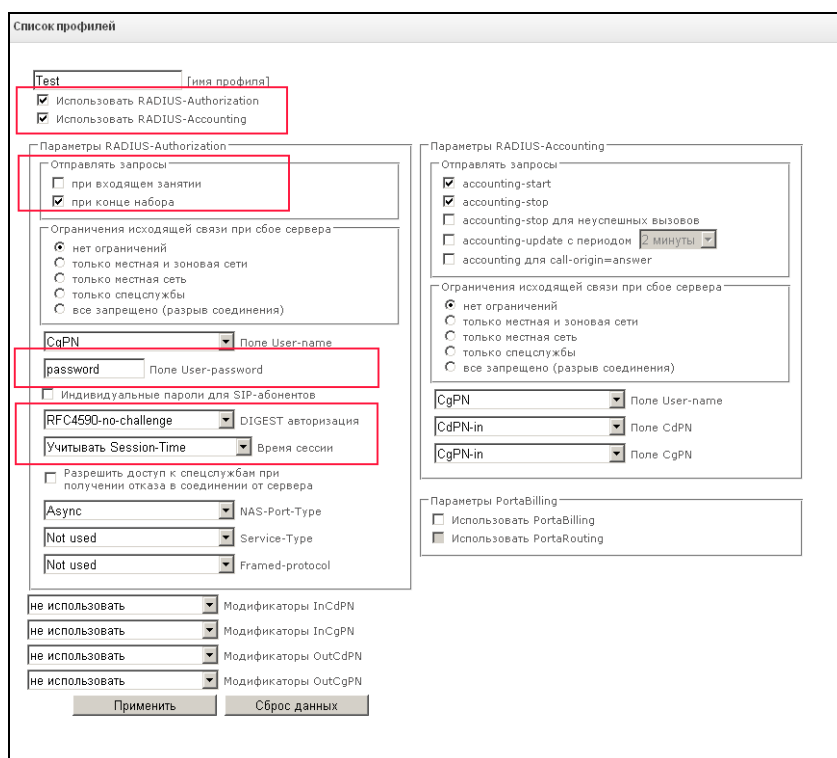
```

22222 Cleartext-Password := "password"
      Session-Timeout := 30,
      Reply-Message = "call from 22222 accepted"

33333 Cleartext-Password := "password"
      Session-Timeout := 30,
      Reply-Message = "call from 33333 accepted"
    
```

Параметр Session-Timeout предназначен для ограничения разговорной сессии. Необходимо сконфигурировать его для обоих абонентов, чтобы любой из них мог стать инициатором разговорной сессии, ограниченной в 30 с.

4. Создаем Radius профиль на SMG-1016M для взаимодействия с RADIUS-сервером



Указать в настройках использование Radius-Authorization и Radius-Accounting, настроить метод передачи запроса авторизации на RADIUS-сервер – «при входящем занятии» или «при конце набора».

Сконфигурировать параметр «Время сессии» – «учитывать Session-Time».

5. В разделе «SIP-абоненты» на SMG-1016M создать двух абонентов:

**SIP-абоненты**

Индекс [ 0 ]  
 Тип [ SIP абонент ]  
 Число абонентов [ 1 ]  
 Начальное название [ Subscriber#000 ]  
 Динамическая регистрация   
 Начальный номер [ 22222 ]  
 Начальный номер АОН [ ]  
 Тип номера АОН [ Subscriber ]  
 Категория АОН [ 1 ]  
 Количество линий [ 0 ]  
 IP адрес [ 0.0.0.0 ]  
 SIP-домен [ ]  
 SIP-профиль [ [1] SIP-interface01 ]  
 PBX-профиль [ [0] PBXprofile#0 ]  
 Категория доступа [ [0] AccessCat#0 ]  
 План нумерации [ [0] NumberPlan#0 ]  
 Авторизация [ With Register ]  
 Логин [ 22222 ]  
 Пароль [ 22222 ]  
 Разрешить переадресацию (302)   
 Разрешить обработку сообщений REFER   
 Режим обслуживания абонента [ Включен ]  
 Голосовая почта [ нет ]  
 Таймаут неответа для перехода на голосовую почту (сек) [ 20 ]

Применить Отменить

Аналогично создать запись для абонента с номером 33333.

