JERASOFT

VoIP Carrier Suite

Integration Manual

http://jerasoft.net/

Table of contents

1. Trivia

To be able to collect the calls data from any switch system, you can go two ways: collect the data via the CDR-files or via the RADIUS-server. The differences in these methods are the following:

- CDR-files import
  - **Advantages:** high reliability and stability, no calls information may be lost due to server or client side;
  - **Disadvantages:** the data is received with delays because files are copying at the defined periods of time.
- RADIUS-server
  - **Advantages:** data is received in real-time mode (the call packet is sent right after the end of the call), call authorization procedure is possible, possibility to utilize advanced routing features;
  - **Disadvantages:** when network or server hardware is unstable, the loss of data is possible (although, this data can be restored later with CDR-files).

Of course you can combine both methods, but note that not all switching equipment is capable of supporting both these methods at once. Some gateways support only one integration type (for example, Cisco gateways do not write any CDR files, so integration is possible only through RADIUS).

In this document you will be able to find instructions on how you can integrate your JeraSoft VCS with different kinds of switching equipment, for proper calls billing and processing.

2. VCS Integration Routines

Regardless of switching equipment model or family, JeraSoft VCS is set absolutely identically for any of them. This section describes what you should do with VCS before attempting switch-specific integration. Please note, that all further sections of this document assume that these steps have been performed successfully.

2.1 Integration via CDR-files

First thing you should start from is creating a set of SSH keys, so your VCS would get access to your CDR-files storage (usually it's your switch server). To create SSH keys, please log in to your VCS server and run following set of commands:

```
sudo -u vcs /usr/local/vcs/bin/setup ssh-keys <username>@<hostname>[:<port>]
```

where *username@hostname* is a set of credentials for accessing a CDR-files storage.

Please note: If your VCS solution was installed before October 1st, 2011, then the command set should look like this:

```
sudo -u billbery /usr/local/billbery/ssh_keys.py root@Switch_server_IP
```

Please note: SSH keys are required for SSH access type, if you prefer to use FTP storage, SSH keys are not required.

Next, open your VCS web interface and perform following steps:

1) Go to *Configuration – VoIP Gateways* and click *«Create New»* to create a gateway integration;
2) In gateway's properties, be sure to set following parameters for CDR-files processing:
   - **Gateway Name:** set a name for your gateway (switch);
   - **IP:** specify your gateway (switch or CDR storage) IP address;

– **Files Downloader:** enable the downloader, specify type of protocol you will be using, port, access credentials and path where your files are stored. Please take note, that most common paths to CDR files differ for each switch model or family and usually are following:

  – ***Aloe MVTS:*** /usr/local/mvts/billing/bill*;
  – ***Aloe RTU Class 4 (MVTS PRO):*** /var/cdrs/bill*;
  – ***Aloe RTU Class 5 (IP Centrex):*** /var/cdrs/bill*;
  – ***Aloe Transit SBC:*** /var/cdrs/*;
  – ***Asterisk:*** /var/log/asterisk/cdr-billing/*;
  – ***Genband (Nextone):*** /home/nextone/cdrs/*.CDR;
  – ***Sansay VSXi:*** /cdr/20*;
  – ***Freeswitch:*** /usr/local/freeswitch/log/cdr-csv/Master.csv.2*

– **Files Collector:** enable the collector and specify collector's type respective to your switch model or family. Some switches may also require you to change the *«Overwrite TZ»* option, as those switches do not send the timezone data in CDRs (for example, Aloe MVTS PRO). If this is your case, please set appropriate timezone value;

3) Save settings and go to *System – Task Scheduler* section. Make sure that *Files Collector* and *Files Downloader* processes are enabled, if not – start them.

2.2 Integration via RADIUS/SIP Redirect

For VCS system, RADIUS/SIP Redirect integration procedure is very alike to one you should perform for CDR files. Please log in to your VCS web-interface and perform following steps:

1) Go to *Configuration – VoIP Gateways* and click *«Create New»* to create a gateway integration;
2) In gateway's properties, be sure to set following parameters for CDR-files processing:

  – **Gateway Name:** set a name for your gateway;
  – **IP:** specify your gateway's IP address;

– **SIP Server:** enable the SIP server to utilize SIP Redirect feature (for gateways that support SIP Redirect routing, for example Sansay VSX/VSXi);

– **RADIUS Server:** enable RADIUS Server if you plan to utilize RADIUS features such as prepaid billing, dynamic authorization/authentication or external routing. Do not forget to specify your secret password, collector type respective to your switch model/family and set relevant timezone if your switch does not send this information in RADIUS packets;

3) Save settings and go to *System – Task Scheduler* section. Make sure that *SIP Redirect Server* and *RADIUS Server* are enabled respectively, and if not – start them. If you plan to utilize external routing features of JeraSoft VCS, also make sure that *DynRouting Manager* process is enabled.

3. Aloe MVTS

3.1 Integration via CDR-files

Please define the period in which your CDR files should be created. To do this, open *meraproxy.cfg* file and define *period* parameter in *[Billing]* section (for example, for 1 hour). Also, specify *cdr_format=0* if you have not already done so (make sure that the format value is equal to the chosen collector in VCS). Thus, the *[Billing]* section may look like this:

```
[Billing]
period = 01:00:00
file = ../billing/bill
cdr_format = 0
level = 3
```

3.2 Integration via RADIUS

3.2.1 RADIUS configuration

To allow the correct data collection via RADIUS, do the following:

1) Open the *meraproxy.cfg* file and define next parameters under the *[Radius]* section:

```
[Radius]
q931_h323_disconnect_cause = 1
use_h323_ivr_in = 1
suppress_Q931_cause = 0
local_auth_port = 11812
local_acct_port = 11813
local_route_port = 11814
acct_port = 1813
auth_port = 1812
```

```
route_port = 1812
secret = --change to your secret in VCS--
acct_enable = 1
acct_address = --VCS IP-address--
acct_type = 1
acct_leg_type = 2
acct_stop_only = 0
dst_user_orig_leg=1
auth_enable = 1
auth_address = --VCS IP-address--
route_enable = 1
route_address = --VCS IP-address--
```

2) Open the user.*cfg* file and define next parameters under the *[default]* section:

```
[default]
user = default
acct_enable = 1
auth_enable = 1
proxy_type = 1
```

Please note that this configuration example includes all RADIUS-provided functions: RADIUS Authentication, Authorization, Accounting and External Routing. In regards to routing though, some additional settings have to be added. Please find these settings in next section of this document.

3.2.2 External Routing settings

In addition to provided above RADIUS settings in *meraproxy.cfg,* External Routing requires the following to be present in *gateways.cfg* file:

```
[BILLBERY_GW]
address = 127.0.0.1
gateway_mode = 3
gateway_type = 1
port = 1720
proxy_type = 1
```

```
[BILLBERY_SIP]
address = 127.0.0.2
converter = --your SIP-HIT converter--
gateway_mode = 3
gateway_type = 1
port = 5060
proxy_type = 1

[public_access]
address = 127.0.0.1
mask = 0.0.0.0
```

Also, open *dialpeer.cfg* file, and add the following dial peers:

```
[R_BILLBERY]
dst_pattern = .+
gateway = EXTERNAL
hunt_stop = 1
priority = 100

[R_ENDPOINTS]
dst_pattern = .+
gateway = ENDPOINTS
priority = 200
```

These settings will insure that all your H.323 and SIP customers will be authenticated, authorized and billed via RADIUS, and every destination will be routed externally through VCS routing mechanism.

4. Aloe RTU Class 4 (MVTS Pro)

4.1 Integration via CDR-files

Make sure that /var/cdrs/ directory is created on MVTS PRO server, or create it by using command:

```
mkdir /var/cdrs
```

Make sure this folder access rights are 02775, or assign them manually with command:

```
chmod 02775 /var/cdrs
```

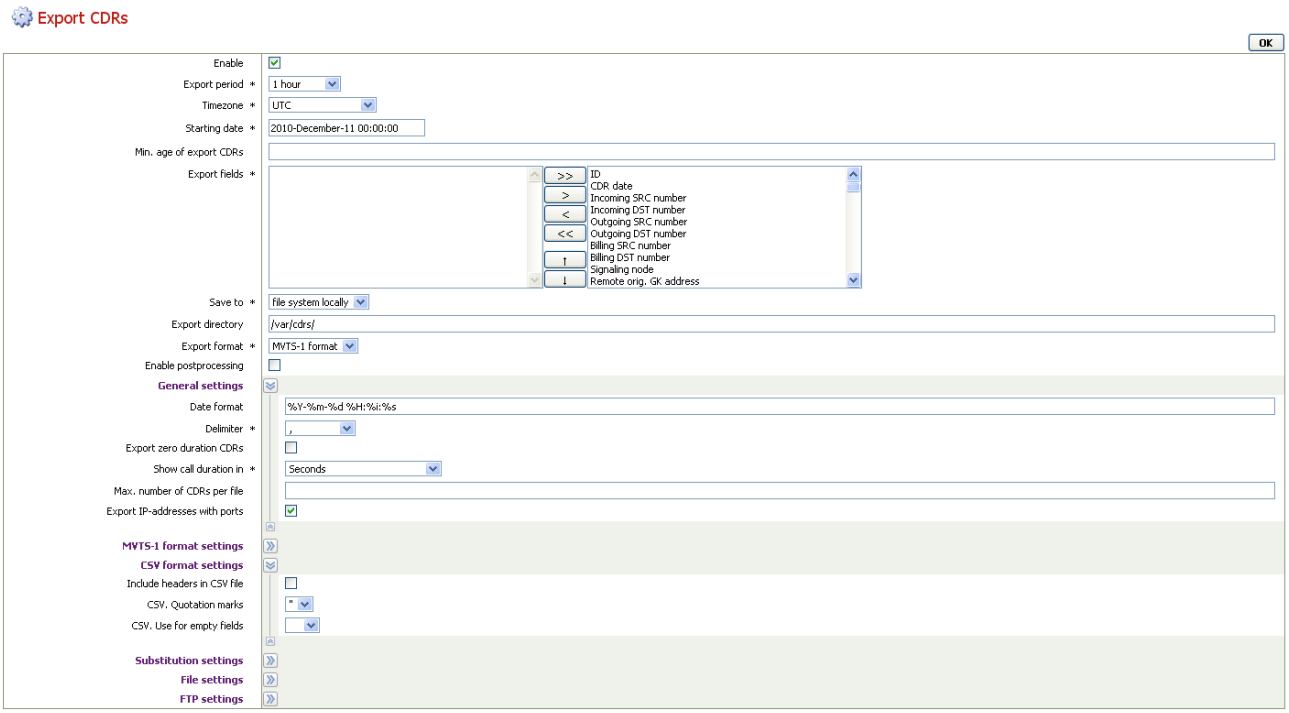

Figure 1: Export CDRs settings

Go to *CDRs – Export CDRs – Scheduled Export* subsection and set all parameters in accordance to screenshot (Figure 1).

Please pay attention to following fields:

- **Export period** – set desirable CDR creation period;
- **Timezone** – it is recommended to set this value to UTC;
- **Export fields –** make sure that all available fields are shown in the right panel;
- **Save to –** select to store files locally, and make sure that storage directory is */var/cdrs/*;
- **Export format –** select *MVTS 1 format* here;
- **Delimiter –** select comma delimiter here;
- **Show call duration in –** make sure that this field is set to *seconds* without any rounding options.

Important: when configuring CDR-files collector on your VCS system, you need to set *Overwrite TZ* setting into actual timezone of your choice (for example, GMT +02) to prevent differences in call times, as MVTS PRO does not supply the actual timezone.

4.2 Integration via RADIUS + Dynamic Routing

The whole setup consists of adding RADIUS-server settings, VCS-related equipment and respective dial peer. Please note that described integration includes RADIUS authentication, authorization, accounting and external routing features.

4.2.1 RADIUS server

Firstly, go to *RADIUS configuration – RADIUS Servers* and add VCS RADIUS server with same parameters as on provided screenshot (Figure 2).

Pay attention to the following fields:

- **RADIUS server name** – enter your RADIUS server name here and activate «Enable» checkbox;
- **Precedence** – set this value to «5»;
- **Enable authentication** – enable this only if you need RADIUS authentication;

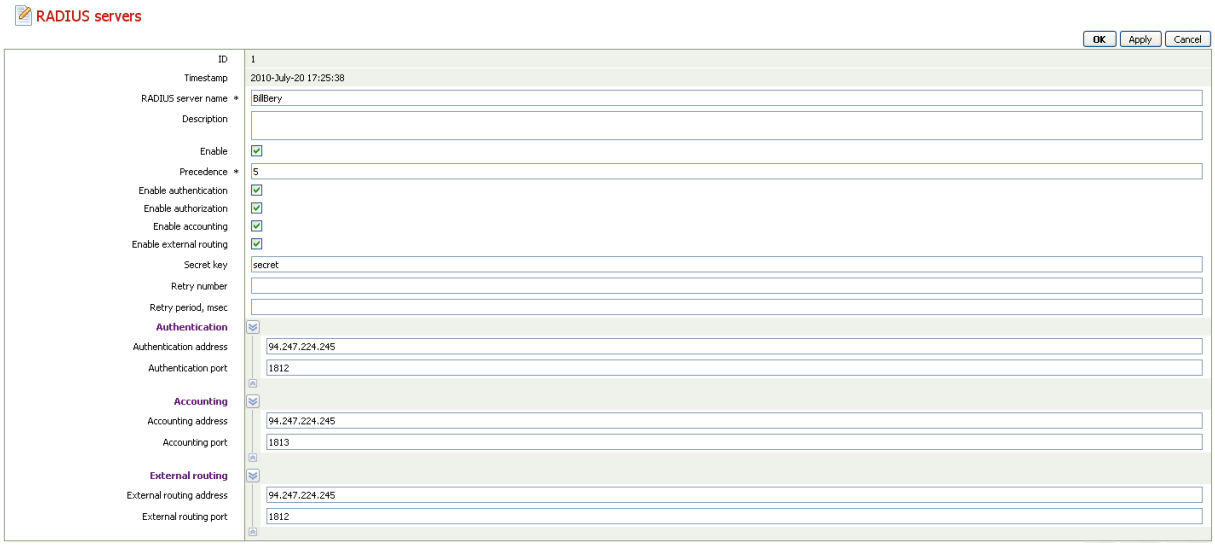

Figure 2: RADIUS server parameters

- **Enable authorization** – enable this only if you need RADIUS authorization;
- **Enable accounting** – enable this only if you need RADIUS accounting;
- **Enable external routing** – enable this only if you need to setup *Dynamic Routing* in VCS;
- **Secret key** – specify your RADIUS password here;
- **Authentication address** – specify the IP of VCS server in this field;
- **Authentication port** – set this value to 1812;
- **Accounting address** – specify the IP of VCS server in this field;
- **Accounting port** – set this value to 1813;
- **External routing address** – specify the IP of VCS server in this field;
- **Routing port** – set this value to 1812.

