This guide is to help unbrick and potentially downgrade a tcp bridge. I provide no warranty or guarantee with this. Proceed at your own risk with caution. Due to the nature of differing hardware and software, this should only be used as a guide.

Firmware files can be downloaded from here: <https://www.exploitee.rs/index.php/Greenwave_Reality_Bulbs>

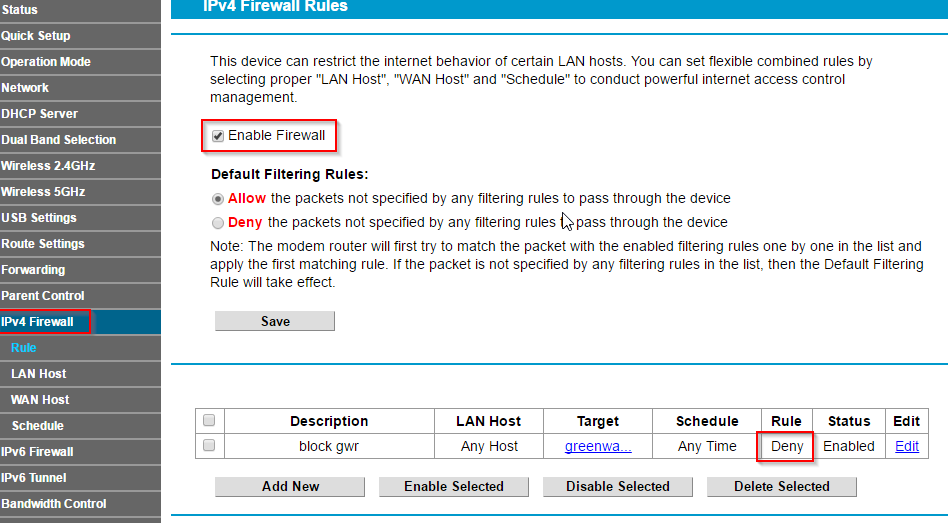
This project is based on:

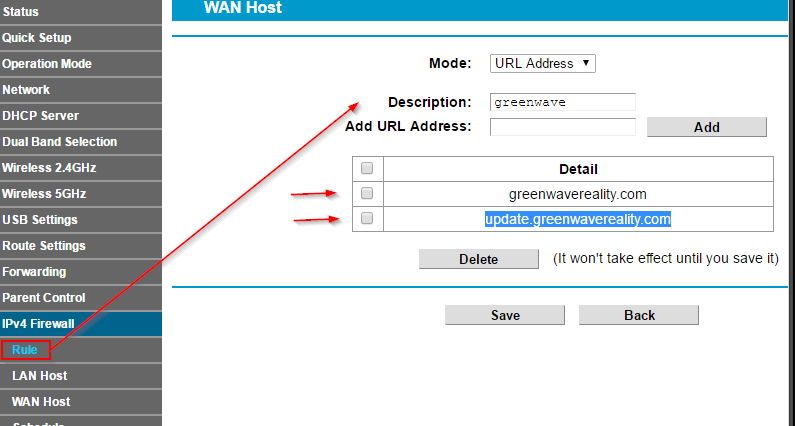
<https://github.com/hypergolic/greeenwave_firmware>

Usage instructions:

1. Download this repo from: <https://github.com/bren1818/TCPFirmwareRestore> and place it into a folder of your choice or your desktop.
2. Ensure you have python installed. You can install Python easily if you download it from ninite.com
3. Install a DNS manager of your choice or set it up yourself. I used Simpledns (<http://simpledns.com/>) on Windows. It comes as a 14 day trial which should be more than sufficient.
4. Configure your router firewall – You need to block outgoing connections to the following:
   1. greenwavereality.com
   2. update.greenwavereality.com

I cannot really document this step as there a many different routers running various firmwares. I use TP-Link as my home router, so in my IPv4 Firewall, I have added a rule called ‘block gwr’ which denies all traffic to the two urls.





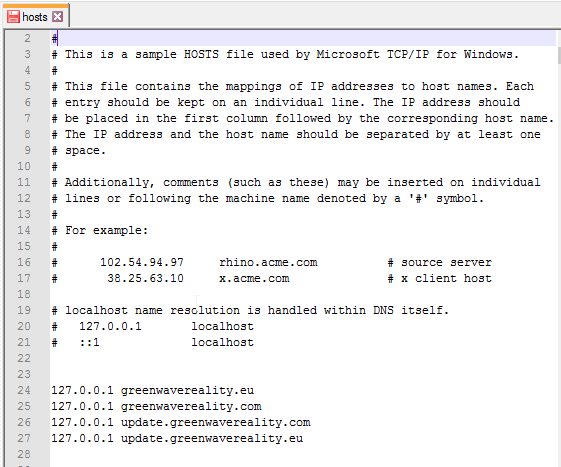
This step is **important** because otherwise, your bridge will likely update itself again, this will prevent the bridge from “phoning home”.

