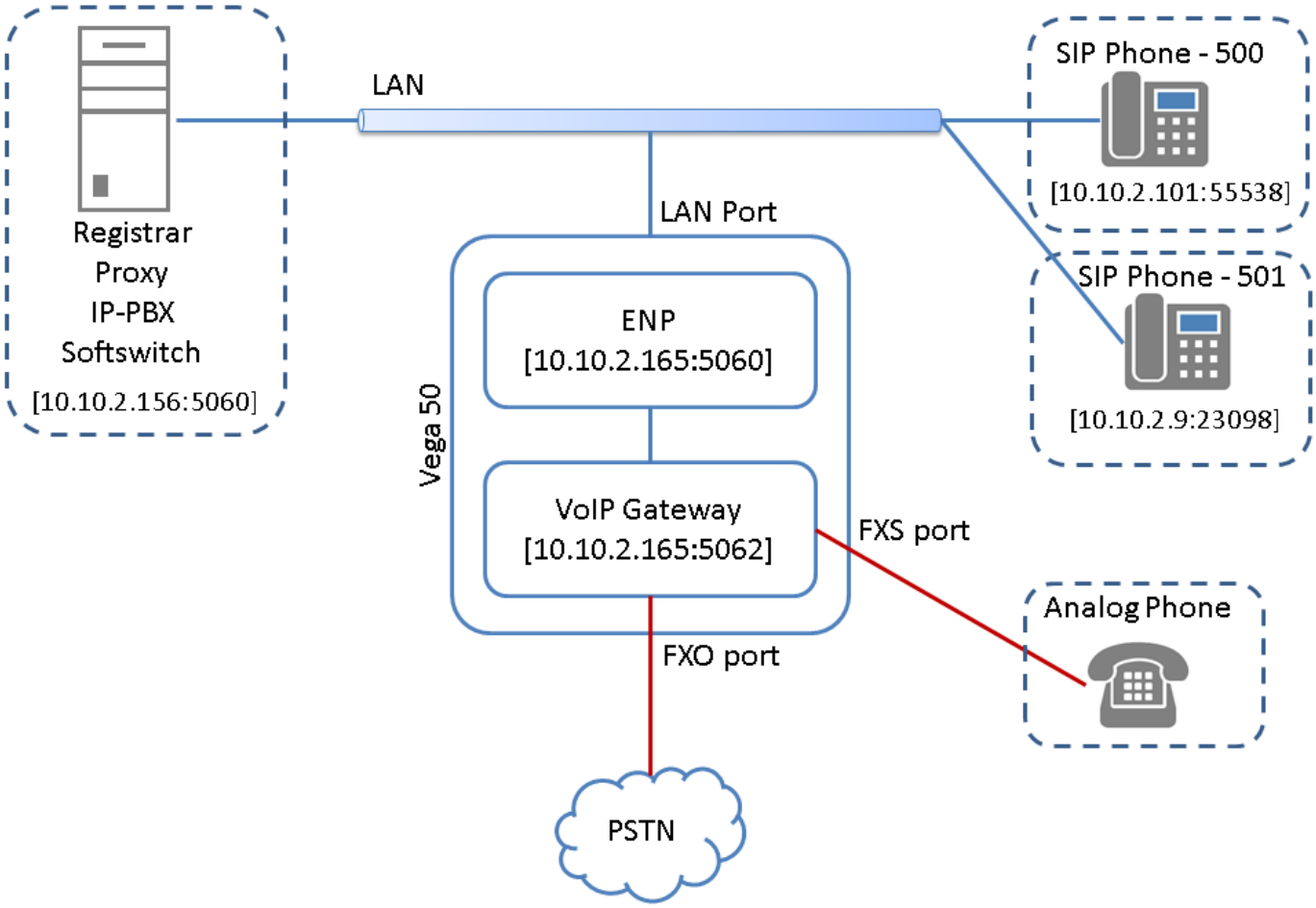
ENP

Enhanced Network Proxy (ENP)

This guide will show how to do a typical configuration of ENP. Below is the network diagram for complete details. In this setup a single subnet was used, but the same steps can be followed for a pbx in the cloud type setup where multiple subnets are involved. Also notice here that the Vega50 is shown as two entities, one being the ENP and the other being the gateway. This is because the ENP is a "service" that is separate from the Vega gateway, but shares the same hardware. As well note the port of the gateway has been changed to 5062 and the port of ENP has been changed to 5060.