Also, go to *RADIUS configuration – RADIUS accounting profiles* and make sure that *Standard* profile has *"of the outgoing leg"* parameter specified for *Send ACCT.START/STOP packets* field.

Secondly, go to *RADIUS configuration – RADIUS attributes* and make sure that *h323-disconnect-time* string value is set to *toVsaTimeFormat(inLeg.disconnectTime, "UTC")*:

	19	mvts-h323-call-id	h323-call-id	1	9 (Cisco VSA)	string	toCiscoCallId(callId)	Идентификатор вызова
	20	cisco-h323-call-type	h323-call-type	27	9 (Cisco VSA)	string	"VoIP"	Indicates call leg type. Possible values are telephony and VoIP.
	21	cisco-h323-call-origin	h323-call-origin	26	9 (Cisco VSA)	string	legType	Gateway's behavior in relation to the connection that is active for this leg.
	22	cisco-h323-gw-id	h323-gw-id	33	9 (Cisco VSA)	string		Domain name server (DNS) name or local name of the voice gateway that is sending the VSA.
	23	mvts-h323-gw-address	h323-gw-address	1	9 (Cisco VSA)	string	getIP(gwAddress)	IP-адрес шлюза-инициатора
	24	mvts-h323-remote-id	h323-remote-id	1	9 (Cisco VSA)	string	outLeg.gwName	Идентификатор терминирующего шлюза
	25	cisco-h323-remote-address	h323-remote-address	23	9 (Cisco VSA)	string	remoteSigAddress	IP address of the remote gateway.
	26	cisco-h323-incoming-conf-id	h323-incoming-conf-id	1	9 (Cisco VSA)	string	toCiscoConfId(inLeg.confId)	Unique number for identifying a calling session on a gateway, where a session is closed when the calling party hangs up. Is used to do the following: •Match the outbound and inbound call legs for a session on a particular gateway •Collect and match all records for multiple calls placed (within the bounds of a session) on the gateway
	27	mvts-h323-incoming-call-id	h323-incoming-call-id	1	9 (Cisco VSA)	string	toCiscoCallId(inLeg.callId)	Call ID пришедший от оборудования
	28	cisco-h323-disconnect-time	h323-disconnect-time	29	9 (Cisco VSA)	string	toVsaTimeFormat(inLeg.disconnectTime, "UTC")	Disconnect time in NTP format: hour, minutes, seconds, microseconds, time_zone, day, month, day_of_month, year.
	29	cisco-h323-disconnect-cause	h323-disconnect-cause	30	9 (Cisco VSA)	integer	reasonToH323(code)	Q.931 disconnect cause code retrieved from CCAPI. The source of the code is the disconnect location such as a PSTN, terminating gateway, or SIP.
	30	cisco-subscriber	subscriber	1	9 (Cisco VSA)	string		T1/channel-associated signaling (CAS) or E1/R2 signal information about a subscriber.
	31	cisco-session-protocol	session-protocol	1	9 (Cisco VSA)	string	proto	Session protocol used for calls between the local and remote router through the IP backbone. Always equal to "sip" for SIP or "Cisco" for H.323.
	32	cisco-release-source	release-source	1	9 (Cisco VSA)	integer	toCiscoReleaseSource(inLeg.disconnectInitiator, proto)	Indicates whether a call was released by a calling party, a called party, or an internal or external source.

Figure 3: RADIUS attributes

4.2.2 VCS (Billbery) equipment

Go to *Equipment* – *Equipment* and create following gateways: BILLBERY_GW, BILLBERY_SIP, BILLBERY_ROUTING and DEFAULT. Please make sure that each gateway parameters match values provided on respective screenshots below (Figure 4-6).

4.2.2.1 BILLBERY_GW

This is main gateway for H323 based traffic. Please pay attention to the following fields:

- **Equipment type** – select *Gateway* in this field;
- **Protocol** – select *H.323* value;
- **Term. Default protocol** – select *H.323* value;
- **Orig. IP address** – enter 0.0.0.0/0 in this field (this is required if your MTS PRO version is 1.6 or above);
- **Term. IP address** – enter IP of your VCS server here;
- **Term. Port H323** – enter 1720 here;
- **Term. Port SIP** – enter 5060 here;
- **Enable RADIUS authorization** – enable this option;

– **Enable RADIUS accounting** – enable this option.

Overall, this gateway configuration should look like on the provided screenshot (Figure 4):

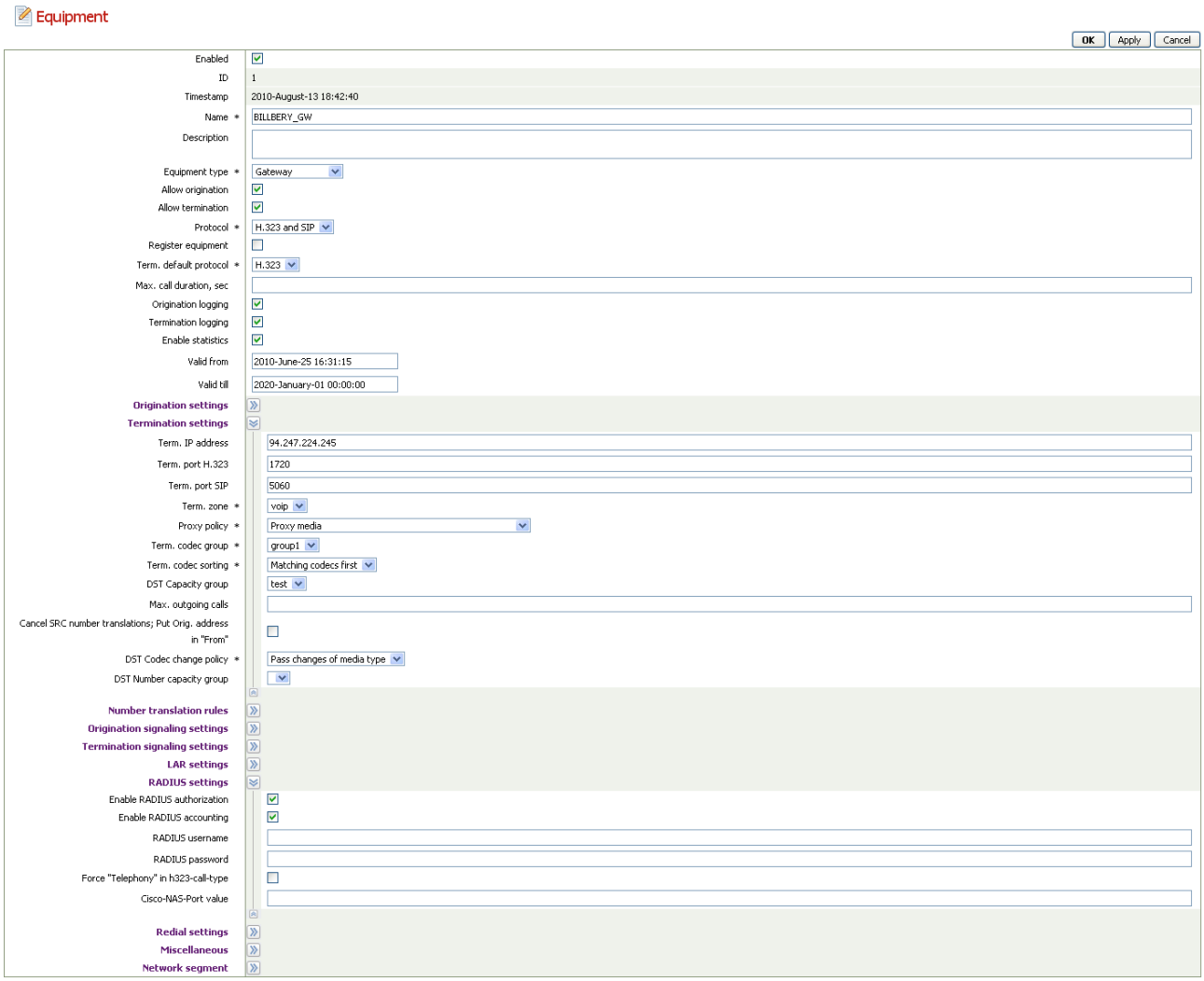

Figure 4: BILLBERY_GW parameters

4.2.2.2 BILLBERY_SIP

This is main gateway for SIP based traffic. Please pay attention to the following fields:

– **Equipment type** – select *Gateway* in this field;

– **Protocol** – select *SIP* value;

– **Orig. IP address** – enter 0.0.0.0/0 in this field (this is required if your MTS PRO version is 1.6 or above);

- **Term. IP address** – enter IP of your VCS server here;
- **Term. Port SIP** – enter 5060 here;
- **Enable RADIUS authorization** – enable this option;
- **Enable RADIUS accounting** – enable this option.

Overall, this gateway configuration should look like on the provided screenshot (Figure 5):

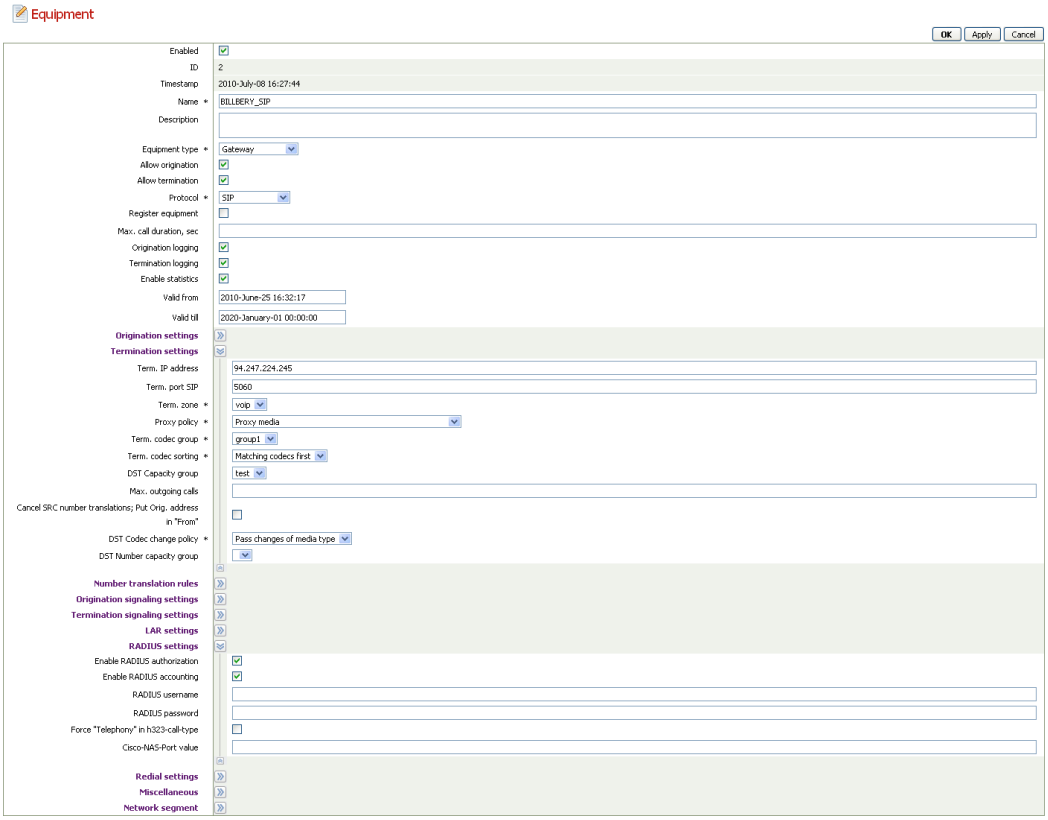

Figure 5: BILLBERY_SIP parameters

4.2.2.3 BILLBERY_ROUTING

This is VCS's routing gateway. Please pay attention to the following fields:

- **Equipment type** – select *Routing Server* in this field;
- **Protocol** – select *H.323 and SIP* value;
- **Term. Default protocol** – select *SIP* value;

– **Term. IP address** – enter IP of your VCS server here (note that in MVTS PRO ver. 1.6 and above you will not be able to set IP for your routing server. System will use address you specify in Radius settings);

– **Term. Port H323** – enter 1720 here;

– **Term. Port SIP** – enter 5060 here;

Overall, this gateway configuration should look like on the provided screenshot (Figure 6):

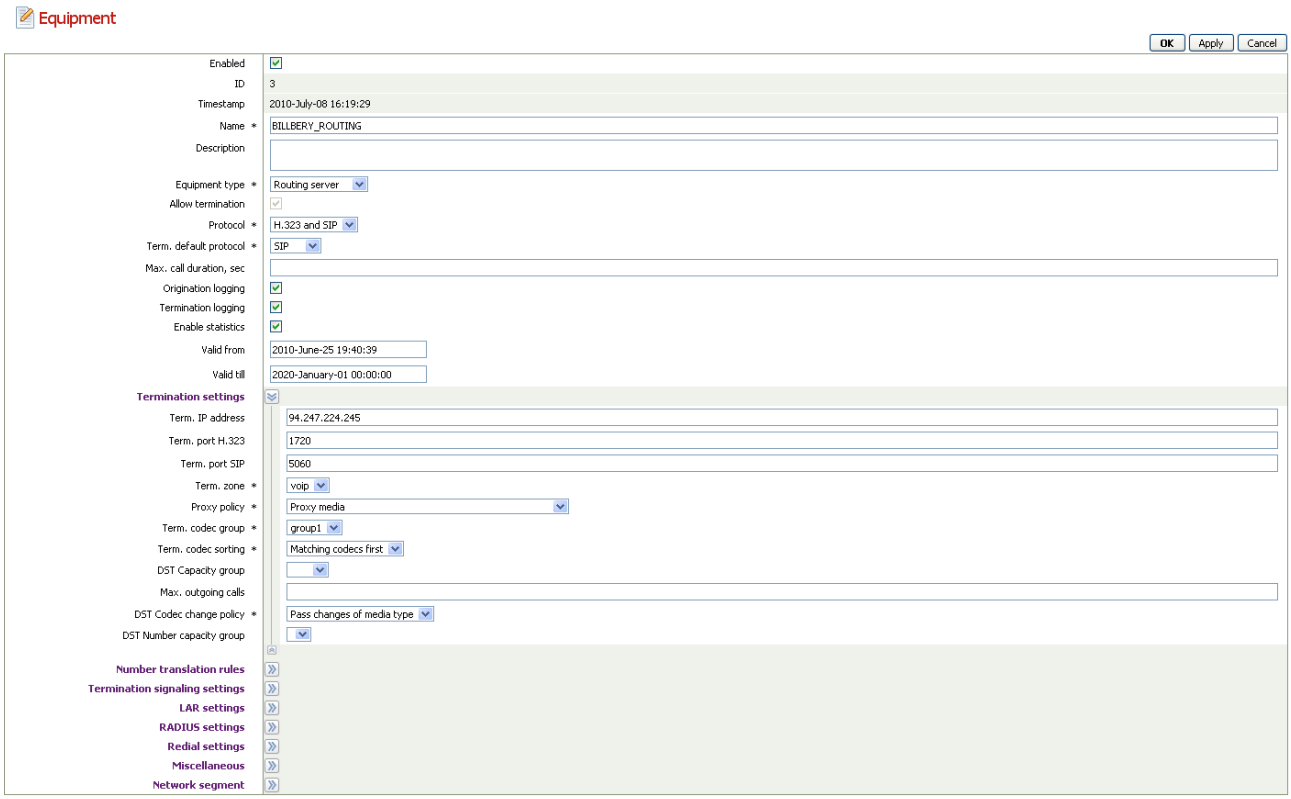

Figure 6: BILLBERY_ROUTING parameters

4.2.2.4 DEFAULT

This gateway can be used to perform *Default authentication* (i.e. user account will be authenticated through RADIUS by settings of VCS's clients, not by adding respective customer equipment within MVTS Pro interface). Please note that this feature works only for SIP accounts, as support for H.323 gateways authentication was deliberately removed from MVTS Pro.

