

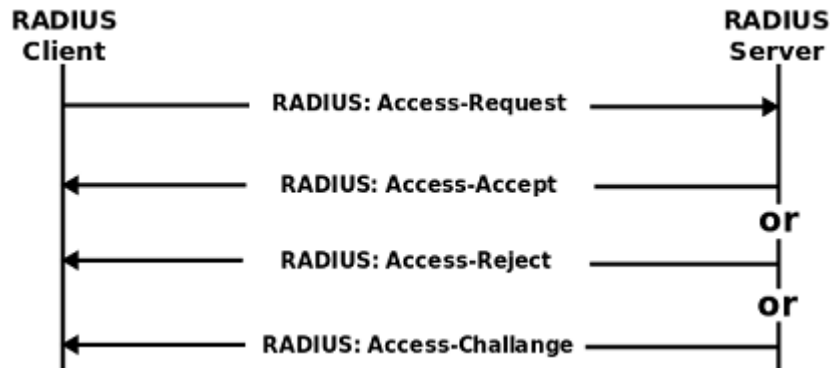
# RADIUS Connectivity

## Overview

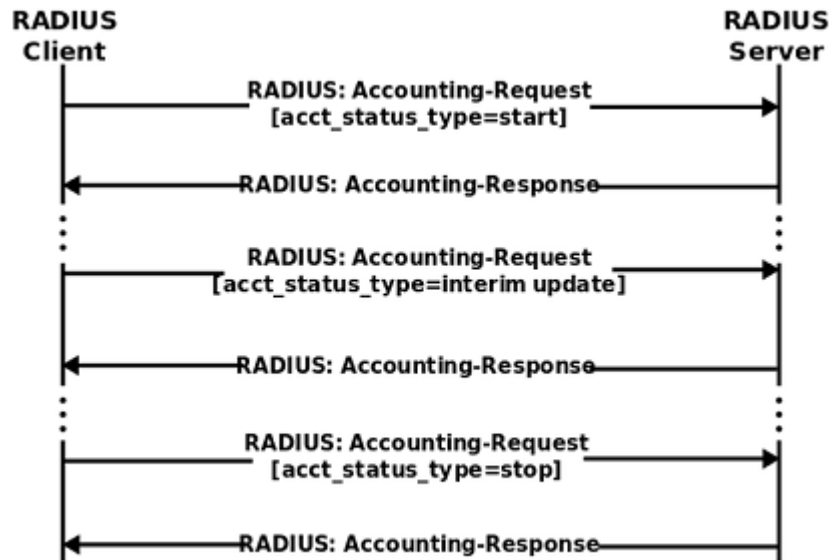
**Remote Authentication Dial In User Service (RADIUS)** is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service.

NSC has built-in RADIUS client function, with which you can easily connect to your existing RADIUS services. (NSC doesn't provide RADIUS server function)

RADIUS Authentication and Authorization Flow:



RADIUS Accounting Flow:



## Configuration

Go to **"Configuration -> Signalling -> RADIUS"**, edit the **"RADIUS Configuration"**;

**RADIUS Configuration**

Radius Server Address	<input type="text" value="192.168.100.25"/>
Authentication Port	<input type="text" value="1812"/>
Radius Shared Secret	<input type="text" value="testing123"/>
Authentication Realm	<input type="text"/>
Radius Timeout	<input type="text" value="10"/>
Request Retries	<input type="text" value="3"/>
Bind Local IP address	<input type="text" value="eth1 - 192.168.100.30"/>
Radius Server Accounting	<input type="text" value="Enable"/>
Radius Accounting Port	<input type="text" value="1813"/>

Save Cancel

- You just need to simply configure the following items:
  - "Radius Server Address"**: FQDN or IP address of RADIUS service (Note: we only support one RADIUS profile now, so only one address can be configured);
  - "Authentication Port"** and **"Radius Accounting Port"**: Usually Authentication and Authorization work on port 1812, and Accounting works on port 1813;
  - "Radius Shared Secret"**: This is the secret to protect the connection itself, please get it from RADIUS administrator;
  - "Bind Local IP Address"**: From which local NIC to send out the RADIUS request;
  - When Authentication/Authorization service is needed:
    - Make sure **"Radius Server Address": "Authentication Port"** is reachable;
    - Add corresponding routing plan rules; Authentication/Authorization can only be used from within routing plan(see next chapter);
  - When Accounting service is needed:
    - Set **"Radius Server Accounting"** to "Enable";
    - Make sure **"Radius Server Address": "Radius Accounting Port"** is reachable, or the call will be blocked; if your RADIUS Accounting Server is still not ready yet, please set **"Radius Server Accounting"** to "Disable";
    - Accounting start RADIUS message is sent to RADIUS server when call is connected, while Accounting Stop RADIUS message is sent when call is disconnected.