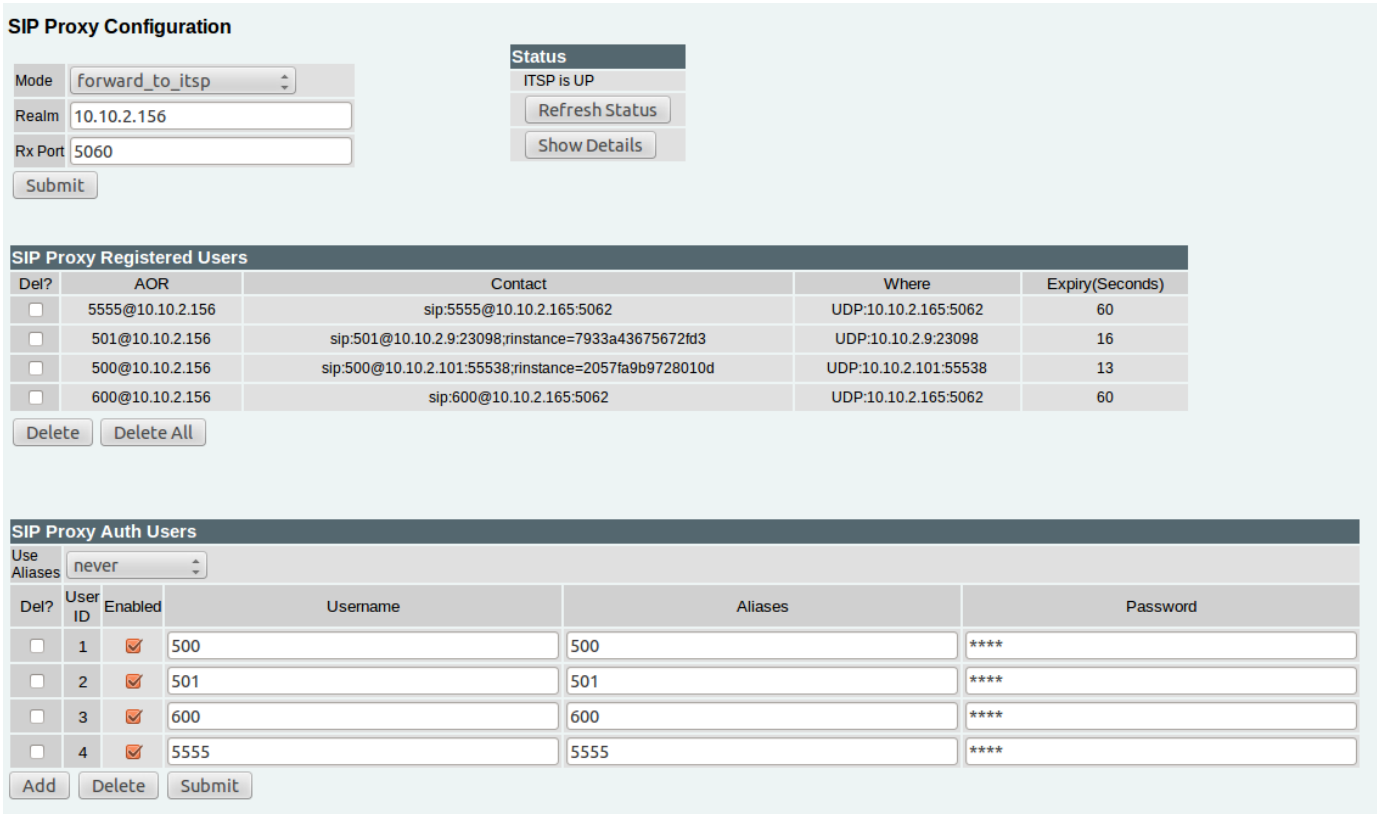
Network Diagram



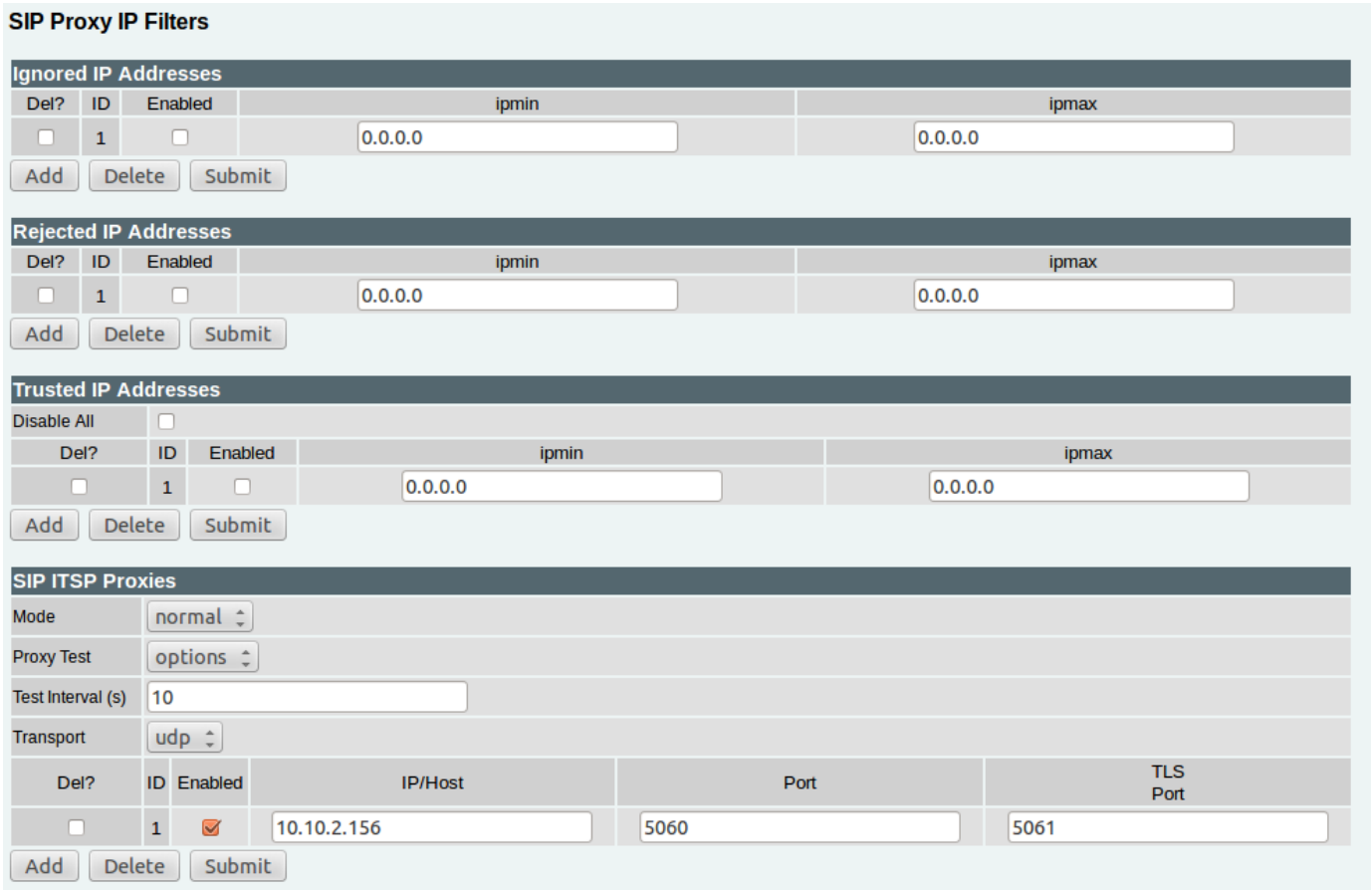
1) The first step here is to go to "**Expert Config->ENP**" and you will see the screenshot below. At this screen place the IP address of your IP PBX into the "**Realm**" field (do not put the port). Then ensure the mode is set to "**forward_to_itsp**" which forwards all messages to the ITSP. Next put each extensions username and password into the "**SIP Proxy Auth Users**" section ensuring each is enabled.