Default gateway configuration should look like on the provided screenshot (Figure 7):

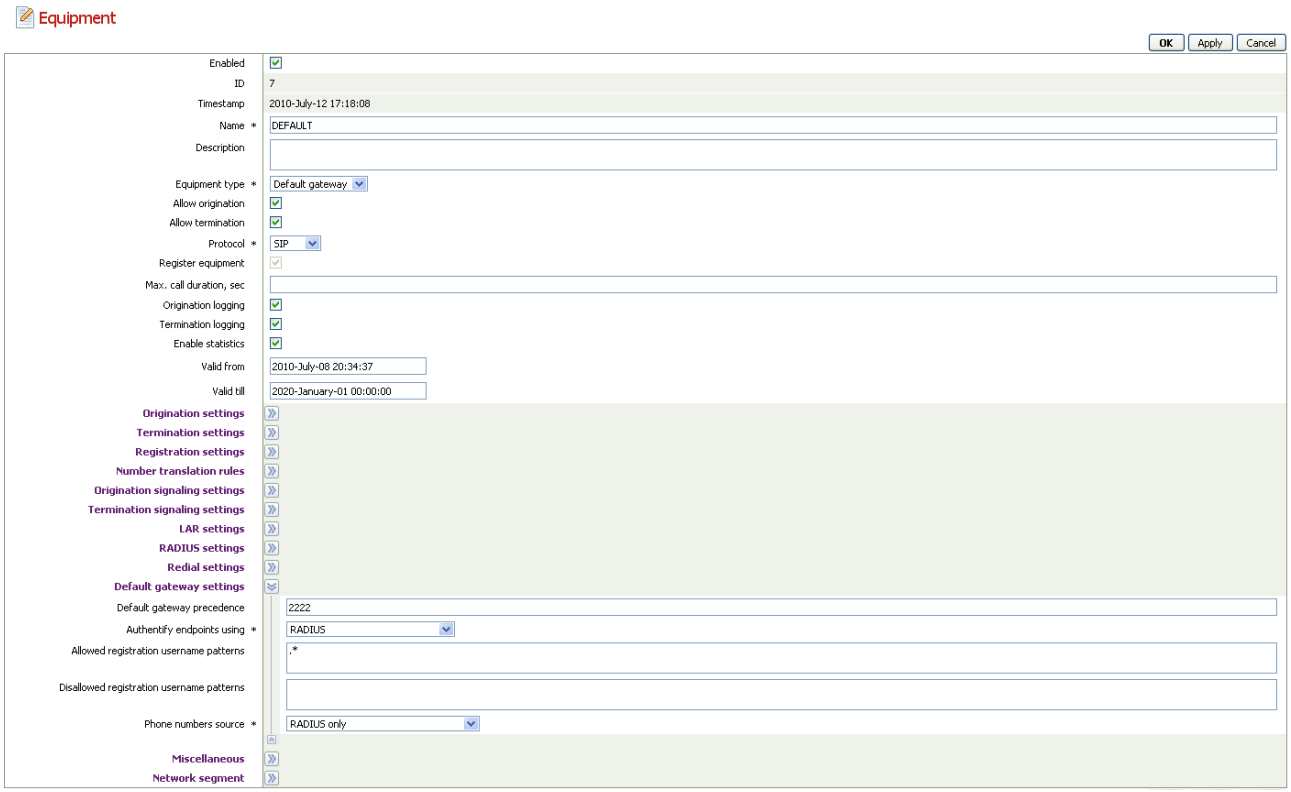

Figure 7: DEFAULT parameters

Please pay attention to the following fields:

– **Equipment type** – select *Default gateway* in this field;

– **Protocol** – select *SIP* value;

– **Term. Default protocol** – select *H323* value;

– **Enable RADIUS authorization** – enable this option;

– **Enable RADIUS accounting** – enable this option;

– **Authentify endpoints using** – select *RADIUS* here;

– **Allowed registration username patterns** – enter .* in this field;

– **Phone numbers source** – select *RADIUS only* here.

4.2.3 VCS dial peer

Go to *Termination – Dial peers* and create a dial peer with settings that match the screenshot below (Figure 8):

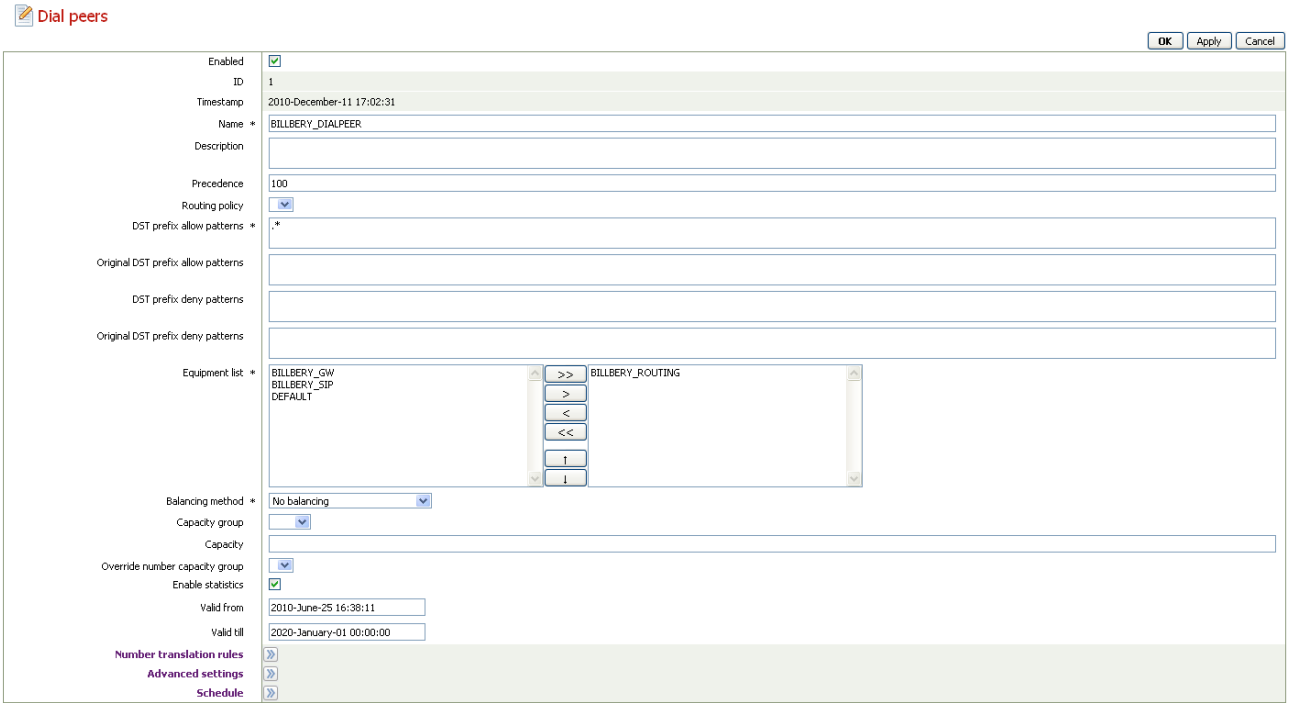

Figure 8: VCS dial peer parameters

Please make sure that you specified following:

– **DST prefix allow patterns** – enter *.** in this field to set all traffic for routing through VCS routing engine. You may set any specific pattern, for example, to match specific destinations;

– **Equipment list** – make sure that BILLBERY_ROUTING is displayed in right part.

5. Aloe RTU Class 5 (IP Centrex)

5.1 Integration via CDR-files

Log in to IP Centrex web-interface, go to *CDRs* – *Scheduled Export* and specify following parameters (Figure 9):

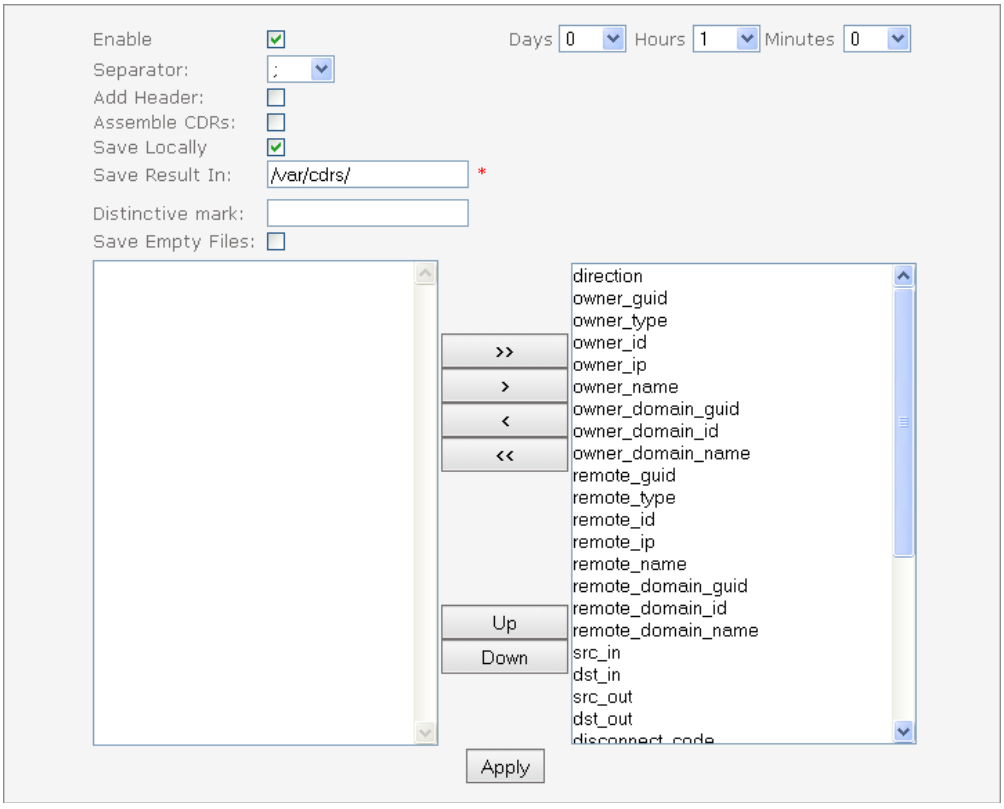

Figure 9: IP Centrex CDR Export settings

Make sure you've specified:

– **Enable** – enable the export and specify export period (1 hour for example);

– **Separator** – specify comma as delimiter for values;

- **Save locally** – make sure that files will be saved locally on IP Centrex server;
- **Save Result In** – specify the path to store CDRs (it should match the path you've already specified in VCS's settings).

5.2 Integration via RADIUS

Please go to *RADIUS* section of IP Centrex's interface and set following parameters (Figure 10).

Please pay attention to the following fields:

- **Mode** – select *«All»*;
- **Secret** – specify your RADIUS secret password here;
- **NAS IP** – enter your IP Centrex's IP-address here;
- **Authentication during registration** – enable this option;
- **Call Authorization** – select *«For all»*;
- **Send accounting START/STOP for** – select «Originate»;
- **Send Domain ID** – make sure that @ sign is selected as separator;
- **Digital Authentication** – select *«Draft Stermann 00»*;
- **Always send accounting STOP** – enable this option;
- **Server addresses** – enter your VCS server IP here and specify access ports (for authorization and accounting by default it's 1812 and 1813 respectively);
- **Local addresses** – enter your IP Centrex's IP-address here and specify access ports (for authorization and accounting by default it's 11812 and 11813 respectively).

