

EZmoto OpenVPN User Guide



Table of Contents

Product Description	3
Setting-up Equipment	5
OpenVPN and MODBUS installation	7
Creating Keys	9
OpenVPN network configuration	13
Modbus serial parameters configuration	16
Appendix A IP Address	17
Appendix B OpenWRT	20
Appendix C putty	23
Appendix D firewall	24
Appendix E Leds	28
Misc	29
Product Variations	29

1. Product Description

The OpenVPN Modbus has few security levels:

1) Encryption.

The OpenVPN use asymmetric keys encryption.

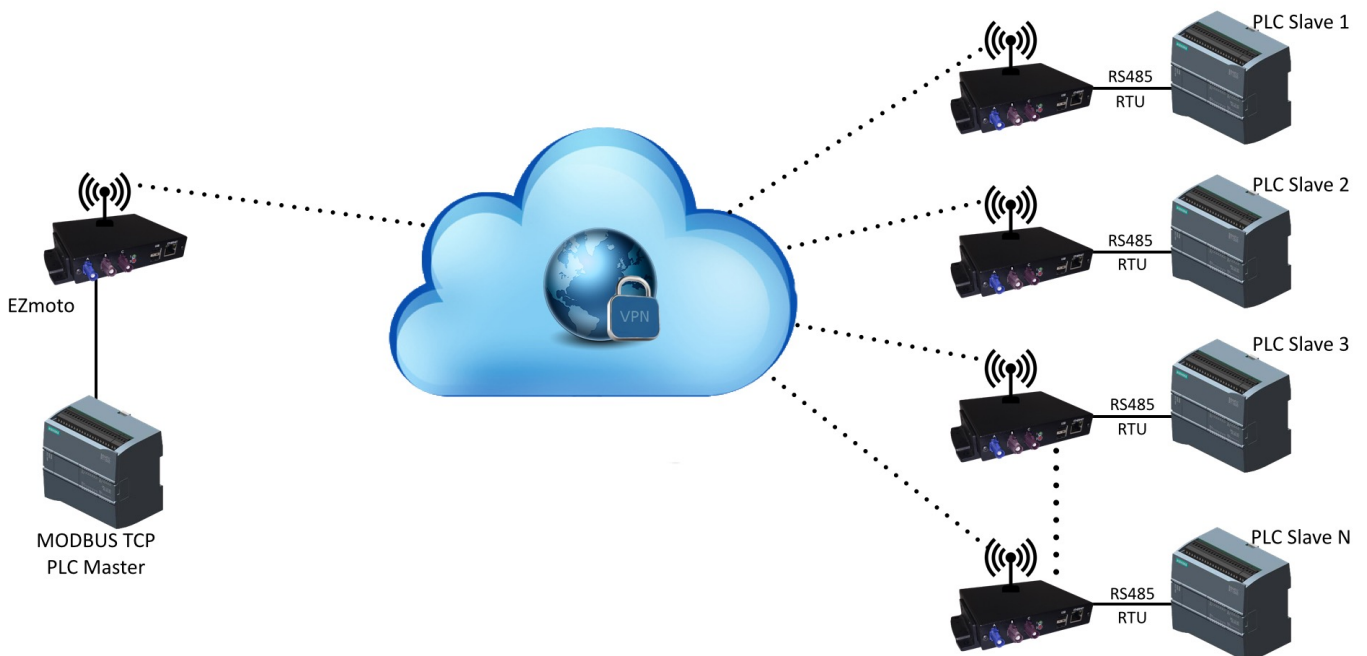
Each unit receives from the server public key and private key which are unique to the unit.

Each time the server sends a message it encrypts it with public key that can be opened with the private key that only the destined unit can decrypt.

2) Differentiate protocols.

The EZmoto client side uses RTU protocol to communicate with its controller, while the EZmoto server side uses TCP protocol to communicate with its controller, this differentiation of protocols prevents from an outside source to change parameters in client controller.

3) The EZmoto has 3 main communication interfaces: Network Wan (3g), Network LAN (Ethernet) and RTU (RS485). All 3 of them are secured, implementing a FW on the network interfaces, and a unique OpenVPN capabilities. The RTU will communicate only with a

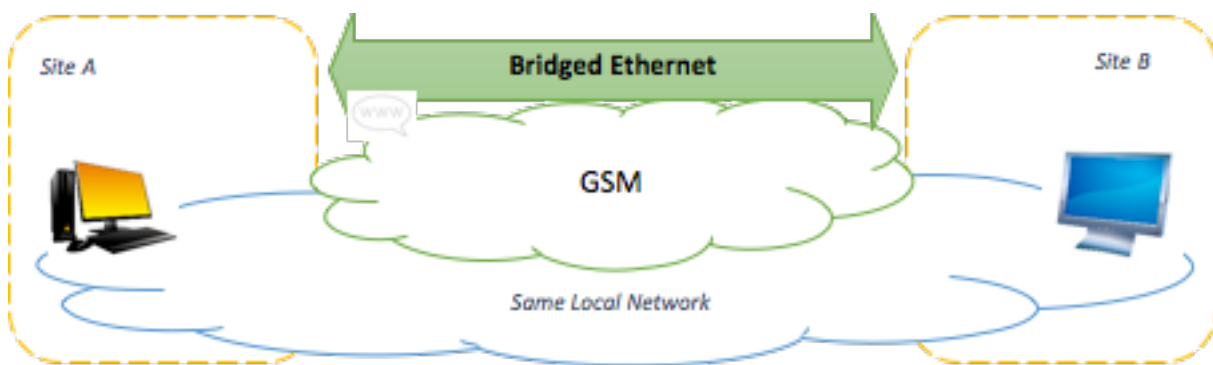


dedicated application (for example Modbus).

The EZmoto OpenVPN product allows two sites to inter-connect seamlessly as if each of them connects through a L2 switching cloud or a simple RJ45 cable.

The communication bridges through a GSM network, and encrypts the data, all the way from L2 (Ethernet frames) to L7 (User applications), allowing the safety, mobility and the use of low level communication methods (for example, L2 broadcasts / multicast frames, low level protocols, etc..).

Furthermore, if managed so by the cellular company, each may also have connection to the Internet, using its own EZmoto unit. This allows sharing the traffic load, instead of creating a bottleneck in a single site leading to the net.

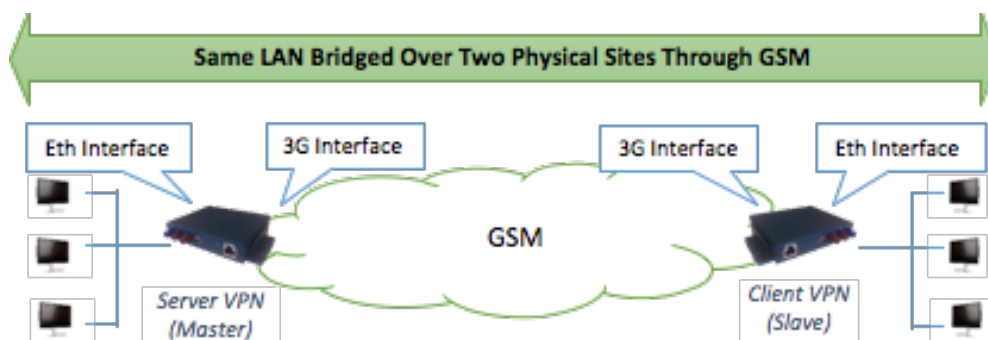


The EZmoto has two configurable IPv4 interfaces:

- 3G Interface
- Ethernet Interface

In addition, the EZmoto L2 Edge Routers divides into two types:

- Server VPN (Master)
- Client VPN (Slave)



There is always a single Server VPN EZmoto (Master EZmoto), **and it should always be up and running**, consider it as the server of this L2 GSM network.

The VPN can hold up to 20 clients.

In order for the VPN to work flawlessly, its server should have a sim card with a static PI Address, so the server would be reachable for the clients at all times.

2. Setting-up Equipment

Setting up a EZmoto unit

- 1) Insert the micro SD card to the EZmoto units.
- 2) Connect the EZmoto units to power.
- 3) Open putty with the correct com at 115200 baud rate (instructions for putty install are in section 5).

If this is the first use of the unit you need to get its IP.

To do so follow these steps:

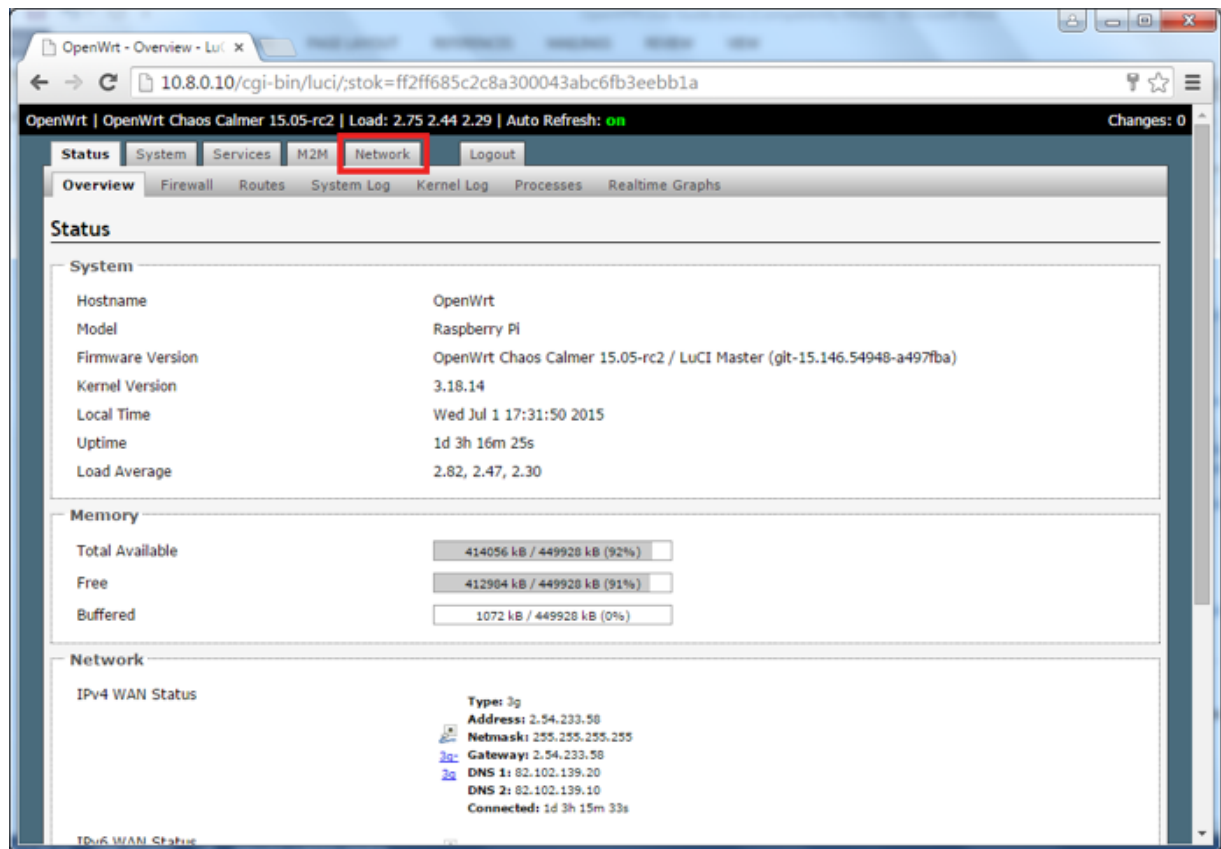
- 1) In the putty window enter the ifconfig cmd.
- 2) Check to see if br0 is present, if so write down the IP.
Otherwise write the IP address under the br-lan interface.
- 3) Do the described steps for all the EZmoto units.

APN configuration

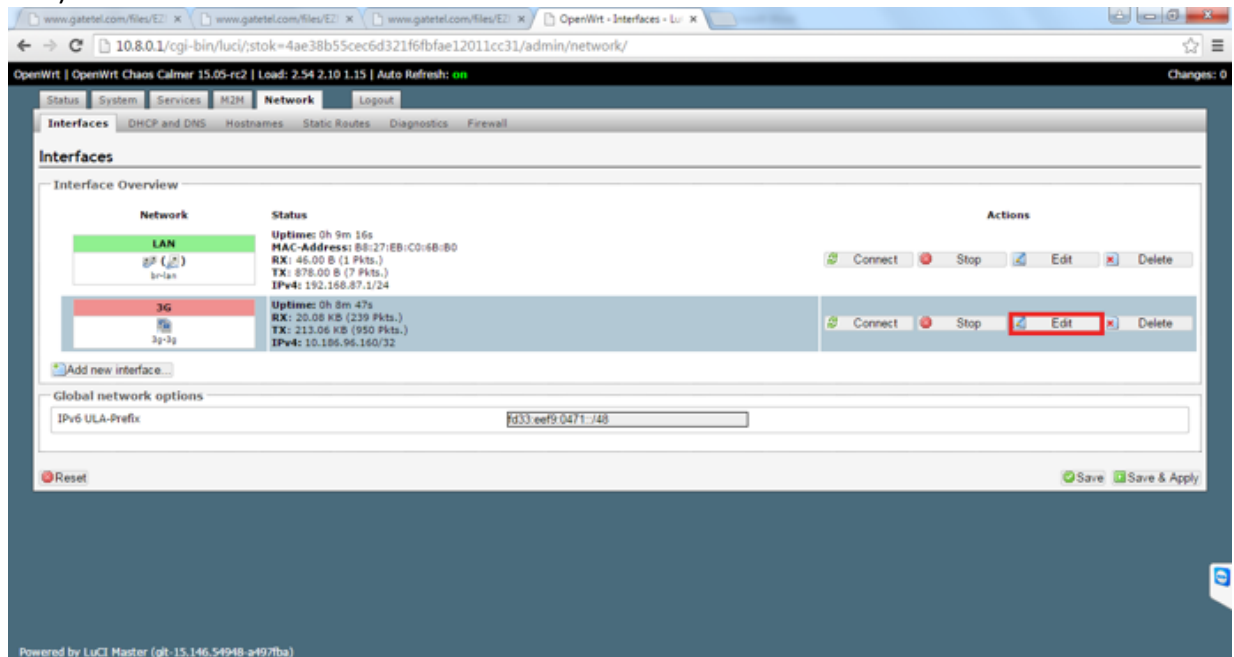
The first time setup of the Master and Slave units requires configuring the APN of both.

- 1) Connect the Ethernet cable, set-up your computer's LAN IP so it would match the EZmoto's network Address (refer to section 3 in this manual for how-to setup IP Address in your local computer).
- 2) Open the Web Browser and enter the EZmoto IP Address. Refer to appendix B for first use of the OpenWRT.

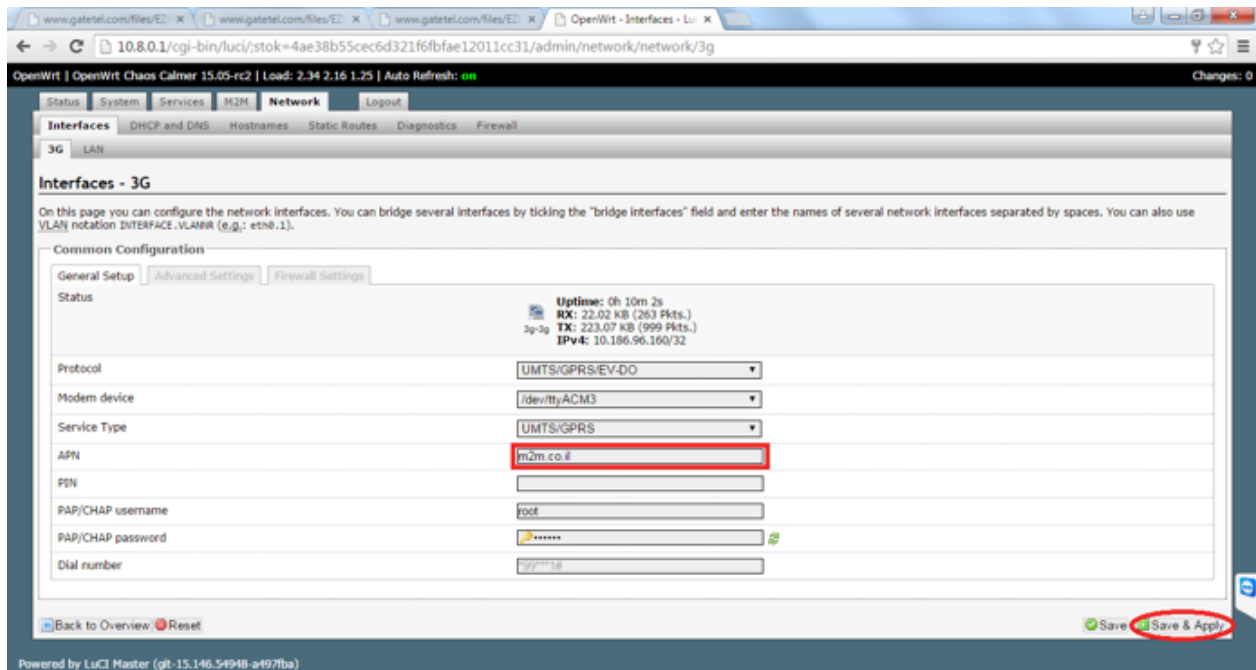
3) Open network tab



4) Edit the 3G interface



5) Enter the APN and click Save & Apply



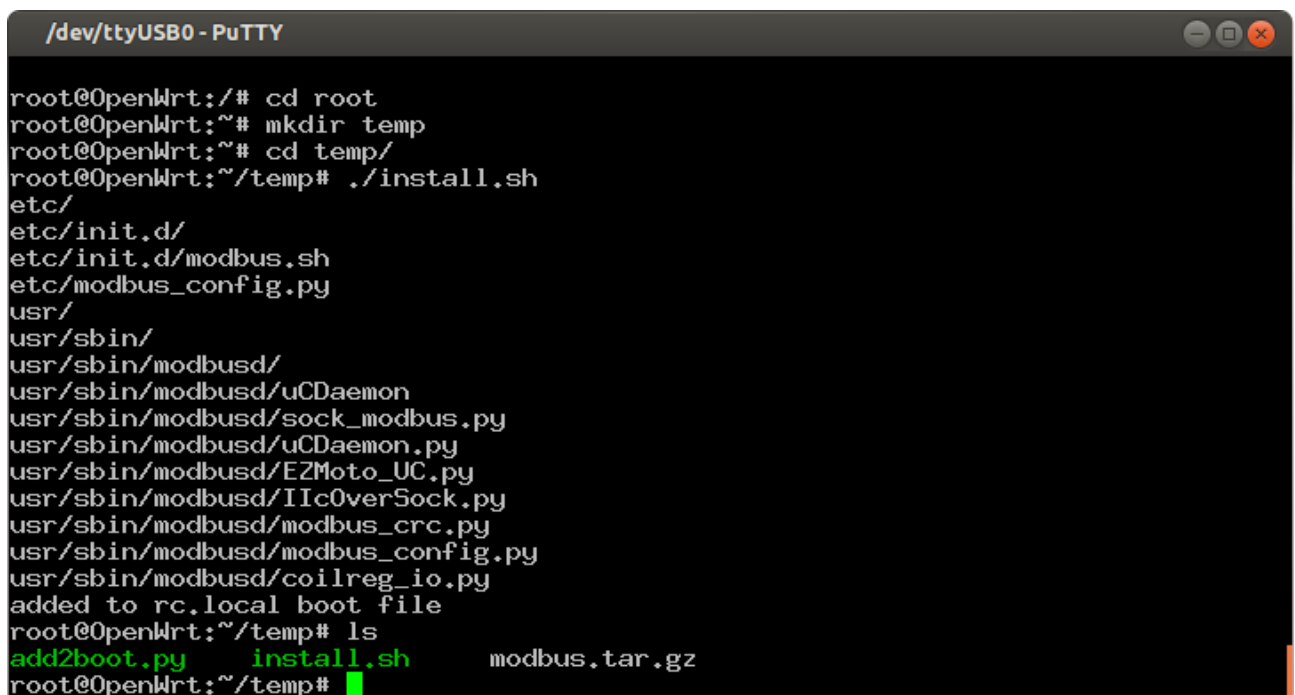
3. OpenVPN and MODBUS installation

To install the OpenVPN on the client or master follow the next steps:

- 1) Make sure you have the installation files on your computer.
- 2) Connect the EZmoto unit to the computer using the USB-RS232 cable.
- 3) Open putty (see appendix C).
- 4) Make sure the firewall is off using the following commands:
'fw3 stop' (the default password is 1-6)
'/etc/init.d/firewall disable'.
- 5) In the computer, where the installation file are, go to the directory of the installation files.
- 6) Copy the installation file using:
In windows command line 'pscp * root@ipaddress:root' (with password 1-6).
In linux terminal 'scp * root@ipaddress:root' (with password 1-6).
e.g. 'pscp * root@10.186.96.168:root'.
- 7) Go to the EZmoto unit you want to install in the OpenVPN via putty.
- 8) Add permission to the installation file enter 'chmod +x install.sh'
- 9) Install using './install.sh'
- 10) 'reboot'.

To install the MODBUS on the client follow the next steps:

- 1) Make sure you have the installation files on your computer.
- 2) Connect the EZmoto client unit to the computer using the USB-RS232 cable.
- 3) Open putty (see appendix C).
- 4) Make sure the firewall is off using the following commands:
'fw3 stop' (the default password is 1-6)
'/etc/init.d/firewall disable'.
- 5) Make a directory in root in which the installation files will be copied to using
'cd ~' and then 'mkdir <name>' e.g. 'mkdir temp'.
- 6) In the computer, where the installation file are, go to the directory of the installation files.
- 7) Copy the installation file using:
In windows command line
'pscp add2boot.py install.sh modbus.tar.gz root@clientipaddress:root' (with password 1-6, temp is the directory you created).
In linux terminal:
'scp add2boot.py install.sh modbus.tar.gz root@ clientipaddress:root/temp' (with password 1-6, temp is the directory you created).
e.g. 'pscp * root@10.186.96.168:root/temp'.
- 8) Go to the EZmoto unit you want to install in the MODBUS via putty.
- 9) Add permission to the installation file enter 'chmod +x install.sh'
- 10) Install using './install.sh' – the screen bellow will appear



```

/dev/ttyUSB0 - PuTTY
root@OpenWrt:~# cd root
root@OpenWrt:~# mkdir temp
root@OpenWrt:~# cd temp/
root@OpenWrt:~/temp# ./install.sh
etc/
etc/init.d/
etc/init.d/modbus.sh
etc/modbus_config.py
usr/
usr/sbin/
usr/sbin/modbusd/
usr/sbin/modbusd/uCDaemon
usr/sbin/modbusd/sock_modbus.py
usr/sbin/modbusd/uCDaemon.py
usr/sbin/modbusd/EZMoto_UC.py
usr/sbin/modbusd/IICOverSock.py
usr/sbin/modbusd/modbus_crc.py
usr/sbin/modbusd/modbus_config.py
usr/sbin/modbusd/coilreg_io.py
added to rc.local boot file
root@OpenWrt:~/temp# ls
add2boot.py  install.sh  modbus.tar.gz
root@OpenWrt:~/temp#
  
```

- 11) Enter 'reboot'

4. Creating Keys

To create keys for the master unit, follow the next steps:

- 1) Connect the EZmoto master unit to a computer using the USB-RS232 cable.
- 2) Open putty (see appendix C).
- 3) Open the vars file found in /etc/easy-rsa using nano or vi
e.g. 'nano /etc/easy-rsa/vars'.
- 4) Scroll down and edit the following parameters:

KEY_SIZE (should be 2048)

KEY_COUNTRY

KEY_PROVINCE

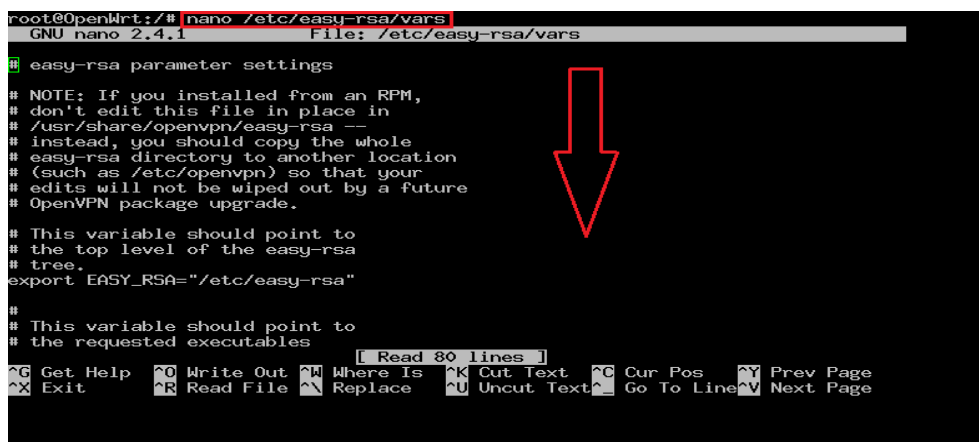
KEY_CITY

KEY_ORG

KEY_EMAIL

KEY_OU

You can choose any name to enter to the specified parameters



```

root@OpenWrt:/# nano /etc/easy-rsa/vars
GNU nano 2.4.1 File: /etc/easy-rsa/vars

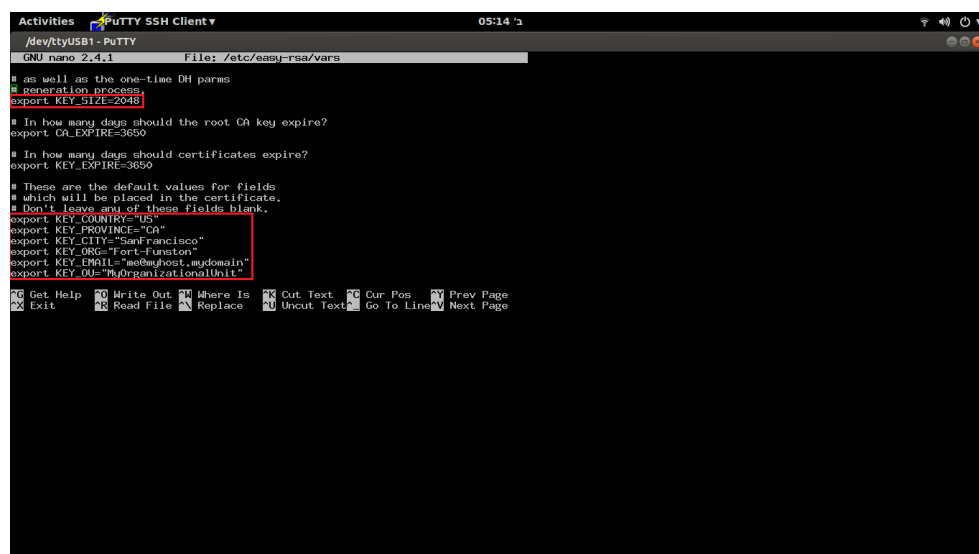
# easy-rsa parameter settings
# NOTE: If you installed from an RPM,
# don't edit this file in place in
# /usr/share/openvpn/easy-rsa --
# instead, you should copy the whole
# easy-rsa directory to another location
# (such as /etc/openvpn) so that your
# edits will not be wiped out by a future
# OpenVPN package upgrade.

# This variable should point to
# the top level of the easy-rsa
# tree.
export EASY_RSA="/etc/easy-rsa"

#
# This variable should point to
# the requested executables

[ Read 80 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^C Cur Pos ^Y Prev Page
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^_ Go To Line ^V Next Page

```



```

Activities Putty SSH Client 05:14
/dev/ttyUSB1 - PUTTY
GNU nano 2.4.1 File: /etc/easy-rsa/vars

# as well as the one-time DH params
# generation process.
export KEY_SIZE=2048

# In how many days should the root CA key expire?
export CA_EXPIRE=3650

# In how many days should certificates expire?
export KEY_EXPIRE=3650

# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="San Francisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_OU="MyOrganizationalUnit"

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^C Cur Pos ^Y Prev Page
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^_ Go To Line ^V Next Page

```

- 5) Run vars as script with the command: '. .vars' (with space between the dots).
- 6) Enter the command 'clean all'.
- 7) Build certificate authority with 'build-ca'.

Check that ca files were created in keys directory 'ls /etc/easy-rsa/keys'. Two files should appear ca.crt ca.key.

```
/dev/ttyUSB0 - PuTTY
root@OpenWrt:~# ls /etc/easy-rsa/keys/
01.pem      c02.crt      c07.crt      ca.crt
02.pem      c02.csr      c07.csr      ca.key
03.pem      c02.key      c07.key      dh2048.pem
04.pem      c03.crt      c08.crt      index.txt
05.pem      c03.csr      c08.csr      index.txt.attr
06.pem      c03.key      c08.key      index.txt.attr.old
07.pem      c04.crt      c09.crt      index.txt.old
08.pem      c04.csr      c09.csr      serial
09.pem      c04.key      c09.key      serial.old
0A.pem      c05.crt      c10.crt      server.crt
0B.pem      c05.csr      c10.csr      server.csr
0C.pem      c05.key      c10.key      server.key
c01.crt      c06.crt      c11.crt
c01.csr      c06.csr      c11.csr
c01.key      c06.key      c11.key
root@OpenWrt:~#
```

- 8) Build server keys with 'build-key-server <name>' e.g. 'build-key-server server'
- 9) Check that server key files were created in keys directory 'ls /etc/easy-rsa/keys'.