Once your extensions are registered you will see them listed in the "**SIP Proxy Registered Users**" section.

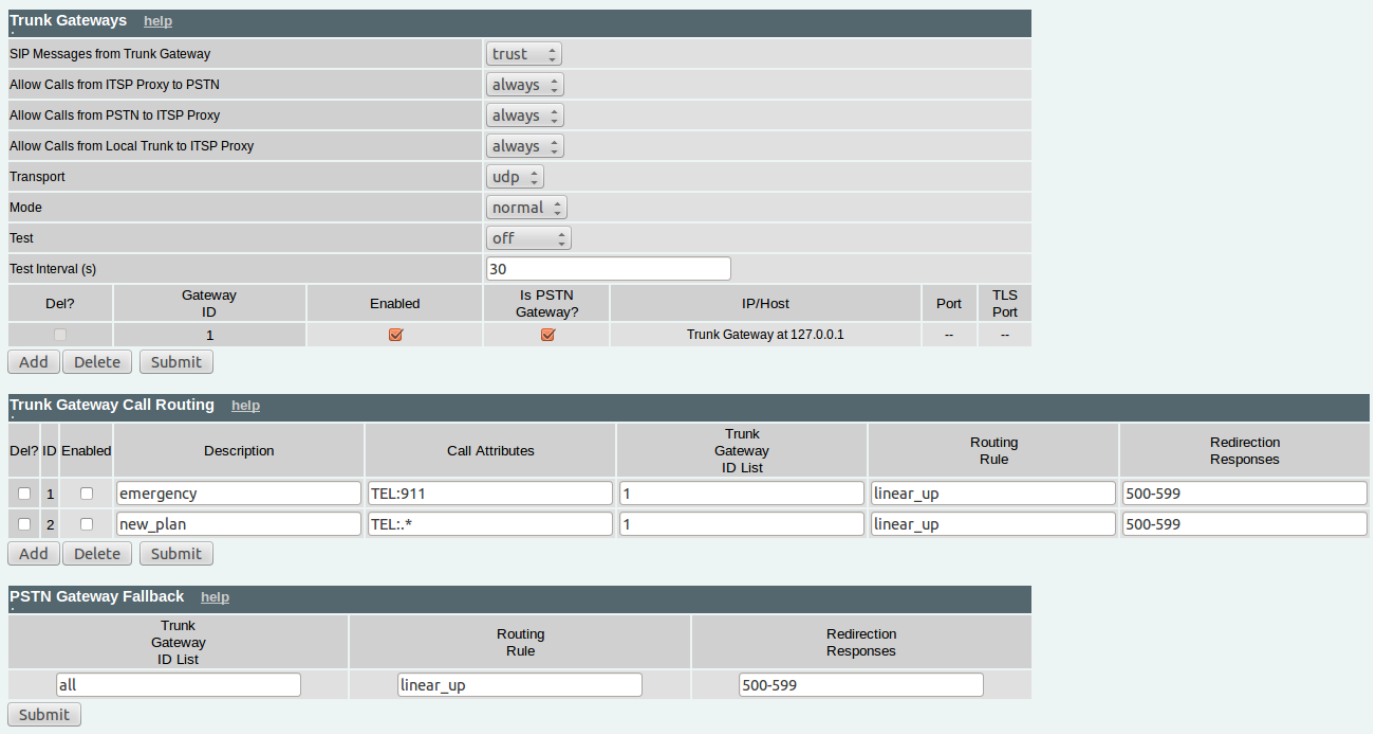
Note: If you do not want to duplicate the usernames and passwords on the Vega you can simply trust your entire subnet. This will tell the Vega to accept all registrations from the LAN without requesting a password. If the ITSP is up then a password will be requested from each phone. Only in the event of the ITSP failure will a password not be required from the specified LAN. For details on how to configure this go to http://wiki.sangoma.com/vega-configuration-enp-trust-lan.