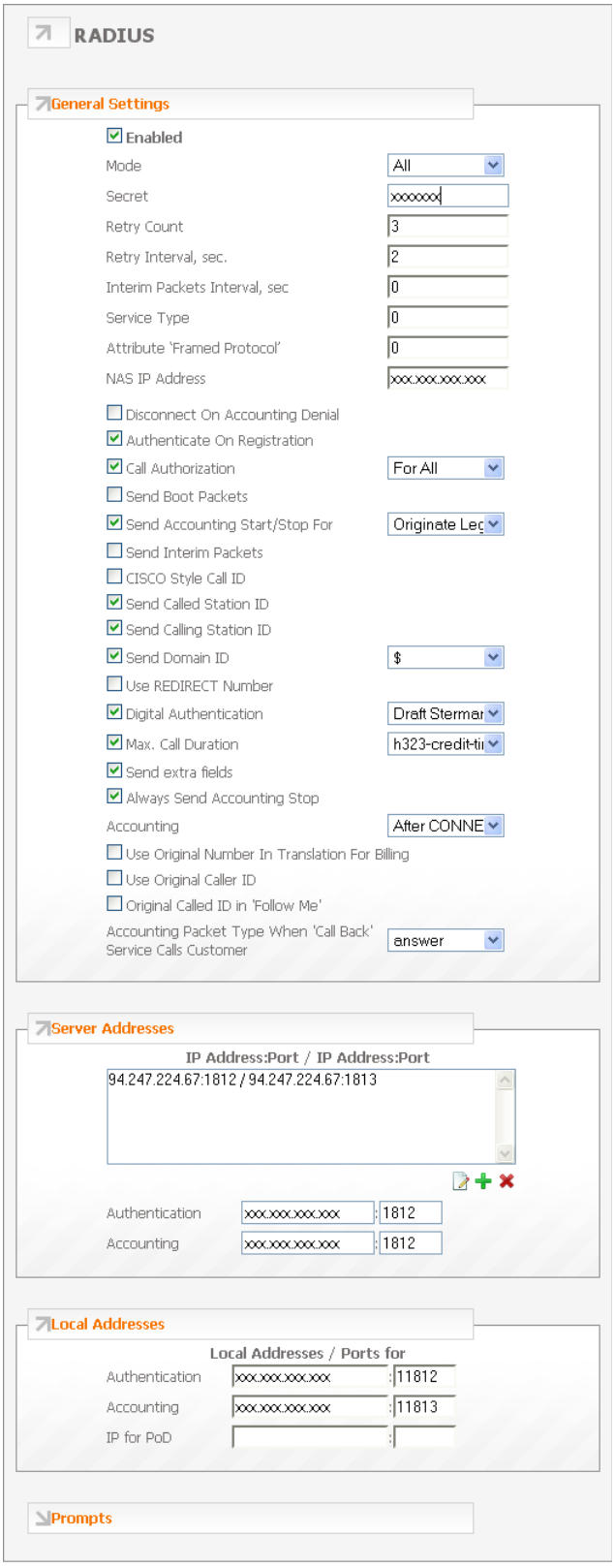

Figure 10: IP Centrex RADIUS settings

Also, make sure that when you add subscribers, you have enabled RADIUS accounting and authorization. As an example, subscriber configuration may look like on screenshot below (Figure 11):

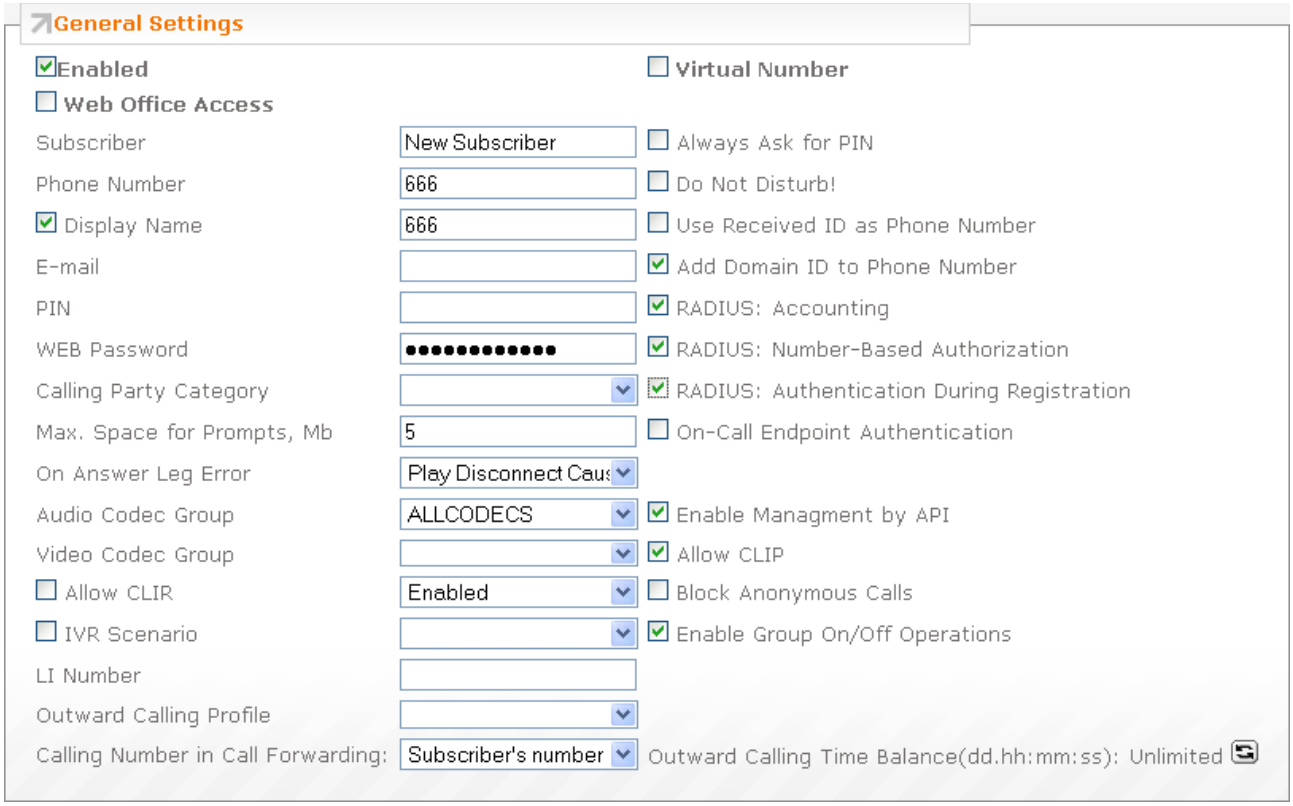

Figure 11: IP Centrex subscriber settings

6. Aloe Transit SBC

6.1 Integration via CDR-files

Make sure that /var/cdrs/ directory is created on SBC server, or create it by using command:

```
mkdir /var/cdrs
```

Make sure this folder access rights are 02775, or assign them manually with command:

```
chmod 02775 /var/cdrs
```

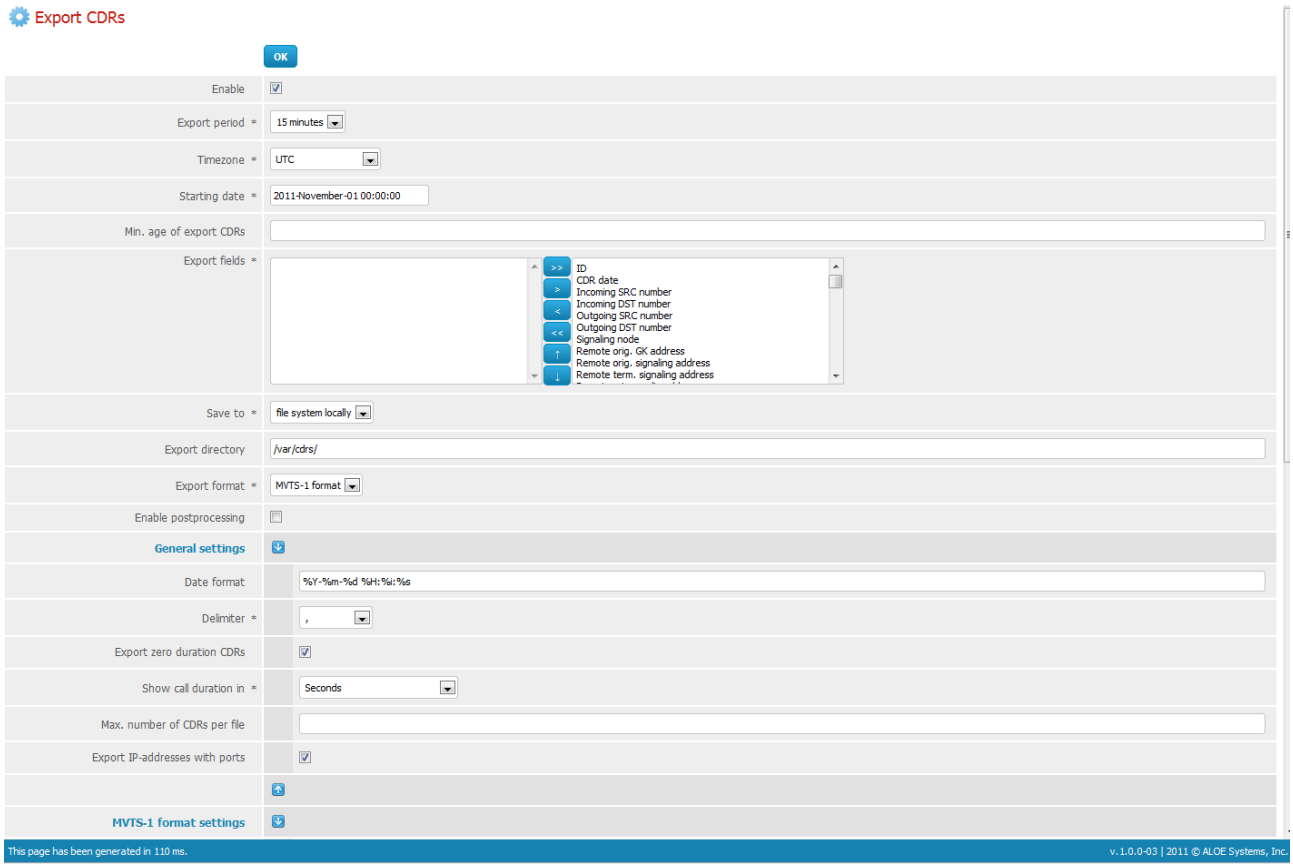

Figure 12: Export CDRs settings

Go to *CDRs – Export CDRs – Scheduled Export* subsection and set all required parameters (Figure 12).

Please pay attention to following fields:

- **Export period** – set desirable CDR creation period;
- **Timezone** – it is recommended to set this value to UTC;
- **Export fields –** make sure that all available fields are shown in the right panel;
- **Save to –** select to store files locally, and make sure that storage directory is */var/cdrs/*;
- **Export format –** select *MVTS 1 format* here;
- **Delimiter –** select comma delimiter here;
- **Show call duration in –** make sure that this field is set to *seconds* without any rounding options.

Important: It is also highly recommended to go to *Global Setings – System global settings* section and set *Disconnect Time* as value for *Date field in CDR*.

Important: when configuring CDR-files collector on your VCS system, you need to set *Overwrite TZ* setting into actual timezone of your choice (for example, GMT +02) to prevent differences in call times, as Aloe SBC does not supply the actual timezone.

6.2 Dynamic Routing setup

Aloe Transit SBC can be set up to utilize external routing features via VCS SIP Redirect Server. Here is a short instruction on how you can do that.

6.2.1 VCS equipment

Go to *Equipment* – *Equipment* section and create a new equipment with following settings (Figure 13):

- **Name** – set *VCS_ROUTING* as name for your equipment;
- **Equipment type** – specify *SIP routing server* here;
- **Term. SRC type of number** – specify *National number* here;
- **Term. DST type of number** – specify *National number* here;
- **SIP router IP address** – specify your VCS server Ip address in this field.

Majority of other settings can be left at default values.

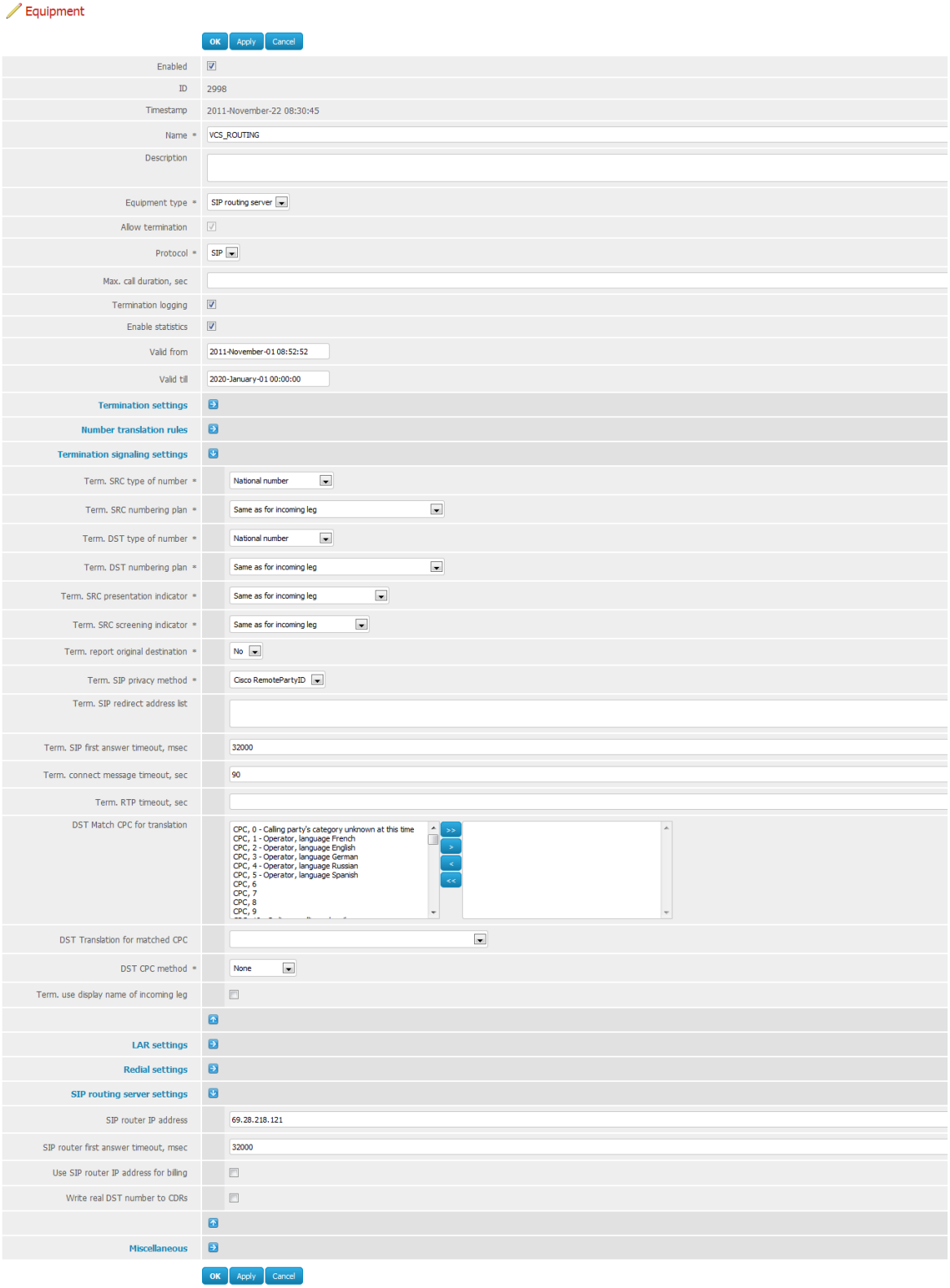

Figure 13: VCS_Routing SIP equipment

6.2.2 VCS dialpeer

Go to *Termination – Dial peers* and create a dial peer with following settings (Figure 14):

- **Name** – set *VCS_DIALPEER* as name for your dial peer or any other name of your choice;
- **DST prefix allow patterns** – specify *.** as pattern to make sure all calls will be caught by this dial peer;
- **Equipment list** – make sure that your *VCS_ROUTING* SIP redirect server is displayed in right panel.

