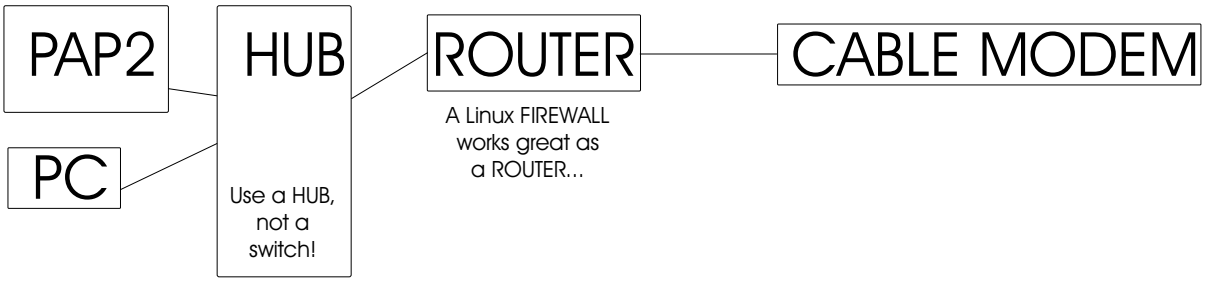
PAP2 Unlocking Guide

For firmware revisions greater than 3.1.6... (3.1.9 is current, so it may not work).



DISCLAIMER: **If you attempt this, you are doing it at your own risk! Most likely, no one will give you money, a new PAP2, or any kind of valuables when you mess up your PAP2...**

Simply put: do your research! Know what your getting into before you start!!

BEFORE plugging-in the PAP2, take the following steps for this procedure:

1. Download Sipura SPA2000 2.0.9d firmware to your PC.
2. Download the SPAtools package to your PC.
3. Disconnect your router from the Cable Modem / DSL box. (Disable INTERNET !!)

To test: from the "PC", open a web site and see if it comes up. it should NOT work!

Next step:

1. Configure your TFTP server on your LINUX router/firewall on the internal interface.
   (that means: make it work, and put the spa-pap2 and pap2-spa bin files there)
   * Remember to use SPAtools to make those files, using spa2000 2.0.9d firmware!

2. Configure your DNS to point ls.tftp.vonage.net to your LINUX box. Note that the PAP2 has two pre-set DNS servers, so you need to clear these settings from the PAP2, or it will bypass your DNS spoofing!

3. Configure your DNS to point httpconfig.vonage.net to your LINUX box (apache web server).

4. Load-up a good sniffer on your PC (remember, you are uisng a HUB, not a switch).. Configure it to monitor/sniff the packets from all but the PC (example syntax: not host 192.168.1.100)

5. Manually download your spa00000000.xml file from ls.tftp.vonage.net using a tftp client.
   NOTE: the 00000000 represents the MAC address of the unit. replace the 0's with the actual MAC.

6. Place the spa00000000.xml file in your TFTP root directory, so it can be fetched from your system.

Now, the tricky part:

7. Rename the modified firmware (the spa2000 firmware that is modified to load on the PAP2) to PAP2-bin-03-01-09-LSc.bin. **Remember: Use spa2000-2.0.9d patched firmware!**

8. Place this firmware at the root level of your apache web server (usually /var/www/html)

Feeling confident that you have your PAP2 secured (vonage spoofed properly, DNS entries REMOVED from the PAP2 web interface, and your ready to go), power-up the SNIFFER and PAP2.

If all goes well, you will see the PAP2 grab the spa00000000.xml file from your TFTP server. In that XML file, a rule instructs the PAP2 to upgrade if the firmware is not currently 3.1.9LSc.

The PAP2 will attempt to go to get http://**httpconfig.vonage.net**/PAP2-bin-03-01-09-LSc.bin.
This is where the PAP2 will be DNS spoofed to your web server, and grab the patched SPA2000.bin file, renamed as the PAP2-3-01-09 file.

If your PAP2 works, you will see the SIPURA firmware loaded when you look at the web interface.
Follow the original PAP2 PDF to complete the unlock procedure from this point!

If it did not work, use the sniffer and figure out what file name it wants to find, and rename the patched SPA2000 firmware to match what it is looking for. Verify you can get the firmware using a PC web browser..

If you have completed the above steps and are unable to 'see' the web configuration page of the PAP2, take these steps:

1. Make a new file in notepad called: spa00000000.xml (use MAC in place of 0's)
2. In this file, put:

```
<flat-profile>
  <Admin_Passwd>4321</Admin_Passwd>
  <Enable_Web_Server ua="na">Yes</Enable_Web_Server>
  <Web_Server_Port ua="na">80</Web_Server_Port>
  <Enable_Web_Admin_Access ua="na">Yes</Enable_Web_Admin_Access>
  <Protect_IVR_FactoryReset ua="na">No</Protect_IVR_FactoryReset>
  <User_Password ua="na">1234</User_Password>
</flat-profile>
```

3. Save this file into your tftp root location.
4. Power-cycle the PAP2. It will fetch the file.
5. Give it a few minutes to get the file.
6. When it is complete, try using a web browser to access the device.

The new USER password is **1234** and the new ADMIN password is **4321**

This XML file will do a couple of things; it will enable the web server, enable factory reset IVR, and change passwords for USER and ADMIN.