#### Authentication/Authorization from Routing Plan

Here below is an example of how to do Authentication/Authorization from within Routing Plan:

```
<extension name="unitest_rad-ANI-auth">
<condition field="destination_number" expression="^(601)$">
  <action inline="true" application="set" data="CALLINGNUMBER=${caller_id_number}"/>
  <action inline="true" application="set" data="USERNAME=netborder"/>
  <action inline="true" application="set" data="PASSWD=sangoma"/>
  <action inline="true" application="set" data="DIALED_NUMBER=$1"/>
  <action application="sleep" data="2000"/>
  <action application="auth_function" data="in ${DIALED_NUMBER}, in ${USERNAME}, in ${PASSWD}, out AUTH_RESULT"/>
  <action application="log" data="INFO AUTH_RESULT=${AUTH_RESULT}"/>
</condition>
</extension>
```

Out channel variable "AUTH\_RESULT" has 2 possibilities:

- "OK": received Access Accpet
- "NOK": received Access Reject

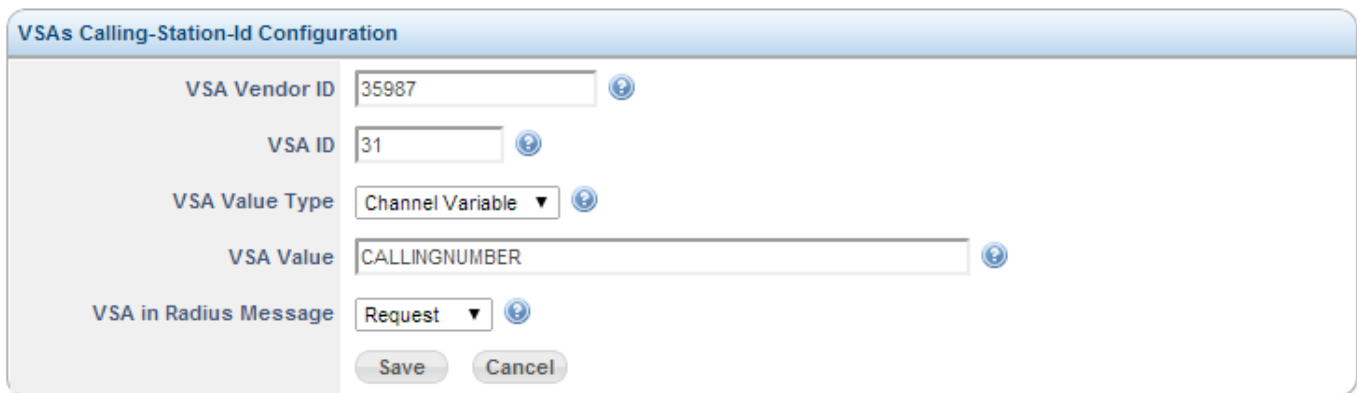
## Adding VSAs for Authentication/Authorization

For Authentication/Authorization(not for Accounting), you can define your own VSAs (in the examples below, I use Sangoma's Vender id 35987 as example; of course you can use your own Vender id):

Define VSAs in the request

E.g. Besides the mandatory "DIALED\_NUMBER", "USERNAME" and "PASSWD"; if you want to add your own VSA "Calling-Station-Id" (Vendor id: 35987, VSA id: 31, value is from channel variable "CALLINGNUMBER") in Access-Request, you can do the following:

- Go to "**Configuration -> Signalling -> RADIUS**", add the "**RADIUS VSAs**" named as "Calling-Station\_Id";



VSA Vendor ID: 35987

VSA ID: 31

VSA Value Type: Channel Variable

VSA Value: CALLINGNUMBER

VSA in Radius Message: Request

Buttons: Save, Cancel

Define VSAs in the response and use from routing plan

E.g. In Access-Accept there is a VSA id = 41, which includes the information for preferred language, you want to put it into channel variable "preferred\_lang":