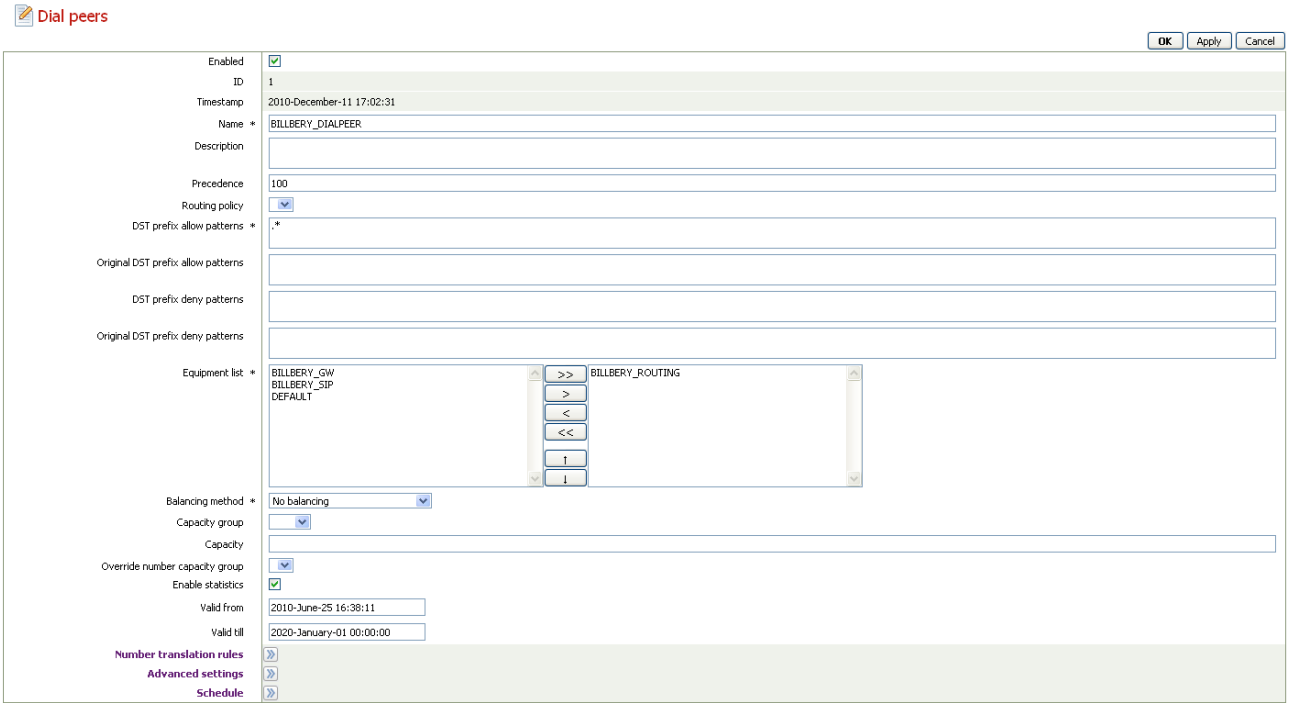

Figure 14: VCS dial peer parameters

6.2.3 Customers configuration

When adding customer's equipment in *Equipment – Equipment* section, make sure that you specify the following translation rule in *Orig. DST number translation* field: ^(.*)/xxx*\1, where xxx* is specific identifier of your customer during SIP authentication (xxx* can be anything, for example 111* or 999*, as long as numbers prior * will match with numbers set on accounts page of respective customer in VCS as *Ident by Name* account).

7. Asterisk

7.1 Integration via CDR-files

Perform following operations in listed order:

1) Copy a file from VCS server from path */usr/local/vcs/share/extra/convertors/asterisk-rotate.sh* into */usr/bin/* folder on Asterisk server, and setup it in *etc/crontab/* as:

```
0 * * * * root /usr/bin/asterisk-rotate.sh
```

i.e. - to be executed hourly.

2) Open */etc/asterisk/cdr.conf* file on Asterisk server and make sure that following lines are present:

```
[csv]
usegmtime=yes    ; log date/time in GMT.  Default is "no"
loguniqueid=yes  ; log uniqueid.  Default is "no"
loguserfield=yes  ; log user field.  Default is "no"
```

7.2 Integration via RADIUS

Native support of RADIUS features for Asterisk is limited for RADIUS accounting, which should be available for you if you performed required VCS settings, listed in section 2.2 of this document. Unfortunately, due to highly customizable nature of Asterisk, all other RADIUS related functions (authorization, authentication, routing etc.) can be supplied only by custom-tailored RADIUS modules for Asterisk.

Note: one of the main things you need to be sure of, is that your Asterisk platform supplies customer IP address in *asterisk-user-field* field of RADIUS accounting stop packets.

8. Brekeke SIP Server

8.1 Integration via RADIUS

Please perform following configurations in your Brekeke SIP Server Admintool. In this example, we use Brekeke SIP Server advanced edition, which already includes the radius setup in the Admintool.

1) Go to Brekeke SIP Server Admintool, *Configuration - SIP - Authentication* and set ***ON*** at authentication for both ***REGISTER*** and ***INVITE*** (Figure 15). Save the settings.

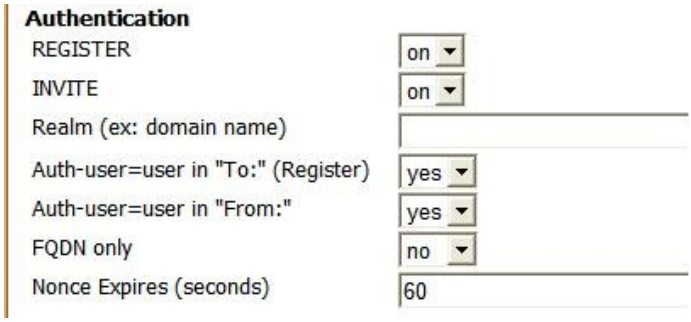

Figure 15: Brekeke SIP Server authentication configuration

2) Go to Brekeke SIP Server Admintool, *Configuration - Database/Radius - Radius*, set up Radius as below, and save settings (Figure 16):

   – **On/Off (Authentication)** – on;

   – **Port Number(Authentication)** – set auth port value here (it should match the auth port set in *Configuration - Settings* section of VCS);

   – **Port Number(Accounting)** – set acct port value here (it should match the acct port set in *Configuration - Settings* section of VCS);

   – **Server IP Address** – JeraSoft VCS server IP address;

– **Shared Secret** – your secret password (should match secret you set in *Configuration - VoIP Gateways* section of VCS).

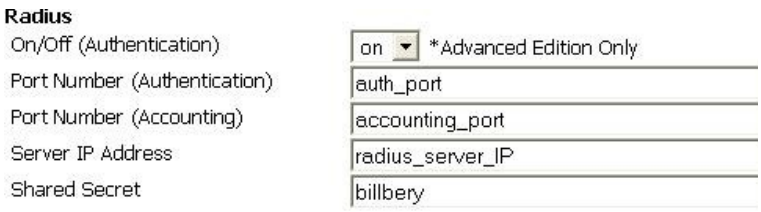

Figure 16: Brekeke SIP Server RADIUS configuration

3) Add the following dial plan to use Radius account plugin for each call:

```
[Matching Patterns]
$request = ^INVITE
[Deploy Patterns]
$session = plugin.radius.RadiusAcct
$continue = true
```

4) If realm is not necessary for the Radius Attribute User-Name, please add the following parameter at Brekeke SIP Server Admintool in *Configuration – Advanced*:

```
radius.addrealmtouser = false
```

5) Restart Brekeke SIP Server from Admintool when above setup is finished.

9. Cisco Switches

9.1 Integration via RADIUS

To allow RADIUS accounting and authorization, add following lines to your Cisco's configuration file:

```
!
aaa new-model
!
gw-accounting aaa
!
radius-server host <BILLING-IP> auth-port 1804 acct-port 1904
radius-server key <SECRET>
radius-server vsa send accounting
radius-server vsa send authentication
!
!
aaa group server radius VCS
server <BILLING-IP> auth-port 1804 acct-port 1904
!
aaa accounting connection h323 start-stop group VCS
aaa accounting send stop-record authentication failure
aaa authentication login default group VCS local
aaa authorization exec default group VCS local
aaa authorization network default group VCS local
```

Where <*BILLING-IP*> should be changed to VCS IP address, and <*SECRET*> should be changed to the *secret* you specified in RADIUS collector in VCS.

To find more information about Cisco switch configuration, please refer to your Cisco User Manuals.

10. Genband (Nextone)

Nextone configurtion has few additional specifics and notes. Please browse them by going to ***Appendix 1*** section of this document.

10.1 Integration via CDR-files

Open your iServer Configuration utility, go to *Billing* tab and make sure that CDR settings are set in accordance to screenshot below (Figure 17):

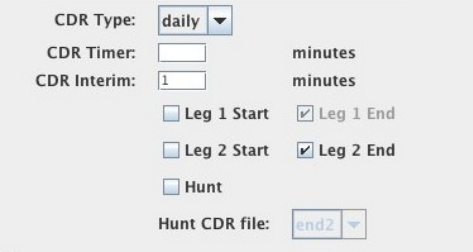

Figure 17: Nextone export CDRs settings

Also, make sure that your Nextone creates CDR-files, they are stored in a folder you specified within *VoIP Gateways* section in VCS, and that folder is accessible.

10.2 Dynamic Routing setup

Dynamic Routing setup is provided by using SIP Redirect server, which is already built into your VCS billing solution. If you want to utilize VCS dynamic routing features with Nextone, you need to do the following: create VCS related equipment and respective call plan on the Nextone side.

10.2.1 VCS equipment (routing gateway)

Log in to your iServer configuration utility and create a gateway with following settings (Figures 18, 19, 20):

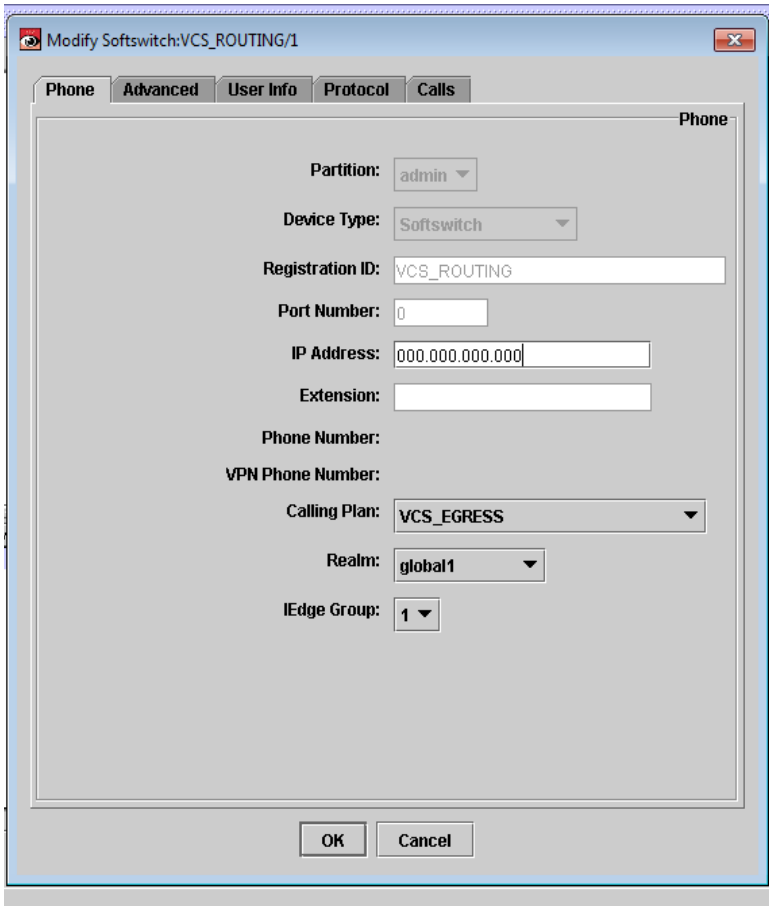

Figure 18: Nextone routing gateway settings (Phone tab)

Mandatory settings on the ***Phone*** tab are the following:

- **Device Type** – specify *softswitch* as device type;
- **Registration ID** – specify *VCS_ROUTING* in this field;
- **IP Address** – specify IP address of your VCS system here;
- **Calling Plan** – select *VCS_EGRESS* calling plan here (next subsection will describe how to create *VCS_EGRESS* plan).

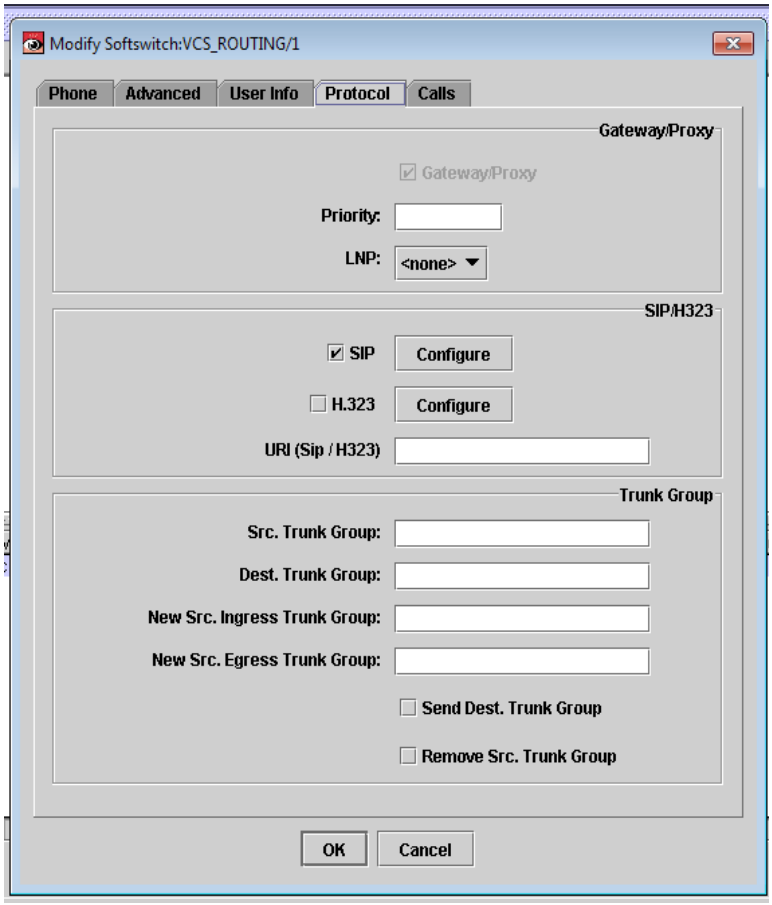

Figure 19: Nextone routing gateway settings (Protocol tab)

Mandatory settings on the ***Protocol*** tab are the following:

– **SIP/H323** – select only *SIP* protocol here.