Three files should appear name.crt name.csr name.key

```
/dev/ttyUSB0 - PuTTY
root@OpenWrt:~# ls /etc/easy-rsa/keys/
01.pem      c02.crt      c07.crt      ca.crt
02.pem      c02.csr      c07.csr      ca.key
03.pem      c02.key      c07.key      dh2048.pem
04.pem      c03.crt      c08.crt      index.txt
05.pem      c03.csr      c08.csr      index.txt.attr
06.pem      c03.key      c08.key      index.txt.attr.old
07.pem      c04.crt      c09.crt      index.txt.old
08.pem      c04.csr      c09.csr      serial
09.pem      c04.key      c09.key      serial.old
0A.pem      c05.crt      c10.crt      server.crt
0B.pem      c05.csr      c10.csr      server.csr
0C.pem      c05.key      c10.key      server.key
c01.crt      c06.crt      c11.crt
c01.csr      c06.csr      c11.csr
c01.key      c06.key      c11.key
root@OpenWrt:~#
```

To complete the master key production enter 'build-dh'. This operation could take a while, be patient.

The final step is updating the settings.conf file with the current key,

- 10) Go to root using 'cd ~'

- 11) Edit the key field in the settings.conf file using 'nano settings.conf'.

```

/dev/ttyUSB0 - PuTTY
GNU nano 2.4.1 File: settings.conf
mode=server
ca-crt=ca.crt
cert=server.crt
key=server.key
ip3g=10.136.96.174
vpnproto=udp
vpnport=1194
ipbr=10.8.0.1
ipbrmask=255.255.255.0
ipbrserv=10.8.0.1

[ Read 10 lines ]
^G Get Help ^O Write Out ^M Where Is ^K Cut Text ^C Cur Pos ^Y Prev Page
^X Exit ^R Read File ^N Replace ^U Uncut Text ^_ Go To Line ^V Next Page

```

- 12) Enter 'reboot' to finish the process.

Now you can create keys for the client units. To do so follow the next steps:

1. In the master unit enter the command 'build-key <name>' e.g. 'build-key c12'.
2. Press enter until questioned 'sign the certificate?' and press y and enter.

When asked if to commit press y and enter.

```

Activities PuTTY SSH Client v 51:14
/dev/ttyUSB0 - PuTTY
root@OpenWrt:/# build-key c12
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-rsa/keys
Generating a 2048 bit RSA private key
.....+++++
writing new private key to 'c12.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [IL]:
State or Province Name (full name) [HFA]:
Locality Name (eg, city) [HAIFA]:
Organization Name (eg, company) [ELECTRICITY-COMPANY]:
Organizational Unit Name (eg, section) [VPN-Manager]:
Common Name (eg, your name or your server's hostname) [c12]:
Name [EasyRSA]:
Email Address [yuri.kritman@ec.co.il]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'IL'
stateOrProvinceName     :PRINTABLE:'HFA'
localityName            :PRINTABLE:'HAIFA'
organizationName        :PRINTABLE:'ELECTRICITY-COMPANY'
organizationalUnitName  :PRINTABLE:'VPN-Manager'
commonName              :PRINTABLE:'c12'
name                    :PRINTABLE:'EasyRSA'
emailAddress            :IASSTRING:'mail.email.com'
Certificate is to be certified until Aug  2 03:17:34 2025 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
root@OpenWrt:/#

```

```

Certificate is to be certified until Aug  2 03:17:34 2025 GMT (3650 days)
Sign the certificate? [y/n]:y

```

```

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
root@OpenWrt:/#

```

- Check that the client key files were created in keys directory 'ls /etc/easy-rsa/keys'.
Three files should appear name.crt name.csr name.key

```

/dev/ttyUSB0 - PuTTY
root@OpenWrt:/# ls /etc/easy-rsa/keys/
01.pem      c02.crt    c07.crt    ca.crt
02.pem      c02.csr    c07.csr    ca.key
03.pem      c02.key    c07.key    dh2048.pem
04.pem      c03.crt    c08.crt    index.txt
05.pem      c03.csr    c08.csr    index.txt.attr
06.pem      c03.key    c08.key    index.txt.attr.old
07.pem      c04.crt    c09.crt    index.txt.old
08.pem      c04.csr    c09.csr    serial
09.pem      c04.key    c09.key    serial.old
0A.pem      c05.crt    c10.crt    server.crt
0B.pem      c05.csr    c10.csr    server.csr
0C.pem      c05.key    c10.key    server.key
c01.crt     c06.crt    c11.crt
c01.csr     c06.csr    c11.csr
c01.key     c06.key    c11.key
root@OpenWrt:/#

```

In order to transfer the keys from the master to the clients via 3g, do the following steps:

- Connect to the client you wish to transfer the key to, using the USB-RS232 cable.
- Disable the firewall at the client using the command 'fw3 stop' (the default password is 1-6) and then '/etc/init.d/firewall disable'.
- Transfer the key files with secure copy using the command:
'scp keys/ca.crt keys/<name>.* root@clientipaddress:/etc/easy-rsa/keys'.
e.g. 'scp keys/ca.crt keys/c12.* root@10.186.96.18:/etc/easy-rsa/keys'.
- Check that the files were transferred using 'ls /etc/easy-rsa/keys'.
Four files should appear <name>.crt <name>.csr <name>.key ca.crt.

```

/dev/ttyUSB1 - PuTTY
root@OpenWrt:/# ls /etc/easy-rsa/keys/
c11.crt  c11.csr  c11.key  ca.crt  index.txt  serial
root@OpenWrt:/#

```

The final step is updating the settings.conf file with the current key,

- Go to root using 'cd ~'
- Edit the key field in the settings.conf file using 'nano settings.conf'.

```

/dev/ttyUSB1 - PuTTY
GNU nano 2.4.1 File: settings.conf
mode=client
ca-crt=ca.crt
cert=c11.crt
key=c11.key
ip3g=10.186.96.174
vpnpote=udp
vpnpote=1194
ipbr=10.8.0.18
ipbrmask=255.255.255.0
ipbrserv=10.8.0.1

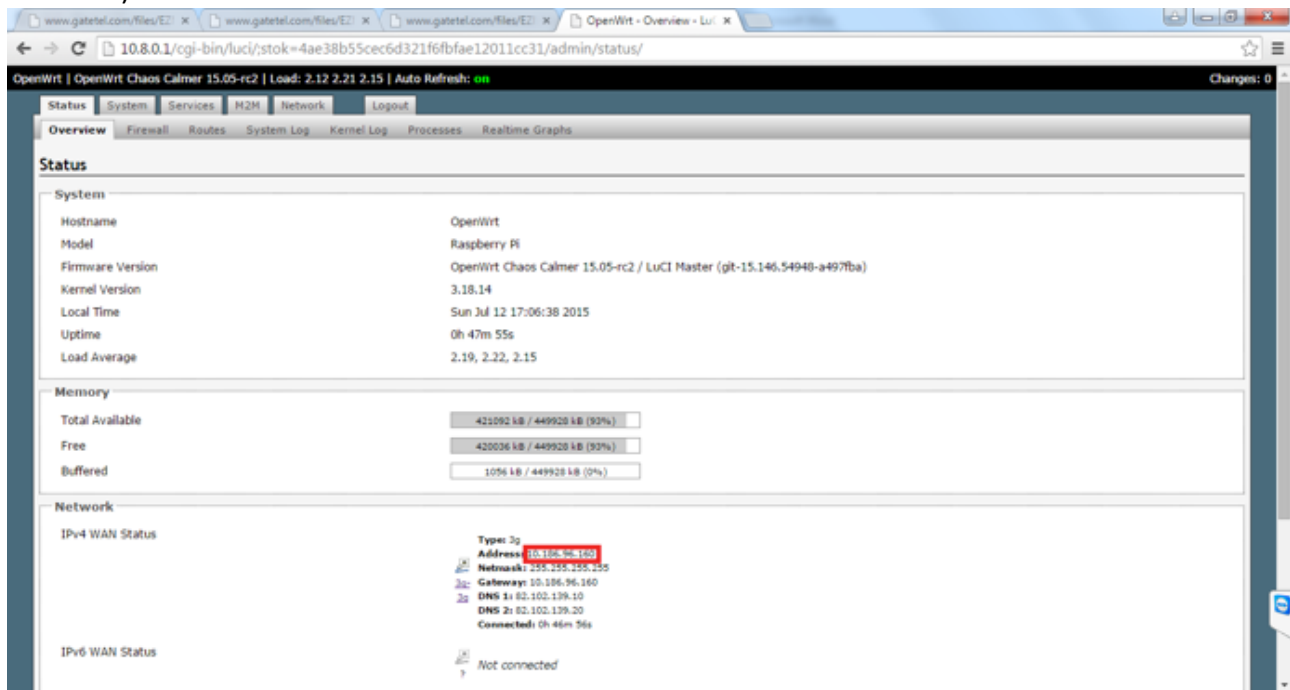
```

- Enter 'reboot' to finish the process of installing key.