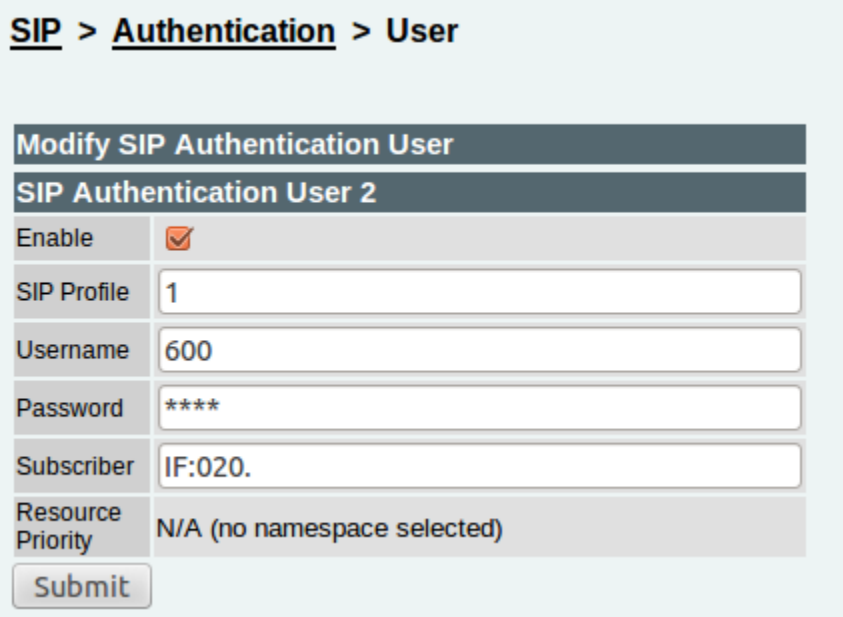
2) To continue scroll down the page until you see the following sections. You can leave the filters empty, but this can be used to whitelist and blacklist certain IPs. Now go to the SIP ITSP Proxies section and enter your IP PBX's IP and port into the fields provided. You can also decrease the test interval as shown here down to a lower value of 10 seconds. Decreasing the test interval will cause options messages to be sent to your IP PBX more often, therefore when if the IP PBX goes down ENP will know about this within 10 seconds. Also ensure proxy test is set to "**options** ".



3) Scrolling down to the Trunk Gateways section you can enable calls from to and from the PSTN, below all options are set to always to allow all directions. Next ensure the single trunk gateway is "**separate**" and check of "**Is PSTN Gateway?**", to ensure the Vega is being used as a trunk. Next you can enable (it is not enabled below) certain numbers like 911, to be dialed out the trunk gateway (FXO/PRI/BRI) directly. This is good for 911 because it will always go out the local POTS line rather than SIP. The last section should be set to "**all**" in the first column, this indicates that all trunks will be used in failover, so leave this as it is the default.