Mandatory settings on the ***Calls*** tab are the following:

– **Limit** – make sure that all options are set to *Unlimited* value.

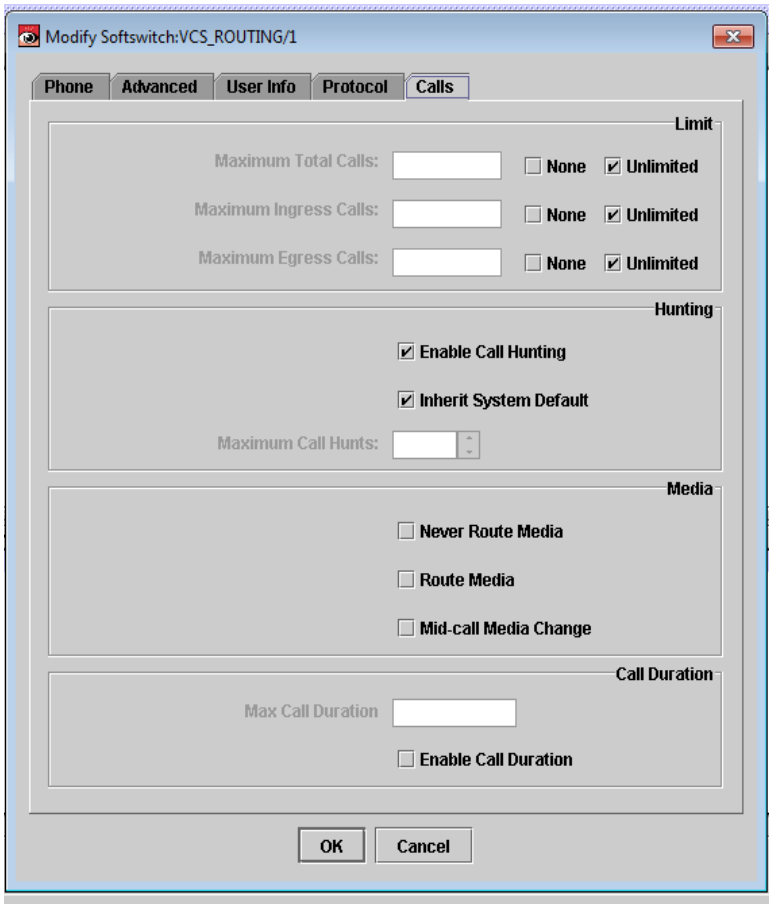

Figure 20: Nextone routing gateway settings (Calls tab)

10.2.2 VCS calling plan

Second step in this setup is to create respective calling plan, so all calls will be forwarded to VCS routing gateway. Please create a calling plan, and make sure you specify the following:

- **Plan Name** – specify the *VCS_EGRESS* as name for your calling plan;
- **Routes** – create a list of routes from 0 through 9, to make sure that all calls will be processed by this calling plan (Figure 21);
- **Routes Type** – make sure that all routes you have added are labeled as *Egress* type.

Save current routing plan and apply it to *VCS_ROUTING* gateway which you already have created.

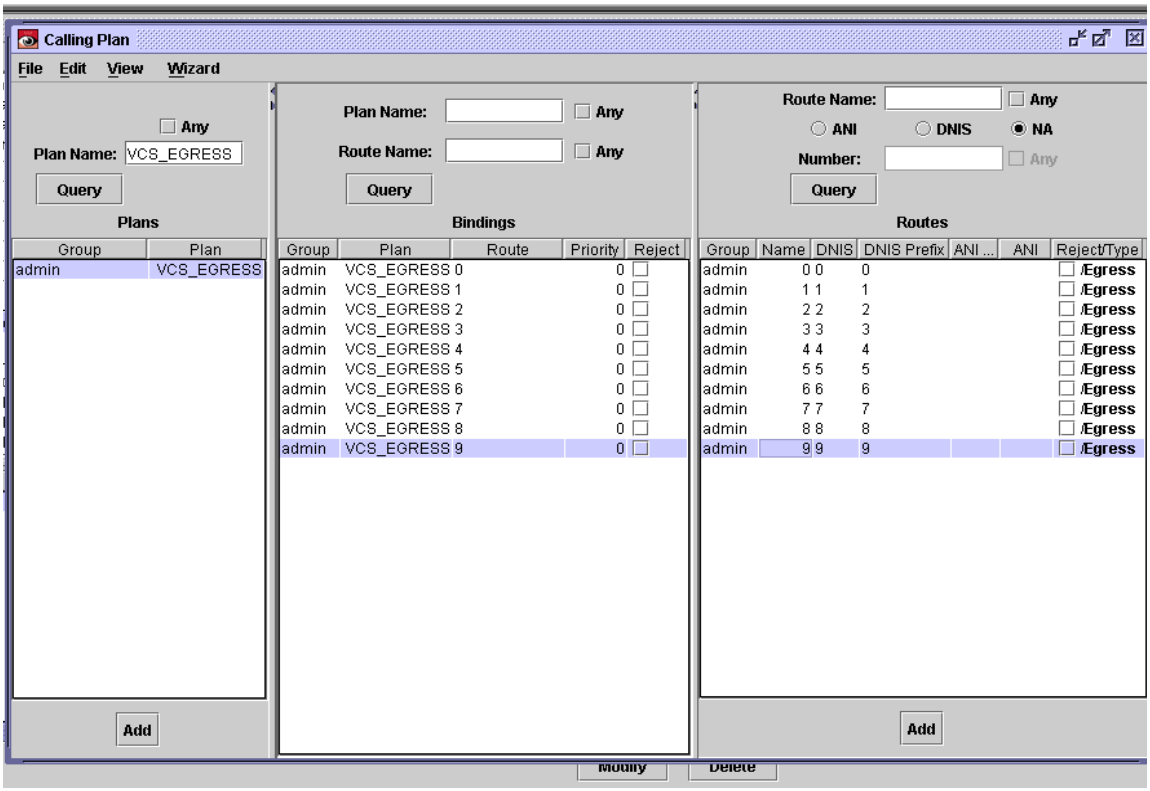

Figure 21: VCS_EGRESS calling plan settings

10.2.3 Adding subscribers

Nextone dynamic routing setup requires you to add origination gateways of customers, which then will be processed by VCS routing engine. Add such subscribers as you normally would, but pay attention to the following detail: if you open your subscriber settings, on the ***Protocol*** tab (Figure 18), you need to specify ***New SRC. Ingress Trunk Group*** with some user identifier, that should match same identifier which you specify in VCS's accounts as ***Ident by Name***. This is required for identification and authorization of customer gateway during routing.

Addition of termination gateways are not required, as everything regarding termination is set on the VCS system side (please refer to VCS User Manual for more information).

10.3. Nextone/Genband Realms

If your Nextone/Genband switch is configured to utilize it's virtualization “realms” feature, JeraSoft VCS can be configured to accommodate that feature.

Such accommodation purpose is to be able to treat each realm as stand-alone switching platform, so it can be assigned to different resellers to comply with full partitioning service.

Configuration itself is quite simple. All you need to do is access *Configuration – VoIP Gateways* section on your VCS, and add some or all of your realms as different VoIP Gateways, using exact match of realm name in Nextone/Genband and VoIP Gateway in VCS.

11. Sansay VSXi

11.1 Integration via CDR-files

Apart of generic VCS configuration for CDR-files, please make sure that your Sansay creates CDR-files and they are stored in a folder which you specified in VCS settings and that folder is accessible.

11.2 Integration via SIP Redirect / RADIUS

The whole setup consists of adding RADIUS and External Routing servers, VCS-related resource and respective route. Please note that described integration includes RADIUS authentication, authorization, accounting and external routing features.

Also, keep in mind that you need to use SIP Redirect feature to utilize external routing with Sansay VSXi and that requires few additional notes in regards to VCS integration. They are following:

1) You will still have to add customers as resources in your Sansay VSXi interface, even if you will utilize External Routing features of JeraSoft VCS;
2) When adding customers in your JeraSoft VCS, you must specify their protocol as SIP.

11.2.1 RADIUS server

Login to your Sansay VSXi web-interface, go to *App Servers* – *Radius*, and create RADIUS server for your VCS (Figure 22). Pay attention to the following fields:

– **Group index** – specify the group number for RADIUS server, for example «1»;

– **Group Policy** – set this value to «round_robin»;

- **Server Secret** – specify your RADIUS password here;
- **Auth Port** – specify 1812 as authentication port;
- **Acct Port** – specify 1813 as accounting port;
- **Resend Period** – up to your preferences, although «5» is a good value;
- **Max Resends** – up to your preferences, although «3» is a good value;

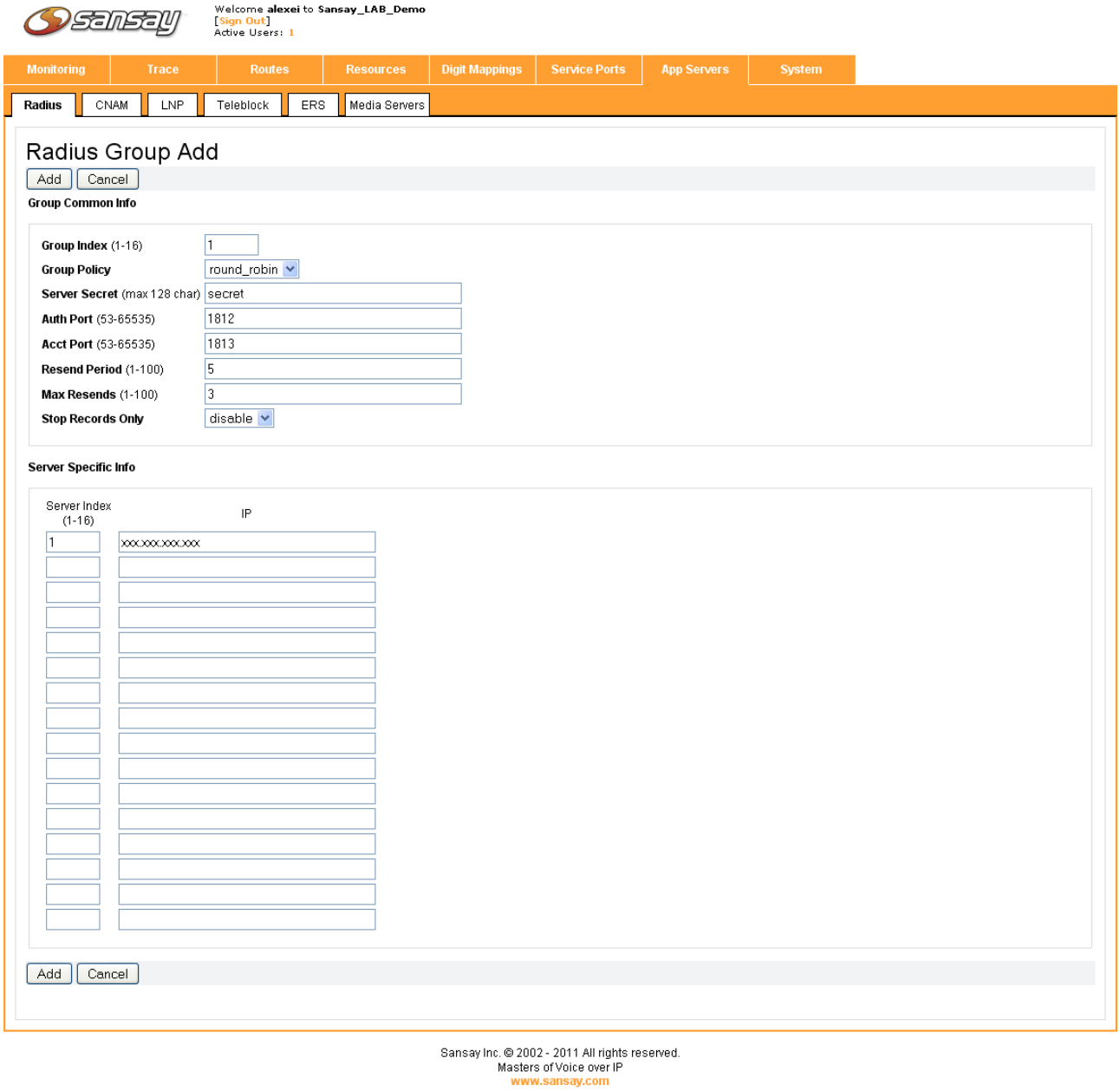

Figure 22: Adding VCS RADIUS server

– **Server Index** – set your VCS server index and IP address here.

Click *«Add»* when you are done to save settings.