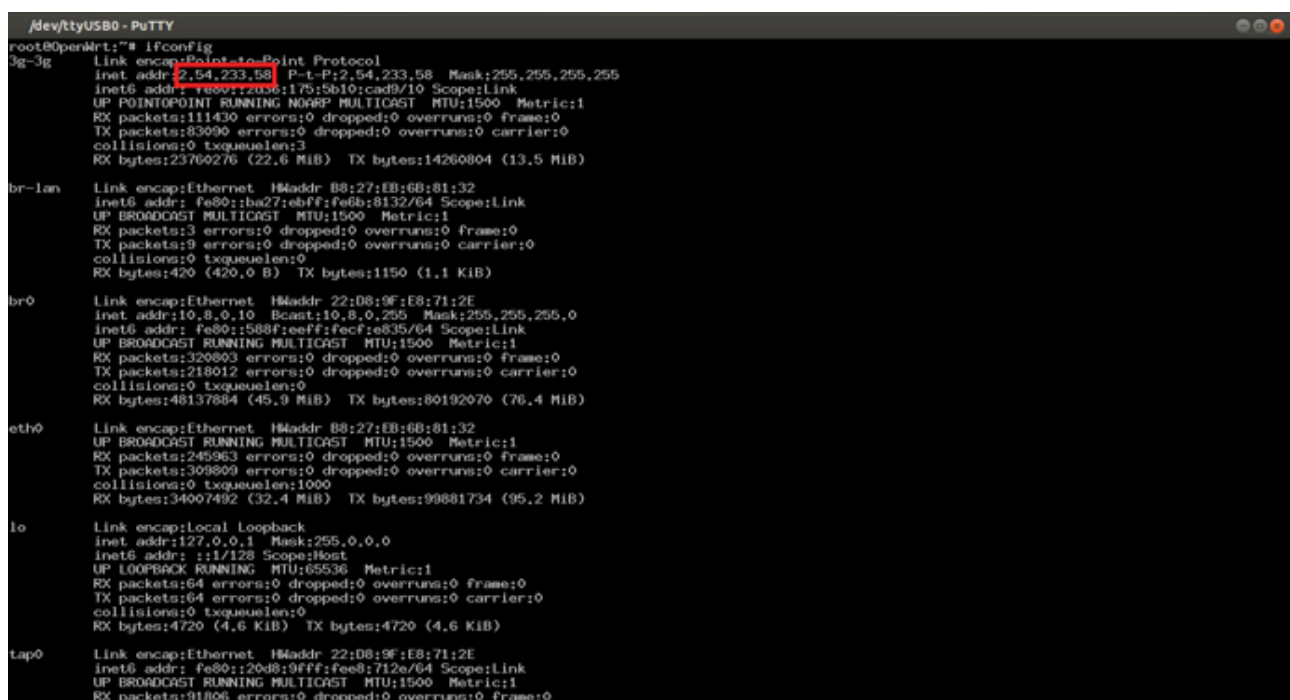
5. OpenVPN network configuration

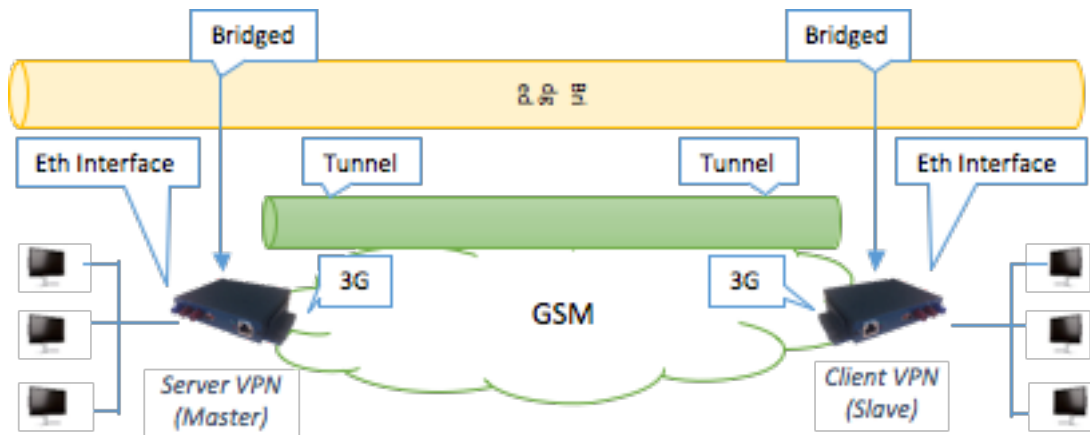
Obtaining the ip3g address of the server after configuration

- 1) Open a browser.
- 2) Enter the IP address of the EZmoto server.
- 3) Login to the OpenWRT.
- 4) Look for the Network -> IPv4 Wan Status section in the page to see the address.
- 5) Write down the address.



Another way to see the 3g IP Address is to enter the console (COM PORT using Putty) and issue 'ifconfig' command.





The

Slave is programmed to look for the Master 3G IP Address, to set up a tunnelled Layer-2 VPN service. Afterwards, the system is automatically bridging the Layer-2 Tunnel with the Ethernet Interface, creating a new Layer 2 Interface called Br0.

In order to set up the VPN Service, an IP Address for the Br0 must be configured. Once configured, the EZmoto client can be queried by the Server side.

If the EZmoto Client's cellular reception / network is by any means not responsive, The Client side will revert to the original LAN address and settings.

The OpenVPN service can be configured with nonstandard IP protocol / port. The configuration method will be explained in detail in the following section. However, if chosen to do so, one must update the local FireWall rules of the EZmoto.

Instructions for opening ports for the OpenVPN (or any other application for that matter) can be found in section appendix D.

Env-variables configuration

The following Env-variables found in /root/settings.conf should be set:

- Master 3G IP Address (for Slaves only)
- VPN Tunneling Proto + Port
- VPN-LAN IP (A.K.A. Br0)

The variables are found in the file settings.conf in the following format:

```
$mode=server/client (constant value)
$ip3g=x.y.z.w (see section 2.3.2)
$vpnproto=udp/tcp (default udp)
$vpnport=#### (default 1194)
$ipbr=x.y.z.w (e.g 10.10.10.10)
$ipbrmask=x.y.z.w (mask address e.g 255.255.255.0)
```

```
root@OpenWrt:~# cat settings.conf
mode=server
ip3g=2.54.233.58
vpnproto=udp
vpnport=1194
ipbr=10.8.0.10
ipbrmask=255.255.255.0
ipbrserv=10.8.0.10
root@OpenWrt:~#
```

To change these parameters, open the described settings file with the terminal using the following commands:

- 1) `cd ~`
- 2) `nano settings.conf`
- 3) Change the described parameters
- 4) Reboot the system (write `reboot` in cmd or issue a hard reset)

Server side configuration

- 1) Get the 3g IP Address of the Server EZmoto (as described in section 3)
- 2) Go to the `settings.conf` file as explained in the previous section.
- 3) Choose an IP Address for your tunneled virtual Lan(for your client and server)
- 4) Enter your choice in `ipbr`, `ipbrmask` and `ipbrserv` fields (`ipbr` and `ipbrserv` should be the same IP, it is the EZmoto IP on the tunnel)
- 5) Reboot to save configuration.

Client side configuration

- 1) Go to the `settings.conf` file as explained in the previous section.
- 2) Config all the following fields: `ip3g` (the server 3g ip address), `ipbr` (the local ip address of the client EZmoto when the VPN is up - a.k.a `br0`), `ipbrmask` (`ipbr` netmask), and `ipbrserv` (the server `ipbr`)
- 3) Reboot to save configuration

6. Modbus serial parameters configuration

1. Edit the configuration file '/etc/modbus_config.py'

You can choose nano or vi.

```
root@OpenWrt:~# nano /etc/modbus_config.py
```

2. Edit the SerialParams variable in the file:

```
# App imports this file to sock_modbus.py
#
# Choose one of the following options: 'tcpserver', 'tcpclient', 'rtuserver', 'rtuclient', 'tcp2rtu', 'rtu2tcp'
mode='tcp2rtu'
# Choose TCP/IP parameters
ip='10.0.0.202'
port=9999
# Choose Serial parameters (uses pySerial default values). Port is mandatory. To Config use one of the following:
#
# string: sets port only (all else uses default values) e.g.
# e.g. '/dev/ttyUSB2' Most simple config, uses default values
# tuple: set values in this order: (port, baudrate, bytesize, parity, stopbits, timeout, xonxoff ..)
# e.g. ('/dev/ttyUSB2', 115200, 8, 'N', 1, 0.4, True) Config in a row (must be the same order as default values)
# ('/dev/ttyUSB2', 9600, 7, 'E', 1)
# dictionary: sets specific parameter use (all else uses default values)
# e.g. {'port': '/dev/ttyUSB2', 'baudrate': 115200} Config in a selective manner (non-configured uses default)
# e.g. {'port': '/dev/ttyUSB2', 'parity': 'E'}
# default values: baudrate = 9600, bytesize = 8, parity = 'N', stopbit = 1, timeout = 0.1 (cannot be in blocking mode), xonxoff = False ...
SerialParams={'port': '/dev/ttyUSB2', 'parity': 'E'}
```