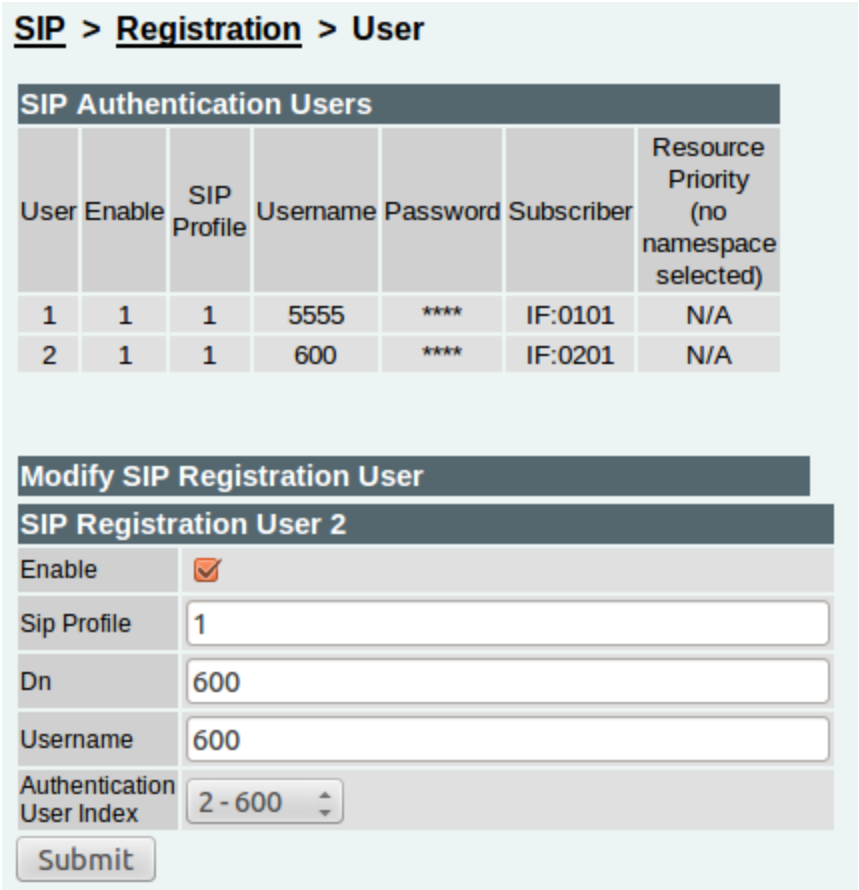


4) Next go to "**Expert Config -> SIP -> SIP Authentication**", then add a new user and click "**modify**" next to the new user. You will then be on the page shown below. Enter the user/pass that you will use to register your FXO lines to your ITSP. Ensure the subscriber is "**IF:020.**", this will allow this to be used for all FXO lines.

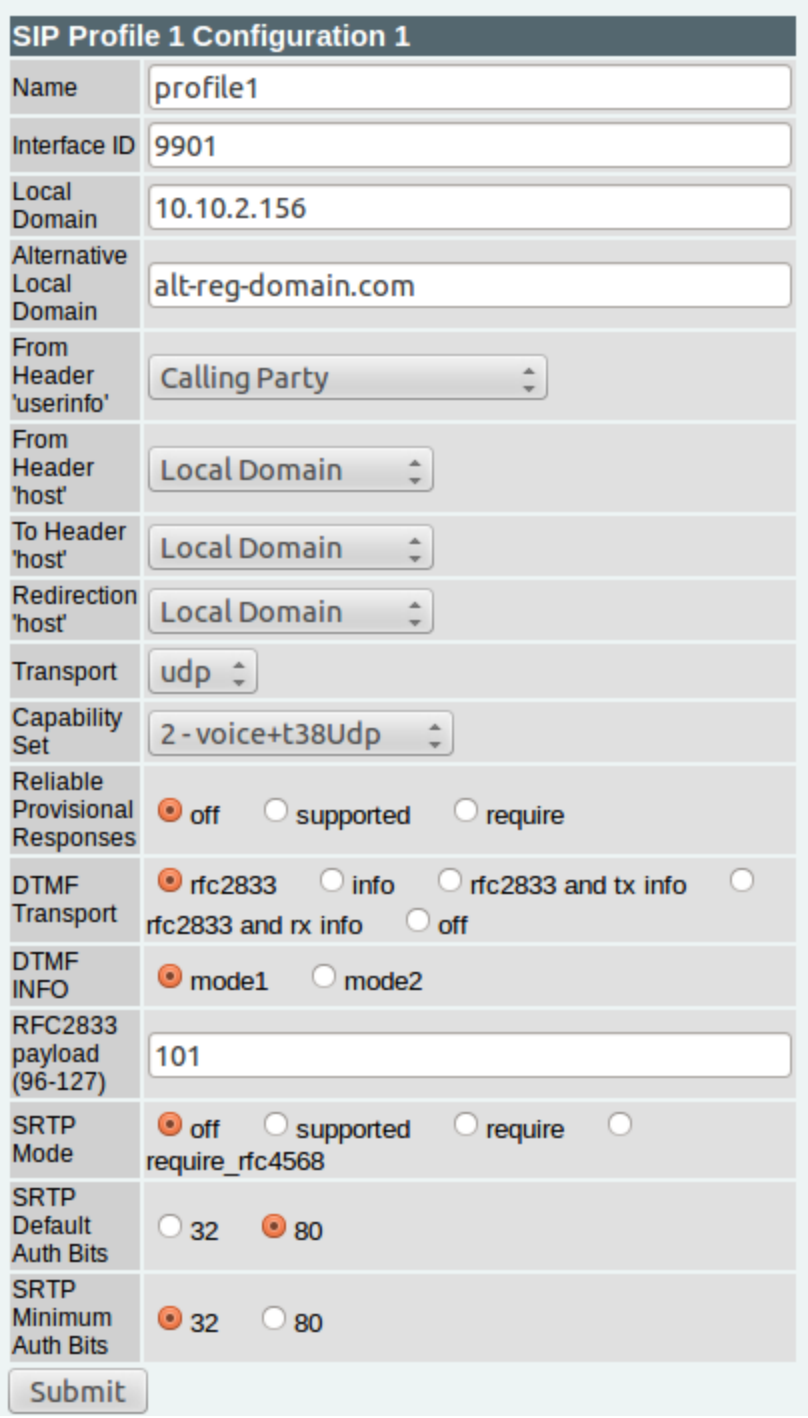


5) Next go to "**Expert Config -> SIP -> SIP Registration**" then add a new user and click "**modify**" next to the new user. You will then be on the page shown below. Enter the username in the DN and the Username field. Then select the Authentication user you have previously made in the authentication section.