11.2.2 External Routing Server (ERS)

While logged in to Sansay VSXi web-interface, go to *App Servers – ERS* and add external routing server for your VCS (Figure 23):

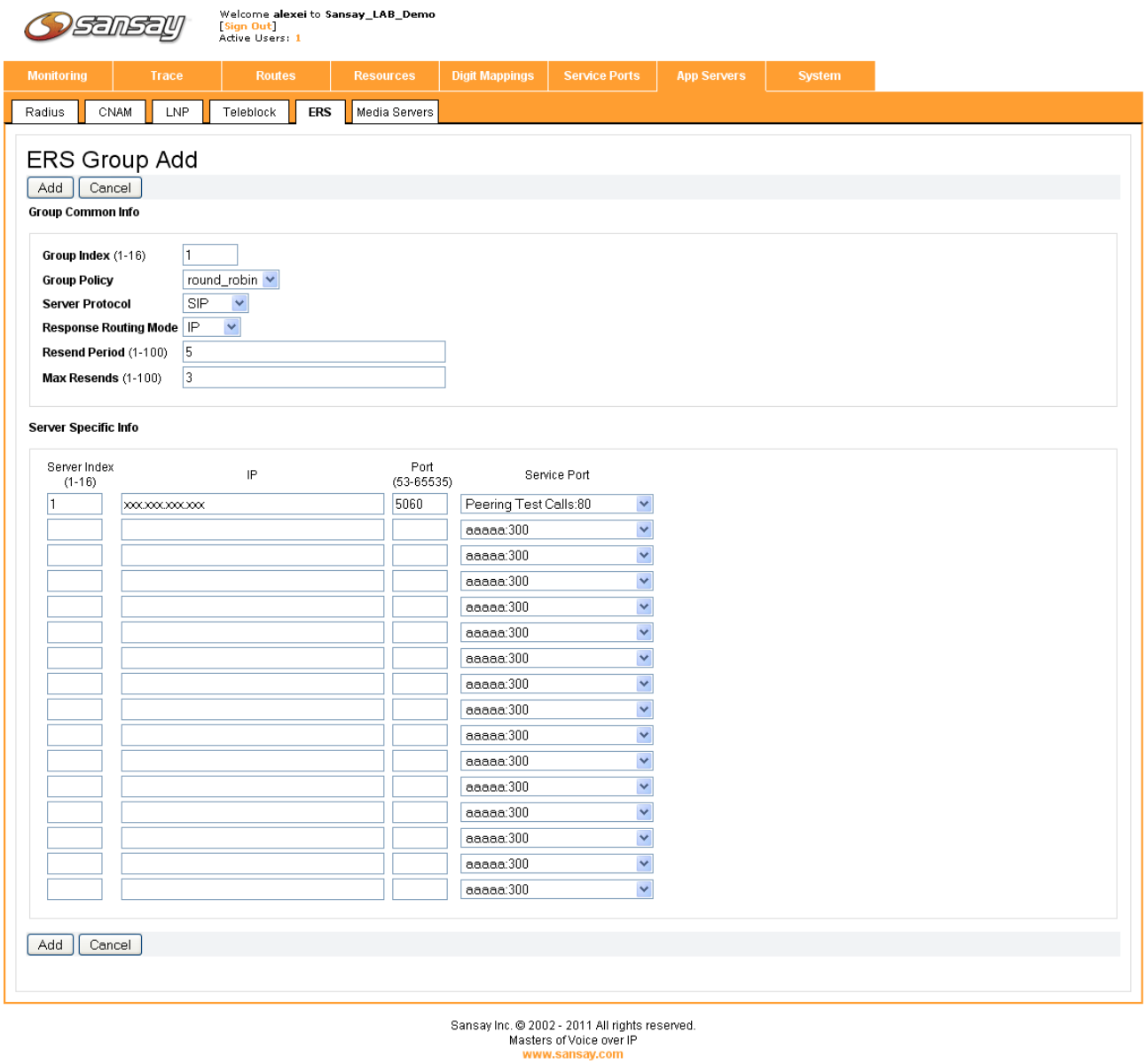

Figure 23: Adding VCS External Routing server

Pay attention to the following fields:

- **Group index** – specify the group number for ERS, for example «1»;
- **Group Policy** – set this value to «round_robin»;
- **Server Protocol** – specify «SIP» value;
- **Response Routing Mode** – defines how Sansay VSXi should respond to VCS in regards to routes. It's recommended to use «IP» setting here;
- **Resend Period** – up to your preferences, although «5» is a good value;
- **Max Resends** – up to your preferences, although «3» is a good value;
- **Server Index** – set your VCS server number, IP address and port here. Port value is «5060».

Click *«Add»* when you are done to save settings.

11.2.3 VCS (BillBery) resource

To make sure that external routing will work correctly, you need to create a specific resource, named BILLBERY_GW. To do that, go to *Resources* – *Resources* and add a resource with following parameters (Figure 24).

Pay attention to the following fields:

- **Resource Type** – set this value to «Peering»;
- **Protocol** – specify «SIP» value;
- **Trunk ID** – set trunk id number for your resource, for example «5000»;
- **Name** – make sure that your resource name is «BILLBERY_GW»;
- **Remote Port** – specify «5060» value as your port;
- **Radius Authentication** – select appropriate number that resembles VCS Radius Server ***Group Index***;
- **Radius Accounting** – select appropriate number that resembles VCS Radius Server ***Group Index***;
- **ERS** – select appropriate number that resembles VCS External Routing Server ***Group Index***;

– **Fqdns** – specify details for your VCS server: IP address, netmask, capacity and CPS limits.

Click *«Add»* when you are done to save settings.

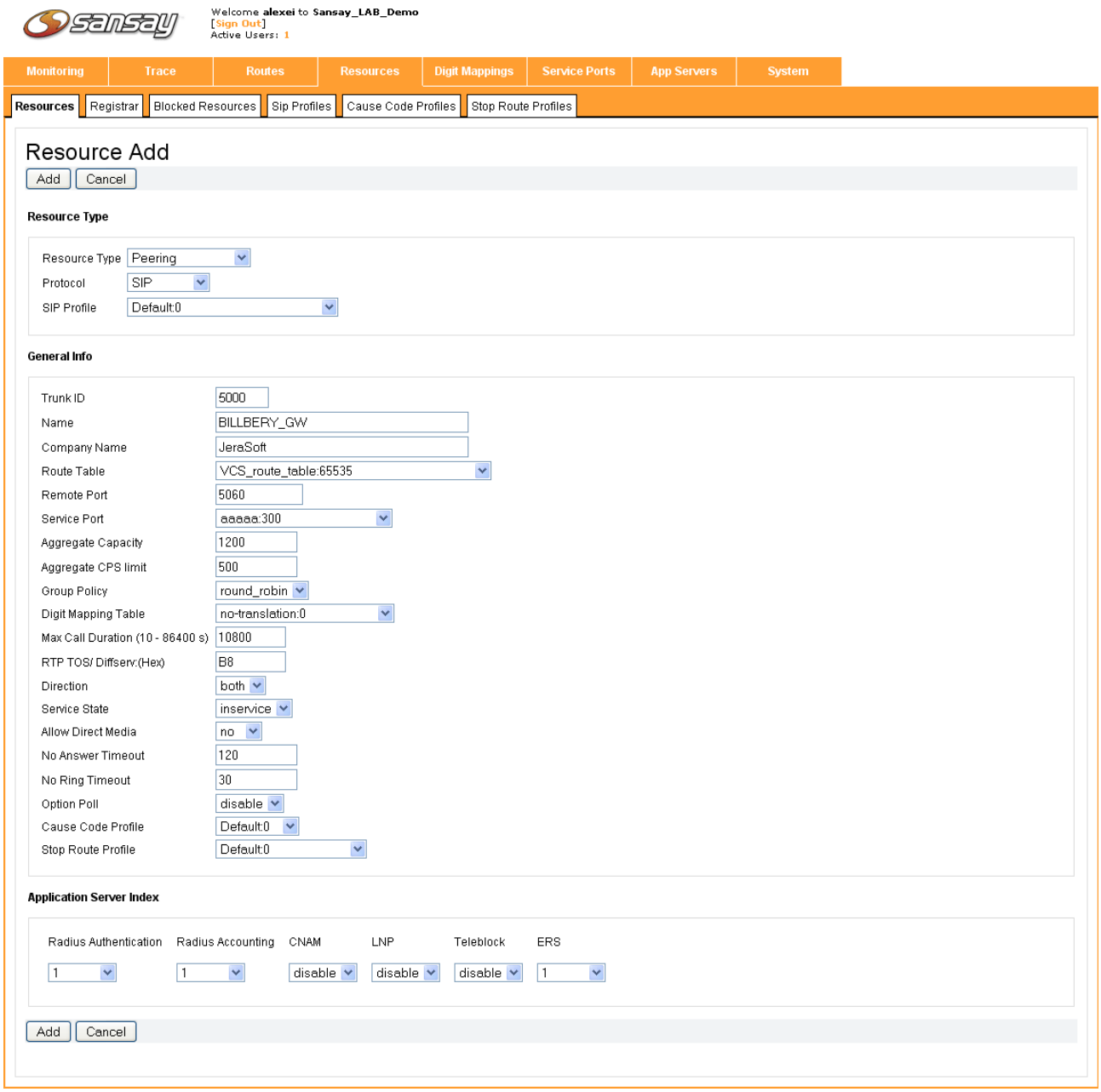

Figure 24: Adding VCS-related resource

11.2.4 VCS route

To be able to direct traffic to VCS for external routing, you need to create respective route. Go to *Routes – Routes* and create the following route (Figure 25):

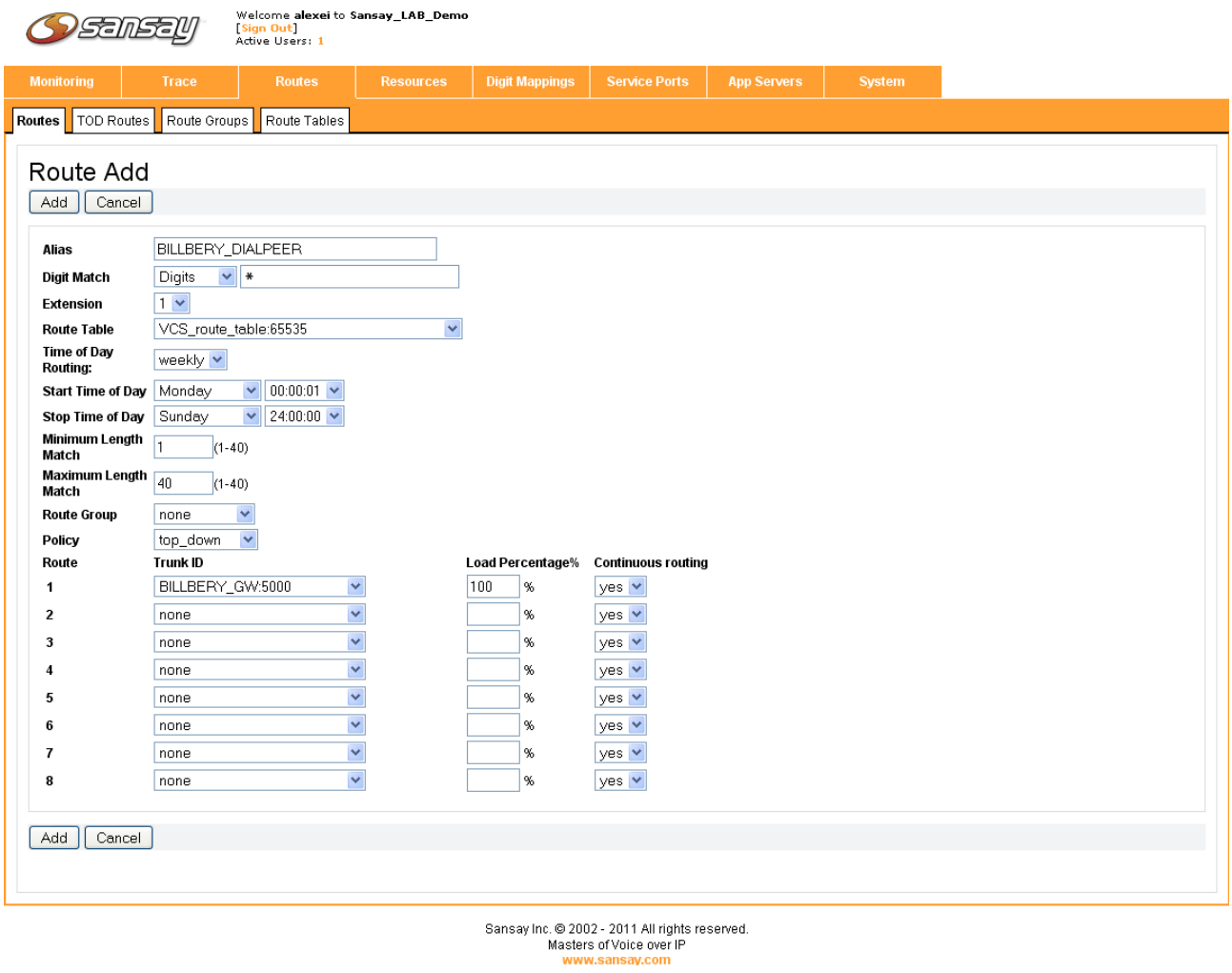

Figure 25: Adding VCS-related route

Pay attention to the following fields:

– **Alias** – specify a name for your route;

– **Digit Match** – specify a match for calls that should be routed externally via VCS;

– **Route** – specify your «BILLBERY_GW» resource as target for current route.

Click *«Add»* when you are done to save settings.

12. Nexge

12.1 Introduction

Nexge switch is capable of sending the CDR's in xml format if Nexge's Billing Server is used and also capable

of sending it in hexadecimal format (Radius Packet) if the third party billing server is used with Radius interface.

12.2 Configuration details to connect to Radius Server

The configuration related to the Radius server will be available in a flat file called radius.properties; this will be available in SIPProxy folder.

For Example: The folder path will be similar to /voip/SIPProxy

Make sure the following parameters are configured properly to connect to Radius server.

Parameters	Value Type	Description
NO_OF_RADIUS_CLIENTS=1	Alpha numeric	This is used to specify number of Radius Client to enable. Maximum allowed client is 2. If the client is specified 2, then we will send Radius Authorization packet to both and based on the first response received Proxy will proceed with the call and send accounting to the same Radius from

		where it got the Authorize response.
PROXY_IP=10.10.10.1	IPv4	Used to specify the Proxy IP. This IP will be sent in the NAS IP attribute.
USER_AUTHENTICATION_REQUIRED=true	Boolean	Used to Specify whether Radius Authentication is required or not. This is applicable only for Retail Calls.
CALL_AUTHORIZATION_REQUIRED=true	Boolean	Used to Specify whether Radius Authorization is required or not. This is applicable only for both Wholesale and Retail Calls.
ACCOUNT_TIME_ZONE=UTC	Alphabet	Used to specify the Time Zone along with the system time in the Start time, Connect time and Disconnect time. There is no time conversion based on the Time Zone configured.
RADIUS_RESPONSE_TIME=2000	Numeric	Used to Specify the Radius Response time out. If there is no response from Radius for the Authorization with in the time specified then session will cleared.
SEND_NEXGE_VSA=true	Boolean	Indicates whether the accounting packet should contain Nexge Attributes or not.
SEND_H323_REMOTE_ADDRESS=true	Boolean	Indicates whether the accounting packet should contain Remote Address or not.
AUTHORIZE_INTERNAL_GW_CALL=true	Boolean	Indicates whether Radius Authorization has to be done for call from internal gateway.
SEND_STOP_ACCOUNTING_FOR_FAILED_GW=true	Boolean	Indicates whether we need to send stop accounting message for each failed gw to Radius server.
SEND_DIGEST_DETAILS_IN_NEXGE_VSA=false	Boolean	Indicates whether to send the Nexge VSA in the Digest Format.