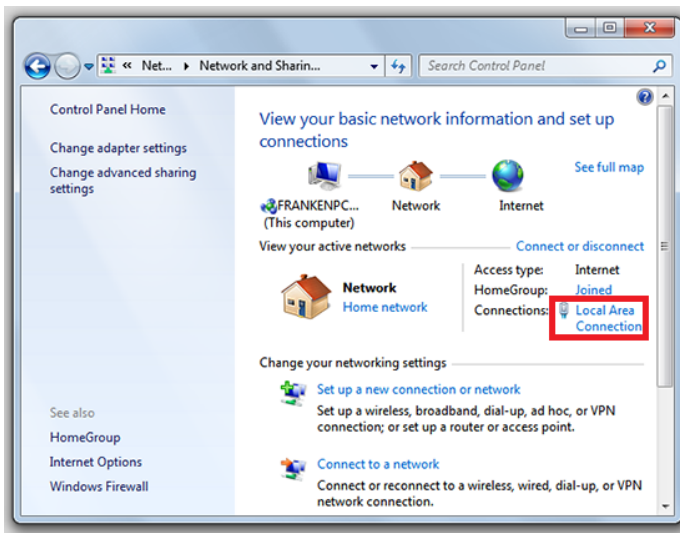
3. Reboot to save

7. Appendix A

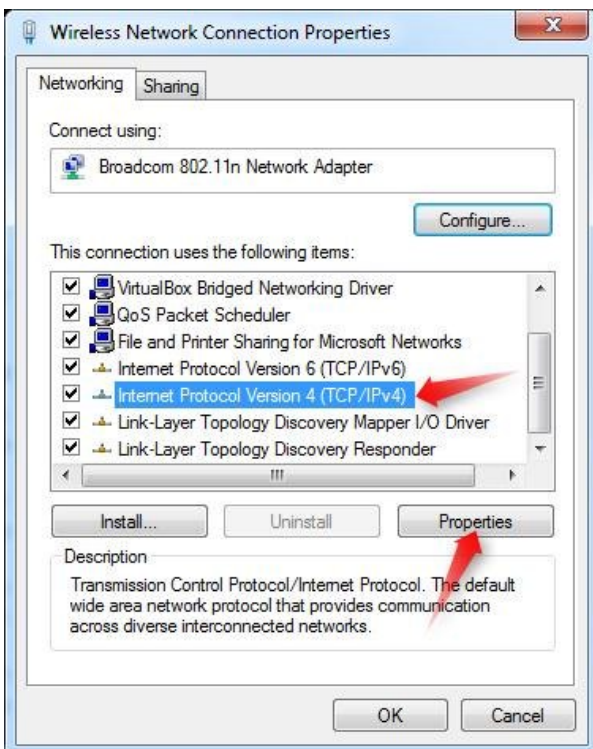
(Windows)

To set an IP address, go to control panel, and choose Network and Sharing Center.

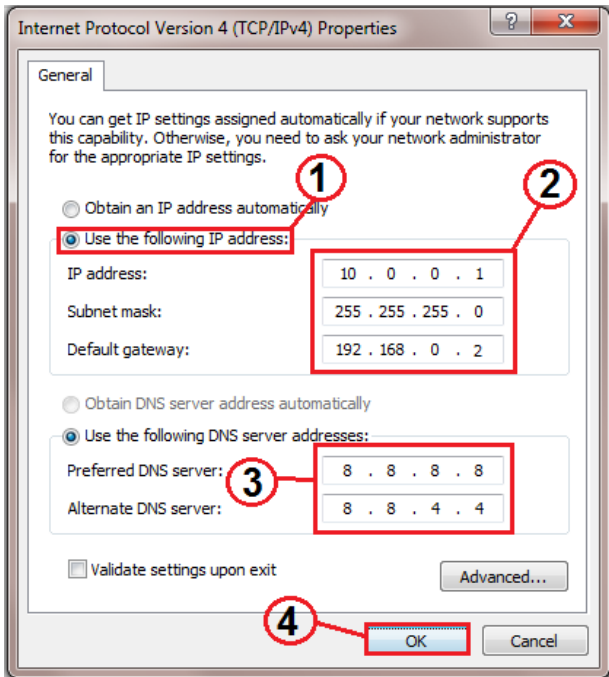
Click on the Local Area Connection and choose properties



Select Internet Protocol Version 4 (TCP/IPv4) and choose Properties



Set up the IP address, Subnet mask and Default gateway, you can also set up DNS Servers if you wish.

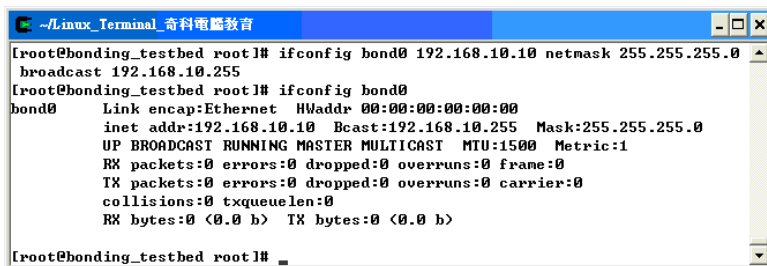


When you are done, press ok to save.

(Linux)

Open a command line terminal, and issue the ifconfig command the following way:

Ifconfig <intf> <ip-address> netmask <subnet-mask>



When you're done you can view the interface with the ifconfig command (you must have privileges to change these settings, be root or use sudo accordingly).

To check connectivity, in any OS, use the ping command in command line.

Here is an example of a working connectivity between two stations:

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>ping 69.147.114.224

Pinging 69.147.114.224 with 32 bytes of data:

Reply from 69.147.114.224: bytes=32 time=400ms TTL=43
Reply from 69.147.114.224: bytes=32 time=403ms TTL=43
Reply from 69.147.114.224: bytes=32 time=382ms TTL=43
Reply from 69.147.114.224: bytes=32 time=402ms TTL=43

Ping statistics for 69.147.114.224:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 382ms, Maximum = 403ms, Average = 396ms

C:\Documents and Settings\Administrator>ping gmail.com

Pinging gmail.com [209.85.153.19] with 32 bytes of data:

Reply from 209.85.153.19: bytes=32 time=140ms TTL=49
Reply from 209.85.153.19: bytes=32 time=131ms TTL=49
Reply from 209.85.153.19: bytes=32 time=131ms TTL=49
Reply from 209.85.153.19: bytes=32 time=131ms TTL=49

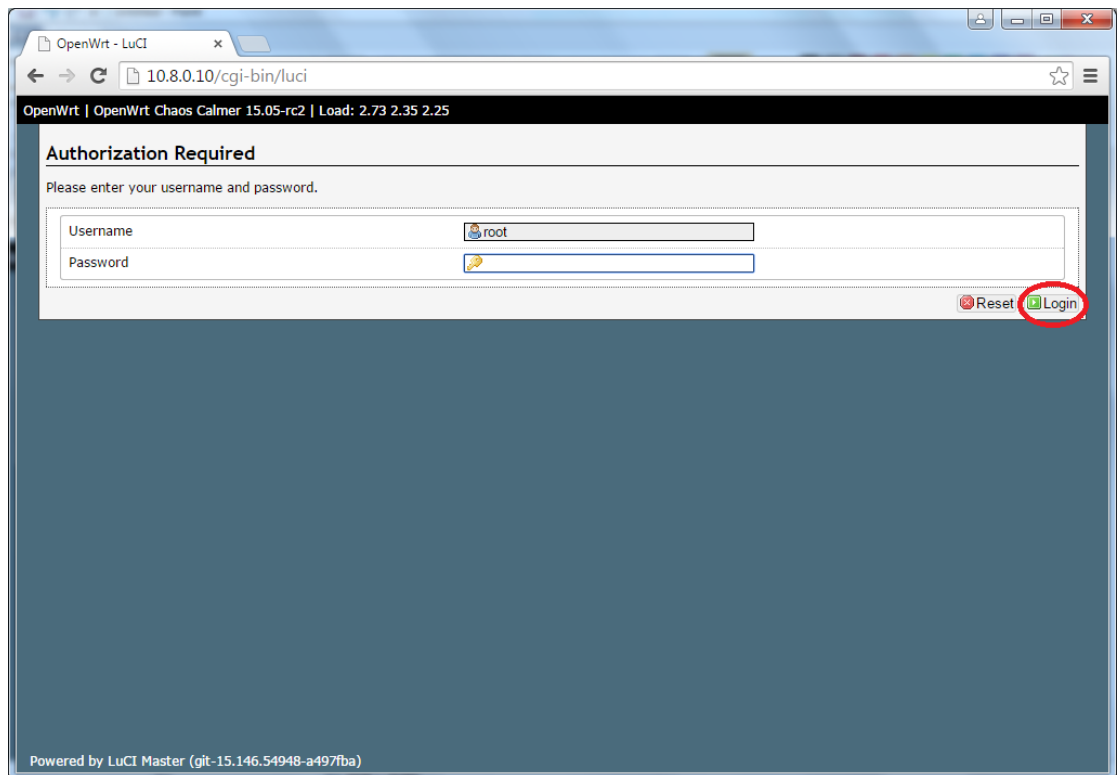
Ping statistics for 209.85.153.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 131ms, Maximum = 140ms, Average = 133ms