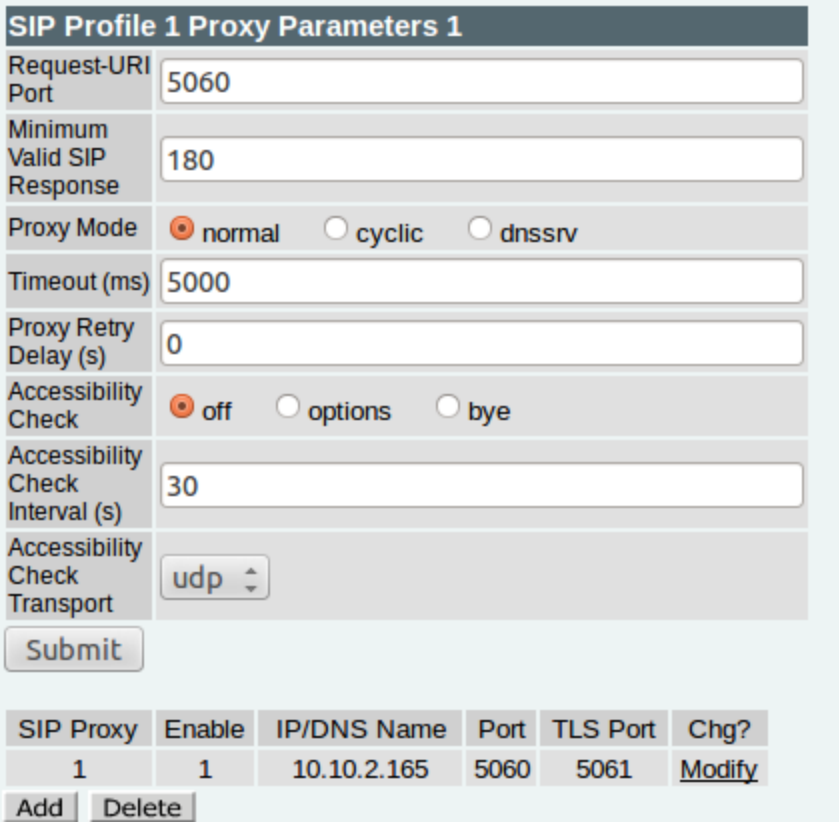
*Repeat the authentication and registration steps for any FXS devices you would like to register through ENP



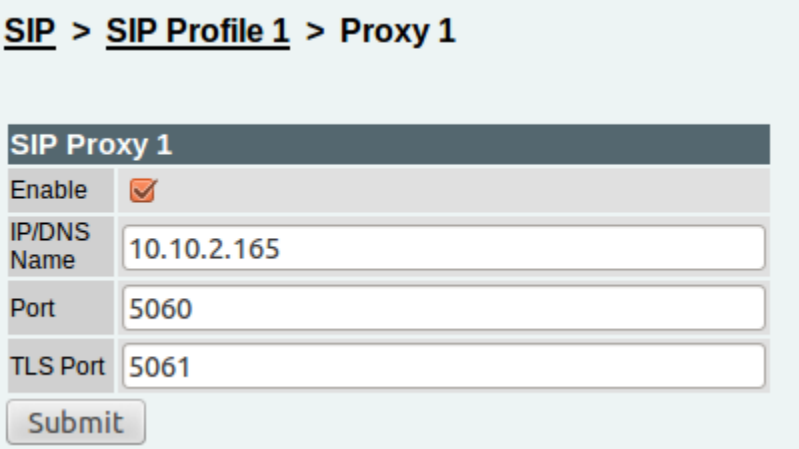
6) Now go to "**Expert Config -> SIP**" and click "**modify**" on the first profile and you will see the info below. Enter the IP address of the IP PBX into the local domain field, leave all other settings as defaults.



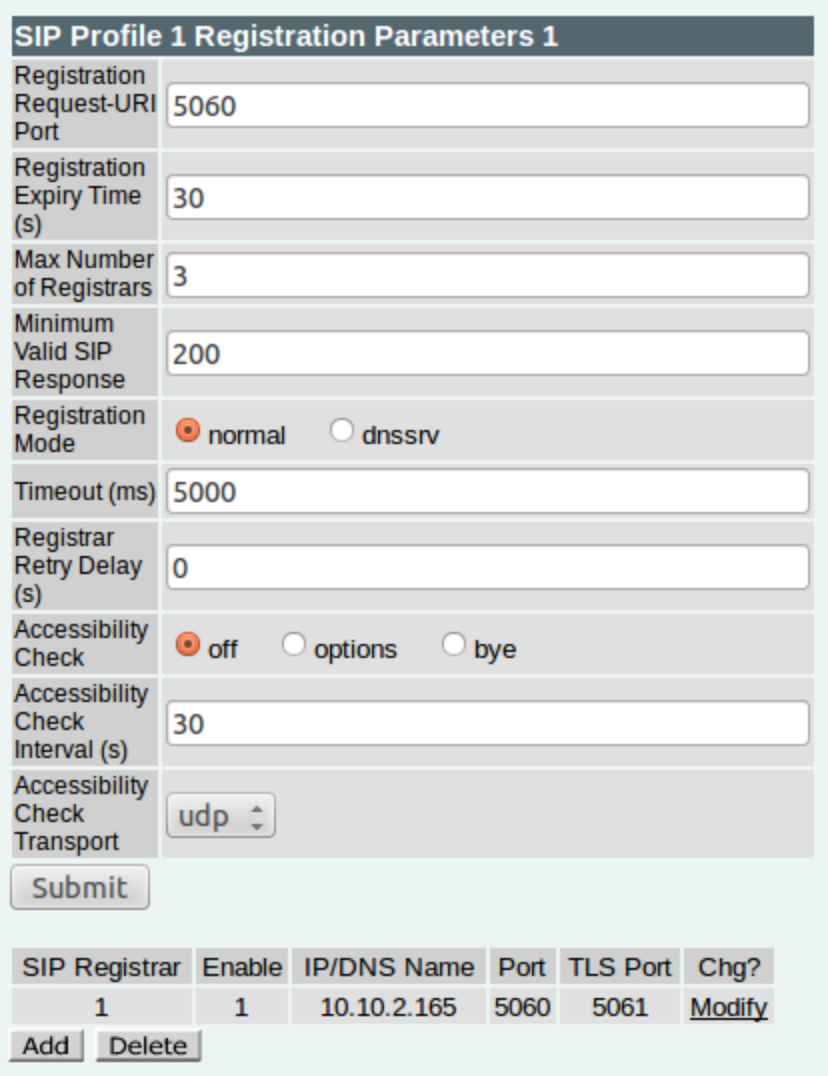
7) Next scroll down the SIP profile 1 page and until you reach the section below, click modify on the first SIP proxy.