В настройках SIP-профиля для абонентов назначить созданный RADIUS-профиль.

**Интерфейсы SIP**

Индекс [ 1 ]  
 Тип [ Интерфейсы SIP ]  
 Название [ SIP-interface01 ]  
 Режим [ SIP-Профиль ]  
 Профиль RADIUS [ [0] Test ]

Кодеки


Вкл.	Кодек	PType	PTE
<input checked="" type="checkbox"/>	G.711A	8	30
<input checked="" type="checkbox"/>	G.711U	0	30
<input type="checkbox"/>	G.729	18	30
<input type="checkbox"/>	G.723.1 (5.3 kbps)	4	30
<input type="checkbox"/>	G.723.1 (6.3 kbps)	4	30
<input type="checkbox"/>	G.726-32	102	30

Детектор активности речи / Генератор комфортного шума (VAD/CNG)   
 Контроль IP:Port источника RTP   
 Эхокомпенсация [ off ]  
 Усиление сигнала на приеме (0.1 dB) [ 0 ]  
 Усиление сигнала на передаче (0.1 dB) [ 0 ]  
 Активных соединений [ 0 ]  
 DSCP для RTP [ 0 ]  
 DSCP для SIP [ 0 ]  
 Период передачи пакетов RTCP (с) [ 0 ]  
 Контроль активности сессии по протоколу RTCP   
 Контроль доступности встречной стороны сообщениями OPTIONS

## Пример успешного установления соединения

Пример успешного установления соединения по протоколу RADIUS между транковым шлюзом SMG-1016M и FreeRadius:

1. Регистрация абонентов на SMG-1016M. В случае успешной регистрации в мониторинге состояние абонентов будет отображено зеленым цветом индикатора («Регистрация активна»).

№	Состояние	Название	Номер	SIP домен	IP:Port	Последняя регистрация	Регистрация истекает
1	 Регистрация активна	Subscriber#000	22222	192.168.0.10	192.168.0.200:8006	04:49:56 15:01:2000	00:08:06

2. При вызове от одного абонента к другому на RADIUS-сервер будет отправлен запрос авторизации вызова Access-Request:

```
----- RADIUS. Accts-Request [002] -----
User-Name           = '22222'
Password            = '22222'
Calling-Station-Id  = '22222'
Called-Station-Id   = '33333'
NAS-Port-Id         = '285213694'
NAS-Port-Type       = 'Async'
Acct-Session-Id     = '110003fe 387fab35 110003fe 387fab35'
h323-conf-id        = '110003fe 387fab35 110003fe 387fab35'
Cisco-AVPair        = 'xpgk-request-type=number'
Cisco-AVPair        = 'xpgk-src-number-in=22222'
Cisco-AVPair        = 'xpgk-dst-number-in=33333'
NAS-IP-Address      = '192.168.0.10'
Cisco-AVPair        = 'h323-gw-address=192.168.0.10'
h323-gw-id          = '192.168.0.10'
```

3. В ответ на запрос сервер, обнаружив запись для абонента и сравнив значение атрибута *Password* в Access-Request с параметром *Cleartext-Password*, ответит либо разрешением на установление соединения - *Accept*, либо отказом – *Reject*. В данном случае появится сообщение *Accept*:

```
----- RADIUS. Accts-Reply [001] -----
Accept
Session-Timeout     = '30'
Reply-Message       = 'call from 22222 accepted'
```