C:\Documents and Settings\Administrator>_
```

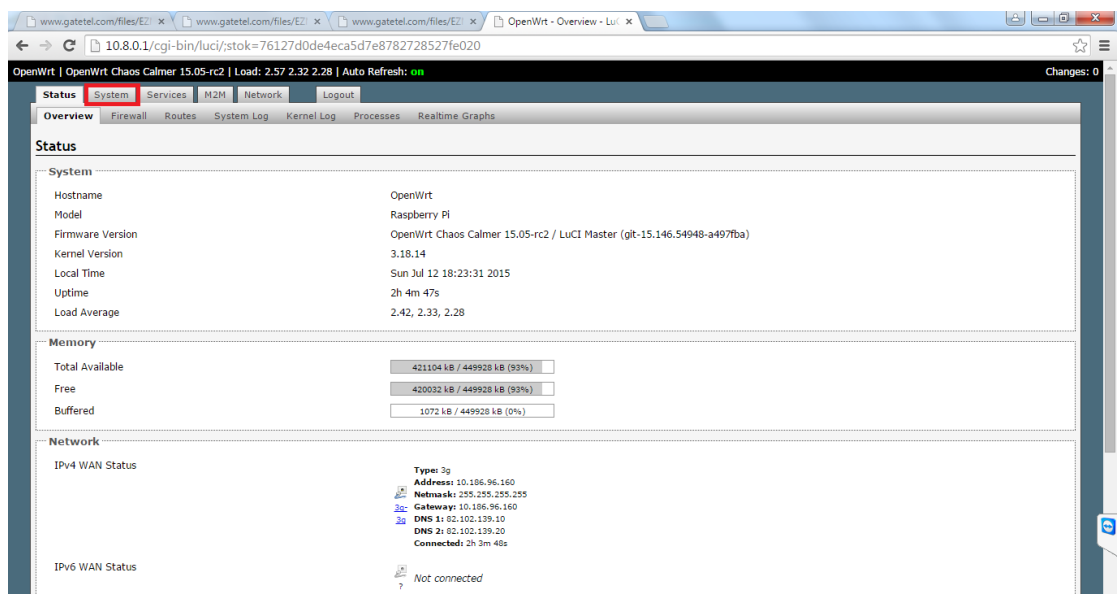
8. Appendix B

Entering the OpenWRT for the first time

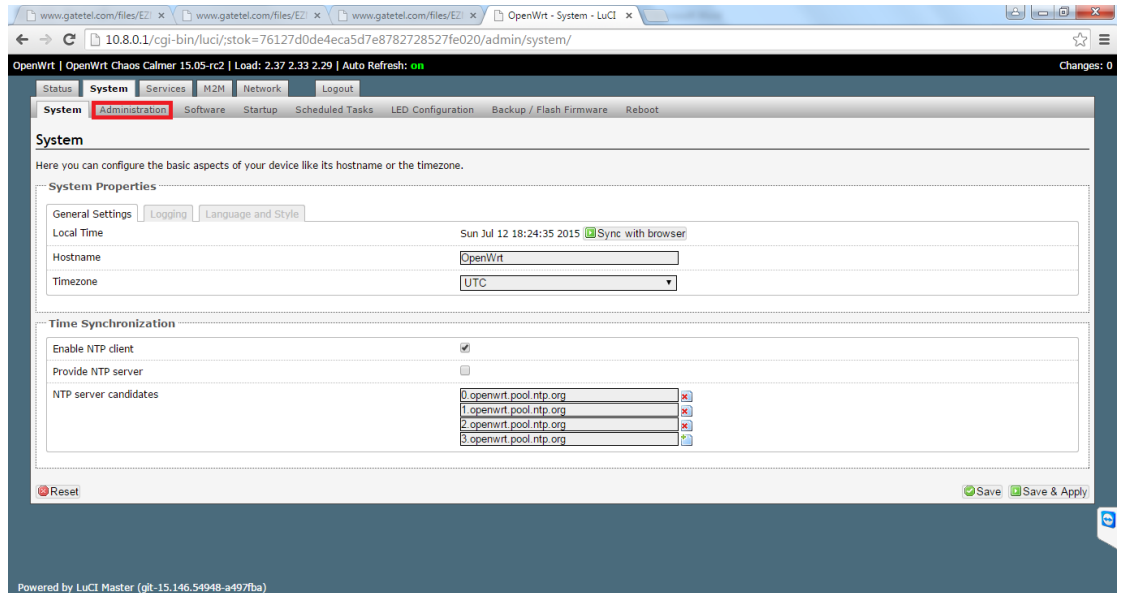
- 1) Open your browser and enter the EZmoto IP Address.



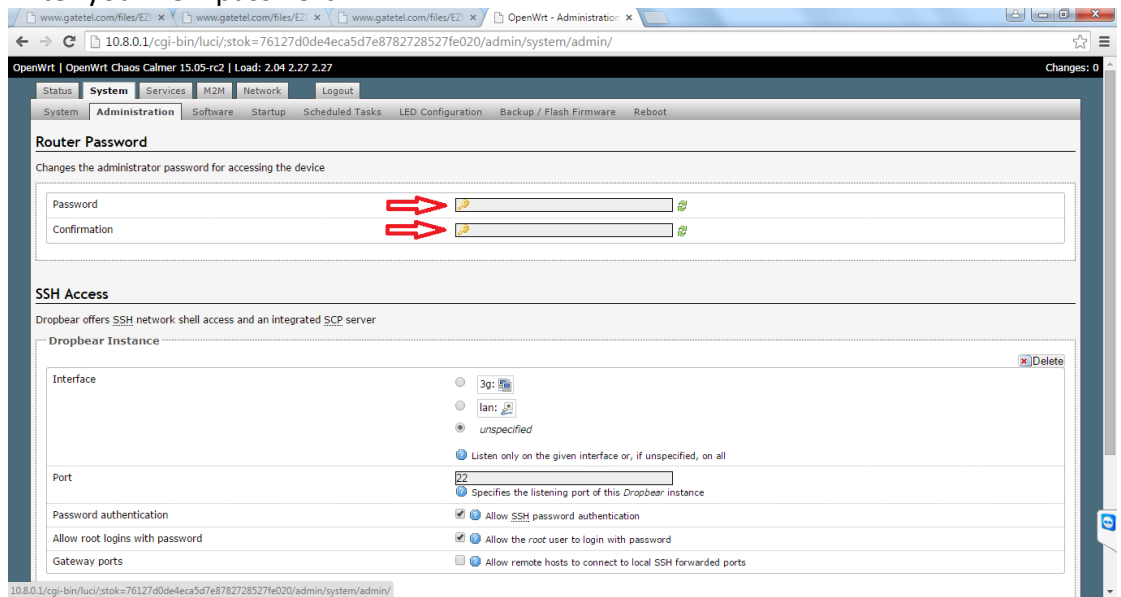
- 2) Enter the password and click Login (the default password is 123456).
- 3) Go to system tab.



4) Go to administration tab.



5) Enter your new password.



6) Click save & apply.

The screenshot shows the 'SSH Access' configuration page in the GateTel web interface. The page title is 'SSH Access'. Below the title, it states 'Dropbear offers SSH network shell access and an integrated SCP server'. The main configuration area is titled 'Dropbear Instance' and includes a 'Delete' button. The configuration options are:

- Interface:** Radio buttons for '3g', 'lan', and 'unspecified'. The 'unspecified' option is selected.
- Port:** A text input field containing '22'. Below it, a note says 'Specifies the listening port of this Dropbear instance'.
- Password authentication:** A checked checkbox labeled 'Allow SSH password authentication'.
- Allow root logins with password:** A checked checkbox labeled 'Allow the root user to login with password'.
- Gateway ports:** An unchecked checkbox labeled 'Allow remote hosts to connect to local SSH forwarded ports'.

Below the configuration area is an 'Add' button and an 'SSH-Keys' section with a text area for pasting public SSH keys. At the bottom of the page, there are 'Reset', 'Save', and 'Save & Apply' buttons. The 'Save & Apply' button is circled in red.

Changing the password is highly recommended.

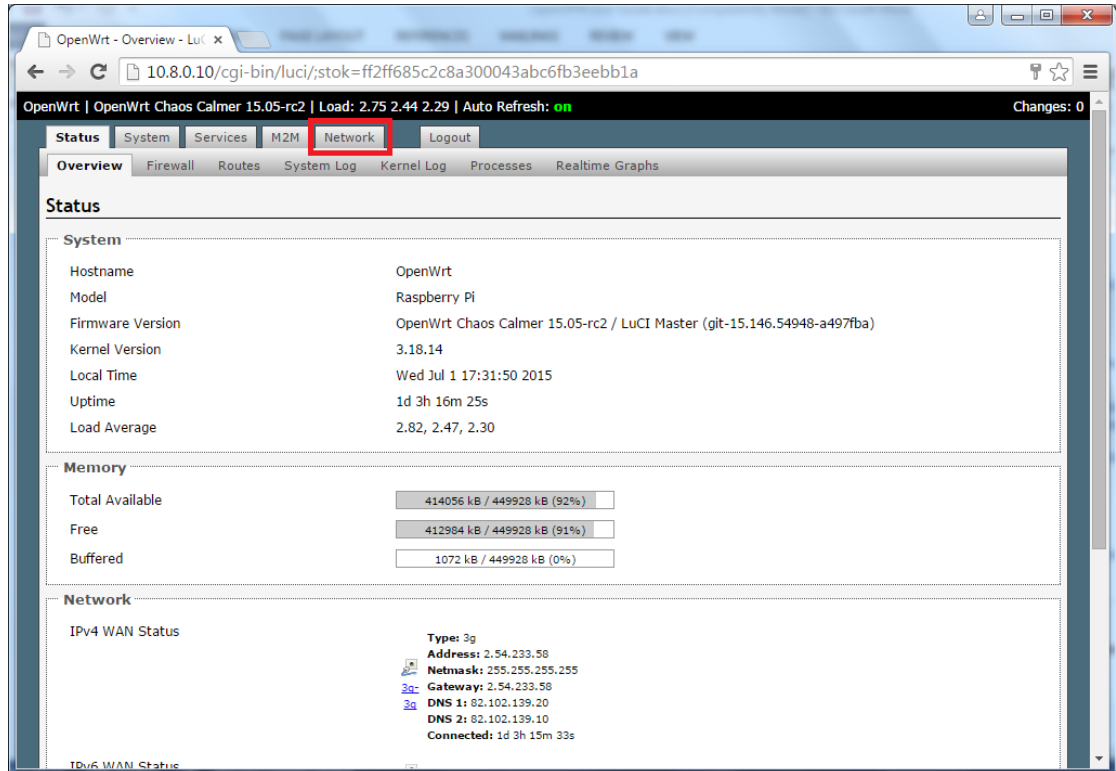
9. Appendix C

- 1) download and install terminal program. Putty is available in [THIS LINK](#).
- 2) insert the usb side of the usb to uart cable to the computer
- 3) check which com is connected: right click on my computer → manage → device manager → COM & LPT → USB Serial Port(COMx)
- 4) Open putty.
- 5) under connection type, mark serial option. Under serial line enter COMx. Under speed enter 115200.
- 6) Open.

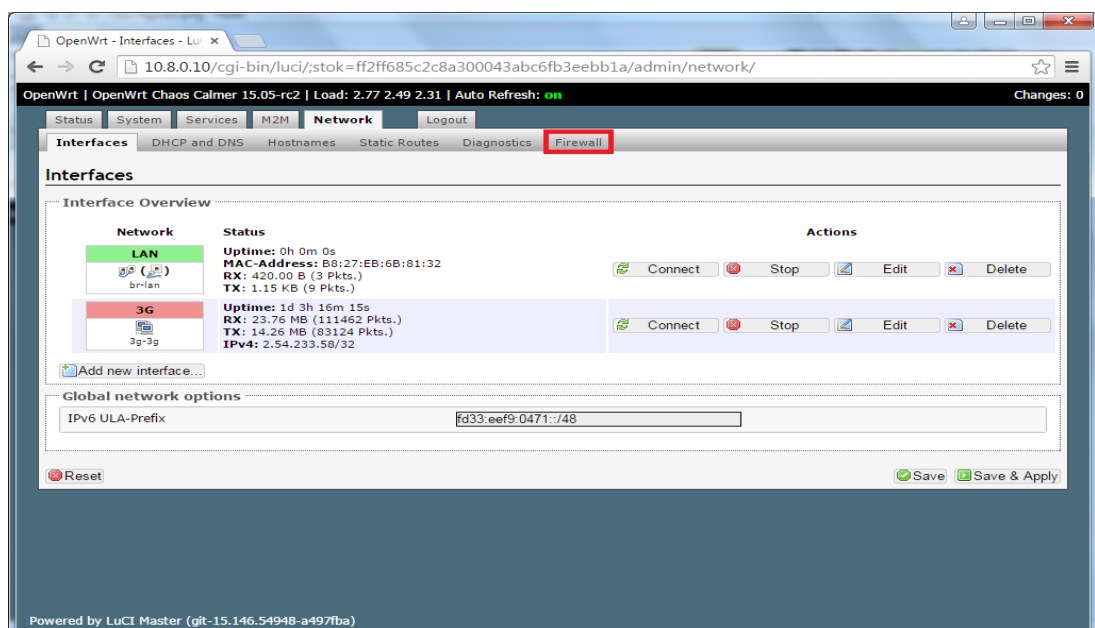
10. Appendix D firewall

To open port in the OpenWRT firewall follow the next steps:

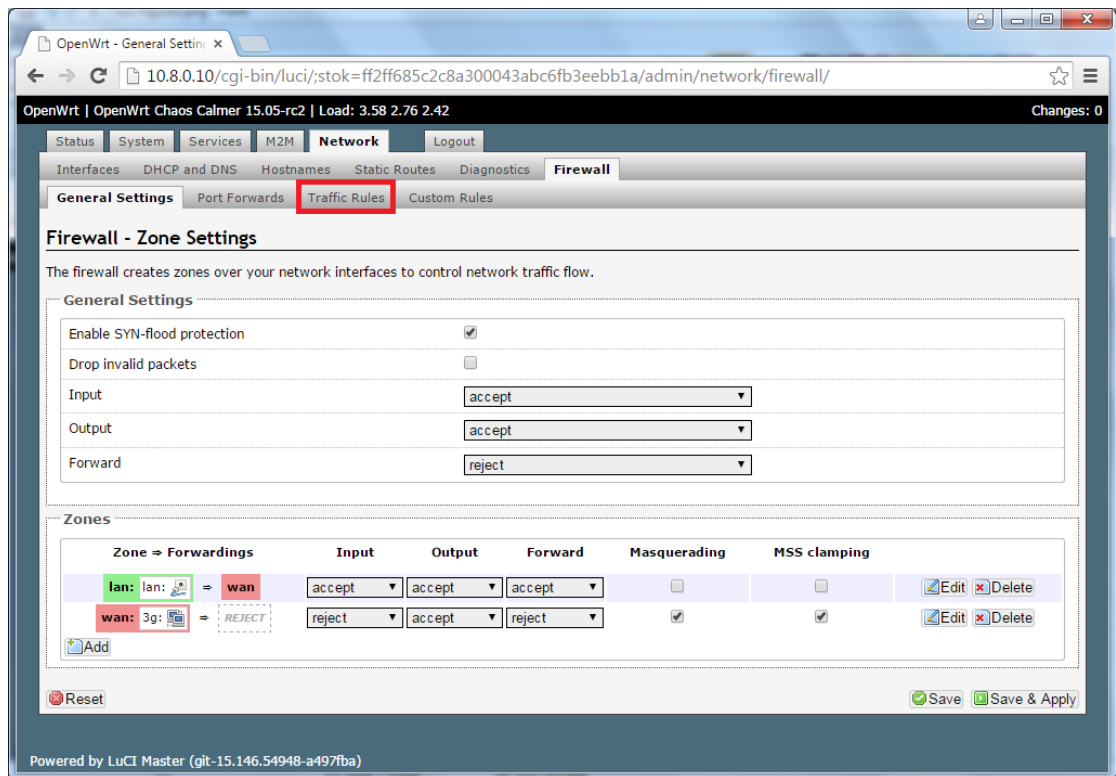
- 1) Click on the Network menu.