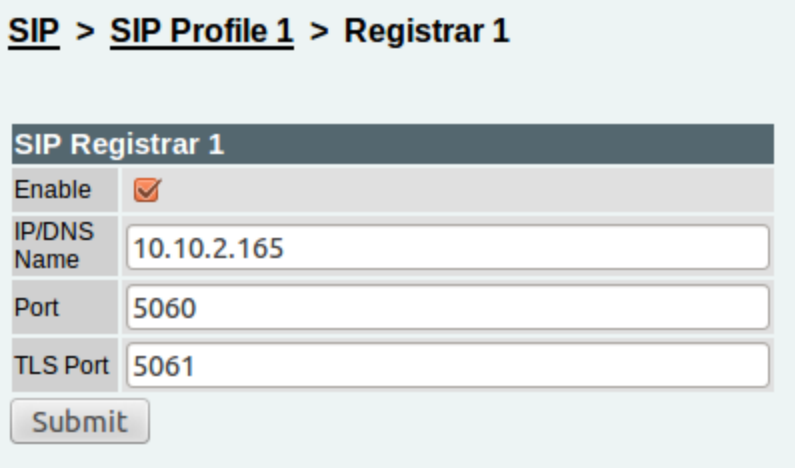
8) Now enter the IP of the Vega (which is the IP of ENP) into the field. Leave the port number at 5060.



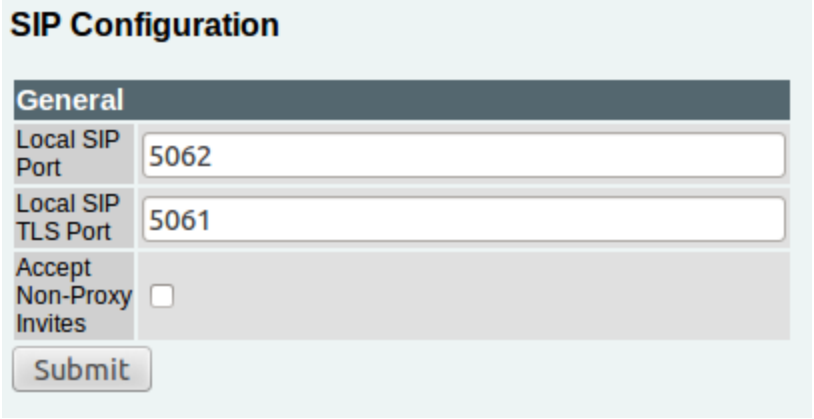
9) Scroll down the SIP profile 1 page and until you reach the section below, click "**modify**" next to the first register.



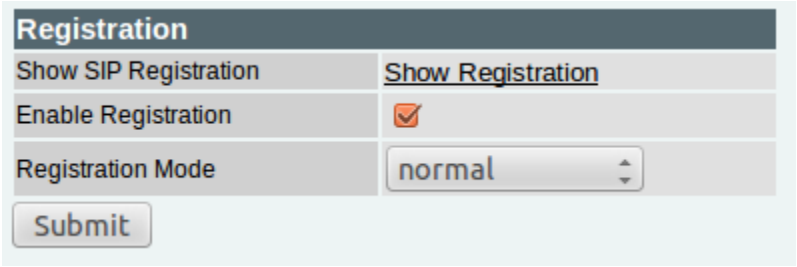
10) Now enter the IP of the Vega (which is the IP of ENP) into the field. Leave the port number at 5060.



11) Go to "**Expert Config -> SIP**" and you will see the following at the top of the page. Change the port number to "**5062**" as shown below.



12) Next in "**Expert Config -> SIP**" enable registration by checking the box shown below.