- VSA Vender ID : 35987
- VSA ID : 41
- VSA Value Type : keep it untouched, which is "Direct String Input"
- VSA Value : preferred\_lang
- VSA in Radius Message : "Response"
- Here below an example of how to use it in routing plan:

```
<extension name="unittest_rad-ANI-auth">
<condition field="destination_number" expression="^(601)$">
...
<action application="auth_function" data="in ${DIALED_NUMBER}, in ${USERNAME}, in ${PASSWD}, out AUTH_RESULT"/>
<action application="log" data="INFO Preferred language of user ${USERNAME} is ${preferred_lang}"/>
</condition>
</extension>
```

## Troubleshooting

- You can easily troubleshoot RADIUS message flow by filtering wireshark pcap trace by filter "radius".
- NSC only has RADIUS client function; for RADIUS server, you can either use your existing RADIUS server, or download and install the the great open source FreeRadius from [www.freeradius.org](http://www.freeradius.org)

Here below is the screen capture of one RADIUS Accounting pcap trace:

Filter: sip || radius    Expression...    Clear    Apply    Save    myfilter    filter\_file\_open

No.	Time	Source	Destination	Protocol	Length	Info
48	3.649651	10.10.2.68	10.10.2.123	SIP/SDP	879	Request: INVITE sip:1003@10.10.2.123   , with session description
49	3.650560	10.10.2.123	10.10.2.68	SIP	370	Status: 100 Trying
50	3.652125	10.10.2.123	10.10.2.68	SIP	849	Status: 407 Proxy Authentication Required
51	3.653848	10.10.2.68	10.10.2.123	SIP	369	Request: ACK sip:1003@10.10.2.123
52	3.658335	10.10.2.68	10.10.2.123	SIP/SDP	1137	Request: INVITE sip:1003@10.10.2.123   , with session description
53	3.659179	10.10.2.123	10.10.2.68	SIP	370	Status: 100 Trying
54	3.670503	10.10.2.123	10.10.2.108	RADIUS	303	Accounting-Request(4) (id=59, l=261)
55	3.672537	10.10.2.108	10.10.2.123	RADIUS	62	Accounting-Response(5) (id=59, l=20)

▸ User Datagram Protocol, Src Port: 58074 (58074), Dst Port: radius-acct (1813)  
 ▸ Radius Protocol  
   Code: Accounting-Request (4)  
   Packet identifier: 0x3b (59)  
   Length: 261  
   Authenticator: f1b42cf1d8d3db00a34d577e80212136  
   [The response to this request is in frame 55]  
 ▾ Attribute Value Pairs  
   ▸ AVP: l=6 t=Acct-Status-Type(40): Start(1)  
   ▸ AVP: l=38 t=Acct-Session-Id(44): d34b577c-b188-4f8e-925a-1580ab99914d  
   ▸ AVP: l=6 t=User-Name(1): 1004  
   ▾ AVP: l=12 t=Vendor-Specific(26) v=NetBorder(35987)  
     ▸ VSA: l=6 t=NetBorder-Src(4): 1004  
   ▾ AVP: l=12 t=Vendor-Specific(26) v=NetBorder(35987)  
     ▸ VSA: l=6 t=NetBorder-CLID(2): 1004  
   ▾ AVP: l=12 t=Vendor-Specific(26) v=NetBorder(35987)  
     ▸ VSA: l=6 t=NetBorder-Dst(5): 1003

- VSAs for NetBorder (Vendor ID: 35987) can be found in file dictionary.sangoma
- If VSAs in RADIUS message can not be decoded correctly, maybe it is because that your wireshark does not have the correct radius dictionary, then please do the following:
  - Open Wireshark, go to "**Help -> About Wireshark -> Folders**", locate where the dictionary.sangoma should be copied to (there is a radius sub-folder which contains a bunch of dictionary.\* files);
  - Download the above dictionary.sangoma file, make sure the file name is dictionary.sangoma, and then copy into the radius sub-folder
  - Edit radius/dictionary file, add one line "\$INCLUDE dictionary.sangoma"
- If your customized VSA cannot be recognized by wireshark, just simply edit dictionary.sangoma to add the attribute