4. После того, как абонент с номером 33333 поднимет трубку, в сторону FreeRadius от SMG-1016M будет передан запрос Accounting-Request со значением *start*:

```
----- RADIUS. Acct-Request [003] -----
Acct-Status-Type    = 'Start'
User-Name           = '22222'
Calling-Station-Id  = '22222'
Called-Station-Id   = '33333'
Acct-Session-Id     = '110003fe 387fab35 110003fe 387fab35'
```

```

Event-Timestamp           = '947891000'
NAS-Port-Id               = '285213694'
NAS-Port-Type             = 'Async'
Cisco-NAS-Port            = 'S IPT:03fe'
Cisco-AVPair              = 'xpgk-src-number-in=22222'
Cisco-AVPair              = 'xpgk-src-number-out=22222'
Cisco-AVPair              = 'xpgk-dst-number-in=33333'
Cisco-AVPair              = 'xpgk-dst-number-out=33333'
Cisco-AVPair              = 'xpgk-route-retries=1'
Cisco-AVPair              = 'h323-call-id=110003fe 387fab35 110003fe 387fab35'
h323-remote-address      = '192.168.0.35'
Cisco-AVPair              = 'h323-incoming-conf-id=110003fe 387fab35 110003fe 387fab35'
h323-conf-id              = '110003fe 387fab35 110003fe 387fab35'
h323-setup-time           = '05:03:17.000 GMT+6 Sat Jan 15 2000'
h323-call-origin          = 'originate'
h323-call-type            = 'VoIP'
h323-connect-time         = '05:03:20.000 GMT+6 Sat Jan 15 2000'
Acct-Delay-Time           = '2'
NAS-IP-Address            = '192.168.0.10'
Cisco-AVPair              = 'h323-gw-address=192.168.0.10'
h323-gw-id                = '192.168.0.10'

```

##### 5. Сервер FreeRadius подтвердит запрос:

```
----- RADIUS. Acct-Reply [003] -----
```

6. Поскольку в Access-Reply от сервера был принят параметр *Session-Timeout* = '30', ограничивающий время разговорной сессии в 30 с., то по истечении указанного времени разговор будет прерван, а в сторону RADIUS- сервера будет передан Accounting-Request со значением stop:

```

----- RADIUS. Acct-Request [004] -----
Acct-Status-Type         = 'Stop'
User-Name                 = '22222'
Calling-Station-Id       = '22222'
Called-Station-Id        = '33333'
Acct-Session-Id          = '110003fe 387fab35 110003fe 387fab35'
Event-Timestamp           = '947891003'
NAS-Port-Id               = '285213694'
NAS-Port-Type             = 'Async'
Cisco-NAS-Port            = 'S IPT:03fe'
Cisco-AVPair              = 'xpgk-src-number-in=22222'
Cisco-AVPair              = 'xpgk-src-number-out=22222'
Cisco-AVPair              = 'xpgk-dst-number-in=33333'
Cisco-AVPair              = 'xpgk-dst-number-out=33333'
Cisco-AVPair              = 'xpgk-route-retries=1'
Cisco-AVPair              = 'h323-call-id=110003fe 387fab35 110003fe 387fab35'
h323-remote-address      = '192.168.0.35'
Cisco-AVPair              = 'h323-incoming-conf-id=110003fe 387fab35 110003fe 387fab35'
h323-conf-id              = '110003fe 387fab35 110003fe 387fab35'
h323-setup-time           = '05:03:17.000 GMT+6 Sat Jan 15 2000'
h323-call-origin          = 'originate'
h323-call-type            = 'VoIP'
h323-connect-time         = '05:03:20.000 GMT+6 Sat Jan 15 2000'
h323-disconnect-time      = '05:03:23.000 GMT+6 Sat Jan 15 2000'
h323-disconnect-cause    = '10'
Cisco-AVPair              = 'xpgk-local-disconnect-cause=1'

```



---

```
Acct-Session-Time      = '3'  
Acct-Delay-Time       = '2'  
NAS-IP-Address        = '192.168.0.10'  
Cisco-AVPair          = 'h323-gw-address=192.168.0.10'  
h323-gw-id            = '192.168.0.10'
```

7. Сервер подтвердит запрос:

```
----- RADIUS. Acct-Reply [004] -----
```