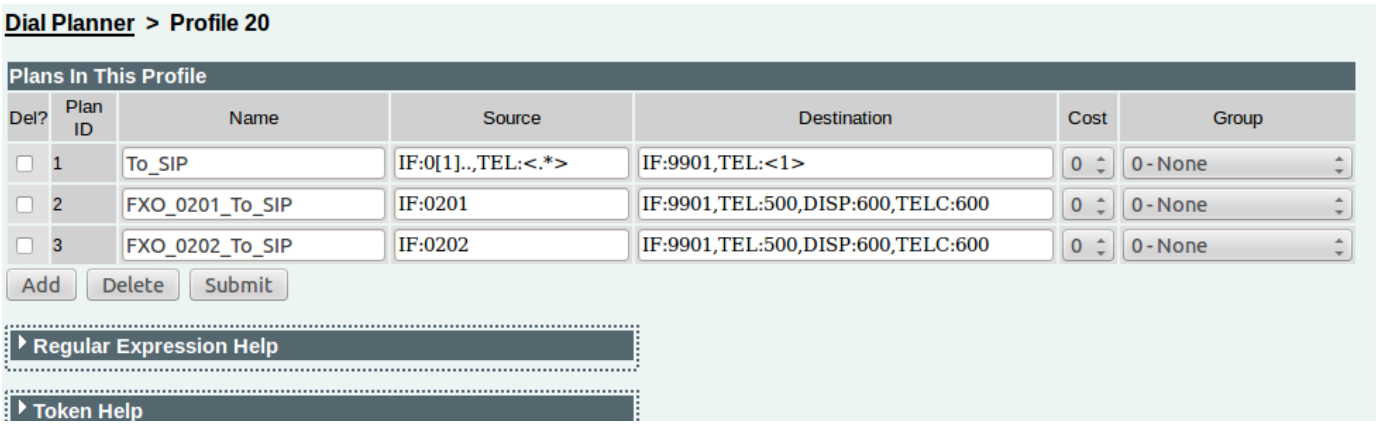
- Next go to "Expert Config -> Dial Plan" then click modify next to the To_SIP, below is an example of what it should look like.

- This is passing all calls from FXS directly to the SIP interface

- Then the last two rules are passing the call to SIP with the extension setup previously (600) as their CID info

- The important thing to note here is "500" is defined in the TEL, this will be the failover extension when the ITSP is down. So all inbound calls will go to this single extension.

- You need to ensure in your ITSP you have a route for when a call comes from "600" with the DID "500" that it should be handled as a normal inbound call. Normally this may be just routed to extension 500, which may be fine, but normally when the ITSP is up you would want to have an IVR answering inbound calls from POTS lines.



- Now the TO_FXO dial plan should look like the dial plan below, this will call out the first FXO and if busy call out the second FXO

Dial Planner > Profile 23

Plans In This Profile

Del?	Plan ID	Name	Source	Destination	Cost	Group
☐	1	FXO_01	IF:99..,TEL:<(.*)>	IF:0201,TEL:<1>	0	99 - Re-Presentation
☐	2	FXO_02	IF:99..,TEL:<(.*)>	IF:0202,TEL:<1>	0	99 - Re-Presentation

Add Delete Submit

Regular Expression Help

Token Help

- The TO_FXS dial plan should look like the one below. Currently only the first rule is being used, the others are the default rules which can be deleted if you are not using those lines.

- The first rule there just says if the call comes from SIP for the extension 5555 (FXS extension that has been setup) then route it to the first FXS port.

Dial Planner > Profile 24

Plans In This Profile

Del?	Plan ID	Name	Source	Destination	Cost	Group
☐	1	FXS_01	IF:99..,TEL:(5555)	IF:0101	0	99 - Re-Presentation
☐	2	FXS_02	IF:99..,TEL:(0102)	IF:0102	0	99 - Re-Presentation
☐	3	FXS_03	IF:99..,TEL:(0103)	IF:0103	0	99 - Re-Presentation
☐	4	FXS_04	IF:99..,TEL:(0104)	IF:0104	0	99 - Re-Presentation
☐	5	FXS_05	IF:99..,TEL:(0105)	IF:0105	0	99 - Re-Presentation
☐	6	FXS_06	IF:99..,TEL:(0106)	IF:0106	0	99 - Re-Presentation
☐	7	FXS_07	IF:99..,TEL:(0107)	IF:0107	0	99 - Re-Presentation
☐	8	FXS_08	IF:99..,TEL:(0108)	IF:0108	0	99 - Re-Presentation

Add Delete Submit

Regular Expression Help

Token Help

- At this point here everything is completed and you can save and submit and reboot the Vega to apply all the changes.

- Once the unit comes up from the reboot everything should be working great.

Limitations

ENP Ignore / reject / trust / authenticate

The ENP has a number of tables that may be configured to define how to initially handle incoming messages:

- IPs to ignore (up to 100 entries):

• Explicit blacklist of specific IP addresses and IP address ranges.

• Any SIP message from any of these addresses will be dropped and not responded to. This can help deter devices from retrying requests or attempting Denial of Service attacks.

- IPs to reject (up to 100 entries):

• Explicit blacklist of specific IP addresses and IP address ranges.

• Any SIP message from any of these addresses will be actively rejected with a 403 – Forbidden

- IPs to trust (up to 100 entries):

• Explicit whitelist of specific IP addresses and IP address ranges.

• If ITSP Registrar / Proxy is in-accessible this list specifies whether endpoint devices should be treated as trustworthy devices for registering and making calls.

- SIP Auth table (up to 120 entries):

• If the ITSP Registrar / Proxy is in-accessible and a SIP message comes from a device that is not in the ‘IPs to trust’ list, the Vega will ask for authentication before handling the message

• The SIP Auth table contains:

  - Authentication User name

  - Authentication password

  - Authentication realm (to be same as Registrar / Proxy domain)

• Failure to authenticate will result in a response 407 – Proxy Authentication Required