SEND_START_ACCOUNTING_AT_INVITE=false	Boolean	Whether to send Accounting at time of INVITE or after call is Connected.
RADIUS_CLIENT_IDENTIFIER_1=NexgeGK	Alpha numeric	Indicates the client identifier which needs to be configured in the AAA.
RADIUS_SERVER_IP_1=10.10.10.20	IPv4	Radius Server IP to which AAA needs to be sent (put your VCS IP here).
RADIUS_SERVER_AUTHENTICATION_PORT_1=1812	Numeric	Radius Server Authentication Port, to which Authentication will be sent.
RADIUS_SERVER_ACCOUNTING_PORT_1=1813	Numeric	Radius Server Authorization Port, to which Authorization will be sent.
CALL_REAUTHORIZATION_REQUIRED_1=false	Numeric	By enabling or disabling this field SIPProxy will decide whether to go for Reauthorization or not once the permitted time exceeds.
REAUTH_BUFFER_TIME_1=2000	Numeric	Based on this value, Reauthorization will be sent to Billing system at the time of Permitted time minus ReAuth Buffer time value defined here is reached. This will work only if the above parameter is set. Time need to be defined in Milliseconds.
NO_OF_RETRANSMISSIONS_1=10	Numeric	By enabling this, Accounting will be sent more than once based on the value defined if there is no ACK for Accounting.
ACCOUNT_RETRY_TIME_1=5	Numeric	Indicates duration between one Accounting packets to the other if there is no ACK for Accounting. Time need to be defined in seconds. With 5, we will send accounting packets five times if no ACK response for Start and Stop.
SHARED_SECRET_1=secret	Numeric	Secret which needs to be sent in the Authorization request.

SEND_MODIFIED_DEST_NUMBER_FOR_AUTHORIZATION_1=false	Numeric	Whether to send the Original Dialed number or the Modified number(dialing number sent to carrier).
SEND_ACCOUNTING_INFO_TO_RADIUS_SERVER_1=true	Numeric	Whether to send Accounting to Radius or not.
SEND_START_ACCOUNTING_INFO_TO_RADIUS_SERVER_1=true	Numeric	Whether to send Start Accounting to Radius or not.
SEND_STOP_ACCOUNTING_INFO_TO_RADIUS_SERVER_1=true	Numeric	Whether to send Stop Accounting to Radius or not.

12.3 Configuration details to connect to Redirect server

The configuration related to the Redirect server will be available in a flat file called *route.properties*; this will be available in SIP Proxy folder.

For Example: The folder path will be similar to /voip/SIPProxy

Make sure the following parameters are configured properly to connect to Redirect server.

Parameters Value	Type	Description
NUMBER_OF_REDIRECT_SERVERS=1	Numeric	This is used to specify number of Redirect servers.

redirectServer<Number>=<Seq. No>-<Redirect Server Name>-IP-Port-Priority-Cost

E.g.: redirectServer1=001-VCSREDIRECT-10.10.10.30-5065-0 (put your VCS IP and port here)

Parameters Value	Type	Description
Seq. No	Numeric	Indicates Sequence Number, this is unique value.
Re-Direct Server Name	Alpha	Indicates the Redirect server name.

	numeric	
IP	IPv4	Redirect Server IP, through which call will be terminated to get the Termination details.
Port	Numeric	Redirect Server Port to which call will be sent.
Priority	Numeric	If there are multiple Re-Direct Server and if different Priority is set, then SIP Proxy routes the call on a Redirect server which has the least 'priority' value. If it fails then SIP Proxy route through next priority.
CONTINUE_ROUTING_AFTER_REDIRECT_COMPLETION=true	Numeric	Indicates whether we have to failover to the configured Termination gateway in the external gateway configuration, if the Redirect server doesn't return the gateways.
ENABLE_DEFAULT_ERROR_CODE=true	Boolean	Indicates whether the error codes configured in the below field should be taken for gateway failover while getting multiple contacts from the Redirect server.
errorCodeString=400_404,480,487,500_505,600_603	String	Indicates to failover to next gateway if the configured error code is returned by the available gateways.

13. Freeswitch

13.1 Integration via CDR-files

To properly integrate with uploading of CDR-files, you are required to perform a specific configuration on Freeswitch side. This configuration consists of few simple steps provided below.

1) Open CDR configuration file, which can be found under following path:
/usr/local/freeswitch/conf/autoload_configs/cdr_csv.conf.xml

Make sure, that contents include the following:

```
<configuration name="cdr_csv.conf" description="CDR CSV Format">
<settings>
<!-- 'cdr-csv' will always be appended to log-base -->
<!--<param name="log-base" value="/var/log"/>-->
<param name="default-template" value="jerasoft_vcs"/>
<!-- This is like the info app but after the call is hung up -->
<!--<param name="debug" value="true"/>-->
<param name="rotate-on-hup" value="true"/>
<!-- may be a b or ab -->
<param name="legs" value="ab"/>
<!-- Only log in Master.csv -->
<param name="master-file-only" value="true"/>
</settings>
<templates>
<template name="jerasoft_vcs">"${uuid}","${bleg_uuid}","$
{network_addr}","$
{sip_to_host}","${sip_gateway_name}","${caller_id_number}","$
{destination_number}","${sip_to_uri}","${start_stamp}","$
{answer_stamp}","${end_stamp}","${billsec}","${hangup_cause}","$
{progresssec}","${read_codec}","${write_codec}","${direction}","$
{digits_dialed}","${provider}","${progress_mediasec}"</template>
```

```
</templates>
</configuration>
```

2) Important parameters that you should pay attention to are:

```
<param name="legs" value="ab"/>
<param name="master-file-only" value="true"/>
```

and

```
<templates>
<template name="jerasoft_vcs">"${uuid}","${bleg_uuid}","$
{network_addr}","$
{sip_to_host}","${sip_gateway_name}","${caller_id_number}","$
{destination_number}","${sip_to_uri}","${start_stamp}","$
{answer_stamp}","${end_stamp}","${billsec}","${hangup_cause}","$
{progresssec}","${read_codec}","${write_codec}","${direction}","$
{digits_dialed}","${provider}","${progress_mediasec}"</template>
</templates>
```

These lines effectively set processing of both call legs and cdr format respectively.

3) After changes to config file are made, please restart Freeswitch by using *restart* command from following path: */etc/init.d/freeswitch*

4) Setup file rotation to be executed once every 30 minutes. To do that, you will require a password, which is stored in *event_socket_conf.xml* file under following path: */usr/local/freeswitch/conf/autoload_configs/event_socket.conf.xml*

This file's contents may be similar to following, where your password value is *"xxxxx"*:

```
<configuration name="event_socket.conf" description="Socket Client">
<settings>
<param name="nat-map" value="false"/>
<param name="listen-ip" value="0.0.0.1"/>
<param name="listen-port" value="8021"/>
<param name="password" value="xxxxx"/>
<!--<param name="apply-inbound-acl" value="lan"/>-->
```

```
</settings>
</configuration>
```

5) After acquiring a password, create *freeswitch-cdr-rotate* file and put it under */etc/cron.d/* folder. This file's contents should be the following:

```
0,30 * * * * root /usr/local/freeswitch/bin/fs_cli -p xxxxx -x 'cdr_csv
rotate'
```

Where *"xxxxx"* is the password you got from previous step.

6) Your Freeswitch CDR-files integration should be finished, if you already have performed settings on VCS side, which are described in section 2.1 of this manual. If you didn't – perform those configurations (use files collector named *"Freeswitch (MIND format)"*).

13.2 Integration via SIP Redirect/RADIUS

This integration will provide you with Dynamic Routing and Authorization features through VCS SIP Redirect and RADIUS servers. To integrate properly, you are required to perform few steps:

1) Perform FreeSwitch installation per installation guide, that may be found here: *http://wiki.freeswitch.org/wiki/Linux_Quick_Install_Guide*

   Pay attention to *"Edit modules.conf"* step, where you need to add following line to file:

```
xml_int/mod_xml_radius
```

2) Move following file from VCS server to FreeSwitch server:

   /usr/local/vcs/share/extra/freeswitch/freeradius-client-1.1.6.tar.gz

   Unpack it and run following commands from main folder of this archive:

```
./configure
make
make install
```

3) Completely delete folder of */usr/local/freeswitch/conf* on FreeSwitch server and place folder of */usr/local/vcs/share/extra/freeswitch/conf* taken from VCS server on that location. Take note, that if Freeswitch was not installed in default directory (*/usr/local/freeswitch*), it is required to open file */usr/local/freeswitch/conf/dictionatires/dictionary* and specify relevant paths in following rows:

```
$INCLUDE /usr/local/freeswitch/conf/dictionaries/dictionary.cisco
$INCLUDE /usr/local/freeswitch/conf/dictionaries/dictionary.rfc5090
```

4) Open file */usr/local/freeswitch/conf/autoload_configs/xml_radius.conf.xml* and specify relevant IP addresses, ports and RADIUS secret in following format:

<ip-of-vcs>:<auth-acct-port>:<radius-secret>

Search for strings that look like these and correct them:

```
127.0.0.1:1812:secret
127.0.0.1:1813:secret
```

Also, search for string of:

```
<param var="sip_to_host" regex="^127\.0\.0\.1" anti="true"/>
```

And change *127\.0\.0\.1* to VCS IP address in exactly same format.

5) This concludes RADIUS integration. If you would like to utilize Dynamic Routing via SIP Redirect server, do the following. On Freeswitch server, open files: */usr/local/freeswitch/conf/default/30_routing.xml* and */usr/local/freeswitch/conf/public/30_routing.xml* and specify VCS IP address instead of 127.0.0.1

6) Run command: mkdir /var/run/freeswitch/

7) In file */usr/local/freeswitch/conf/autoload_configs/acl.conf.xml*

add this:

```
<node type="allow" cidr="0.0.0.0/0" />
```

it allows traffic for all IP's in the world. Maybe it's a good idea to have it restricted to IP's of your customers, but that is up to your preference.

Important: the RADIUS collector type you need to choose for this integration is ***"Jerasoft VCS Common"***. If you choose other collector, integration will not function properly.

Appendix 1. Nextone special notes

Client setup

All Nextone switches create CDR-files based on call *setup time*, so it is advised to set all your clients in VCS to be billed by setup time. To do this, go to VCS *Management – Clients* section, open client properties and set *Bill Calls By = Setup Time.*

Nextone Radius stability issues

It has come to our attention that in some cases RADIUS capability of Nextone switches is very unstable, which causes constant crashes and other critical issues on Nextone server. Therefore, please attempt RADIUS integration at your own risk and only when you know what exactly you are doing and are capable of resolving mentioned issues, if they will be present.

In case you see the mentioned stability issues with Nextone server, it is strongly advised to contact Nextone support team to work out means of improving Nextone RADIUS stability.

To turn on RADIUS on your Nextone box, please do the following.

Open your iServer Configuration utility, go to *Billing* tab and make sure all settings match the data on provided screenshot (Figure 26).

Pay attention to the following fields:

- **Billing Type** – select *ciscoprepaid* value;
- **First User** – specify first user login;
- **First password** – specify first user password;
- **Leg 2 End** – enable this option;
- **Primary Server** – specify VCS server IP in this field;

- **Primary Secret** – specify secret in this field;
- **Send RADIUS Accounting Messages** – enable this option;
- **Enable POD** – enable this option;
- **Use IP Ani Auth** – enable this option.

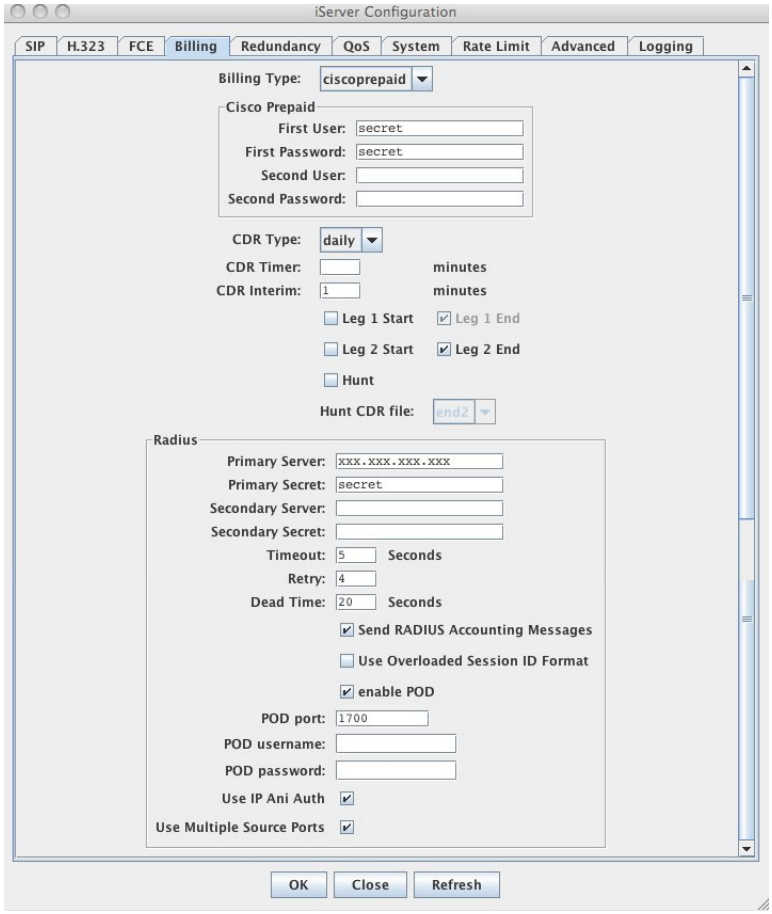

Figure 26: Nextone RADIUS parameters

Active Calls

Another possible issue concerning Nextone's RADIUS is provisioning of Active Calls. Unfortunately, in some cases, Nextone sends excessive amount of RADIUS START packets. Usually every single call is initiated by single START packet, and closed by respective STOP packet. In this case we can see that sometimes there are two or more START packets and only single STOP packet sent, which means that your Active Call will have one or more additional

instance of already existing call opened and not closed afterwards. If you encounter this issue, please contact Nextone support team for resolving the issue and prevent excessive START packets from being sent.

It is strongly recommended to purchase Nextone Active Calls Module, with spec means that allow to pull active calls from Nextone database, without using RADIUS start/stop packets.

Statistics display specifics

Usually, when you go to *Statistics – Summary Report* section of your VCS and query a report, similar periods of data for origination and termination should match (for example, total daily origination minutes will be equal to total daily termination minutes). In some cases, when processing Nextone CDR-files, you will see a mismatch on those figures. This happens because or Nextone's internal default rounding of origination and termination calls durations. The reason of different rounded call duration figures is the following: termination is disconnected after origination, creating a small delay, thus, for example, origination leg session time is 13,49 seconds, and termination is 13,51 seconds. After rounding you will see that origination is 13 seconds, and termination is 14 seconds, thus creating a mismatch between total origination and termination time.

Due to nature of this mismatch, it will be barely noticeable (around 0,5% difference).