1. Edit your hosts file, this file lives in: C:\Windows\System32\drivers\etc on Windows. Add the following to your host file and save:  
     
   127.0.0.1 greenwavereality.eu

127.0.0.1 greenwavereality.com

127.0.0.1 update.greenwavereality.com

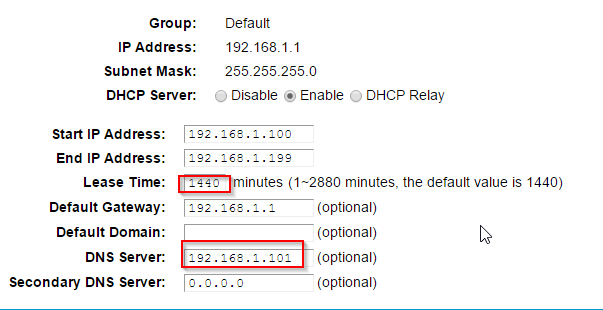
127.0.0.1 update.greenwavereality.eu

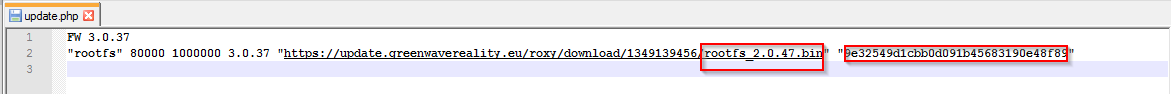


This will point local traffic to your local host machine. The reason we do this is so that the bridge checks for updates, the DNS routing will route the request to your local machine, and then your local machine will serve up the old binaries as an upgrade, even though it is a downgrade.

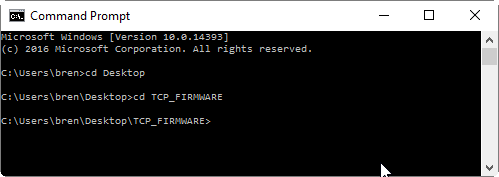
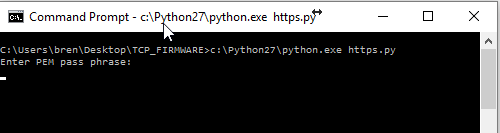
1. In your router, under the DHCP server settings – set your DNS Server to your computer’s IP address. **\*Warning\*** this will break your internet temporarily as all requests will be routed through your local host. Take note of your bridge IP and your current computers IP.

In My Scenario my bridge has the IP of **192.168.1.109**, and my desktop has the IP of **192.168.1.101**

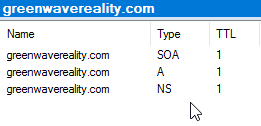
  
You may wish to change your lease time to something small – which should flush the DNS cache faster. I suggest 2 mins.

1. Edit the https.py file in this project and set the IP address on line 29 to your IP address.
2. (optional) Open up the roxy/update.php file and replace the binary and hash, with a bin/hash found in FIRMWARE FILES folder. The corresponding hashes can be found in the md5s.txt file  
   

For this project I defaulted the firmware to version 2.

1. Open up command prompt and navigate to where you checked out the files.  
   
2. Use python to run the https.py script. This will depend on how you have python installed. For Me I performed the following:  
   **c:\Python27\python.exe https.py**  
     
     
   it will prompt you for the PEM pass phrase. It is “thinkgreen”.  
     
   The server should now be listening…
3. Open up the Simple DNS trial, and create some DNS records for:

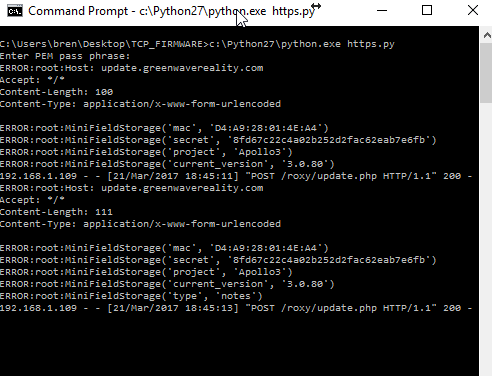
Greenwavereality.com and update.greenwavereality.com and point them to your localhost (Desktop). The ttl should be set to a low number like 1.



With your DNS pointing to your localhost, the’ performance host’ graph should be jumping around as it caches requests.

1. Reboot your bridge… (pull power cable and maybe hold sync button). when the bridge powers up, it should phone home to check for a software update, and should route to the python server you’re running. You \*\*may have to hold the sync button on your device to trigger the update. In one instance I did, in another, I didn’t.

Your command prompt window should show something like this:

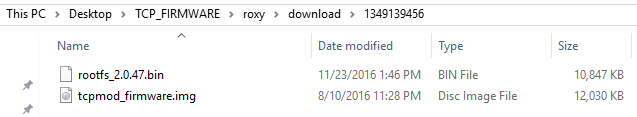


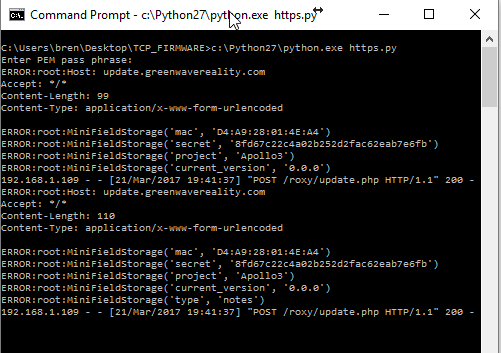
Indicating it has updated by downloading the downgrade.

You can now kill the server by pressing ctrl + c.

Here is another screenshot where I switched the firmware to hypergolics “tcpmod\_firmware.img” by modifying the update.php to:



And copied the tcpmod\_firmware.img to the roxy/download/1394139456 folder.  




Once this is complete, turn off Simple DNS, and change your DNS Server on your router back to it’s default.

In theory, your bridge should be back to an older firmware / restored.

I suggest you also check out: <https://github.com/hypergolic/greeenwave_firmware> as he was the progenitor of this code

In jurisdictions that recognize copyright laws, the author or authors of this software dedicate any and all copyright interest in the software to the public domain. We make this dedication for the benefit of the public at large and to the detriment of our heirs and successors. We intend this dedication to be an overt act of relinquishment in perpetuity of all present and future rights to this software under copyright law.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR

OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR

OTHER DEALINGS IN THE SOFTWARE.

For more information, please refer to <http://unlicense.org>