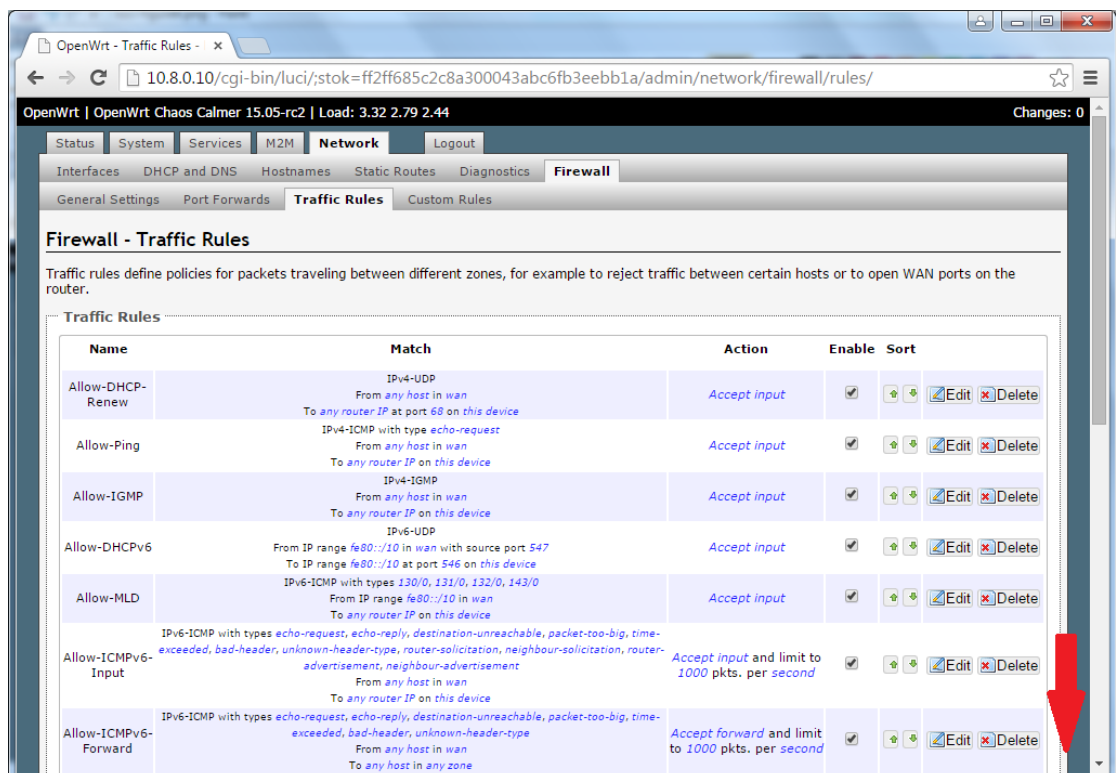
- 2) Click on the Firewall tab.



3) Click on the Traffic Rules.



4) Scroll down and look for the "Open ports on router" section of the page.



- 5) Assign a name to the new Firewall Rule, and enter the protocol and port details. When you are done click Save & Apply.

OpenWrt - Traffic Rules - x

10.8.0.10/cgi-bin/luci/stok=ff2ff685c2c8a300043abc6fb3eebb1a/admin/network/firewall/rules/

Name	Protocol	External port	Action	Enable	Sort
modbus-tcp-port-9998-rtu	Any TCP	From any host in wan To any router IP at port 9998 on this device	Accept input	<input checked="" type="checkbox"/>	Edit Delete
test_open_502	Any TCP	From any host in wan To any router IP at port 502 on this device	Accept input	<input checked="" type="checkbox"/>	Edit Delete
Allow-SSH	Any TCP	From any host in wan To any router IP at port 22 on this device	Accept input	<input checked="" type="checkbox"/>	Edit Delete
Allow-Openvpn-1194	Any UDP	From any host in wan To any router IP at port 1194 on this device	Accept input	<input checked="" type="checkbox"/>	Edit Delete

Open ports on router:

Name	Protocol	External port	Add
New input rule	TCP+UDP		Add

New forward rule:

Name	Source zone	Destination zone	Add and edit...
New forward rule	lan	wan	Add and edit...

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port	Add and edit...
New SNAT rule	lan	wan	-- Please choose	Do not rewrite	Add and edit...

OpenWrt - Traffic Rules - x

10.8.0.10/cgi-bin/luci/stok=ff2ff685c2c8a300043abc6fb3eebb1a/admin/network/firewall/rules/

Name	Protocol	External port	Action	Enable	Sort
test_open_502	Any TCP	From any host in wan To any router IP at port 502 on this device	Accept input	<input checked="" type="checkbox"/>	Edit Delete
Allow-SSH	Any TCP	From any host in wan To any router IP at port 22 on this device	Accept input	<input checked="" type="checkbox"/>	Edit Delete
Allow-Openvpn-1194	Any UDP	From any host in wan To any router IP at port 1194 on this device	Accept input	<input checked="" type="checkbox"/>	Edit Delete

Open ports on router:

Name	Protocol	External port	Add
Allow-FTP	TCP	21	Add

New forward rule:

Name	Source zone	Destination zone	Add and edit...
New forward rule	lan	wan	Add and edit...

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

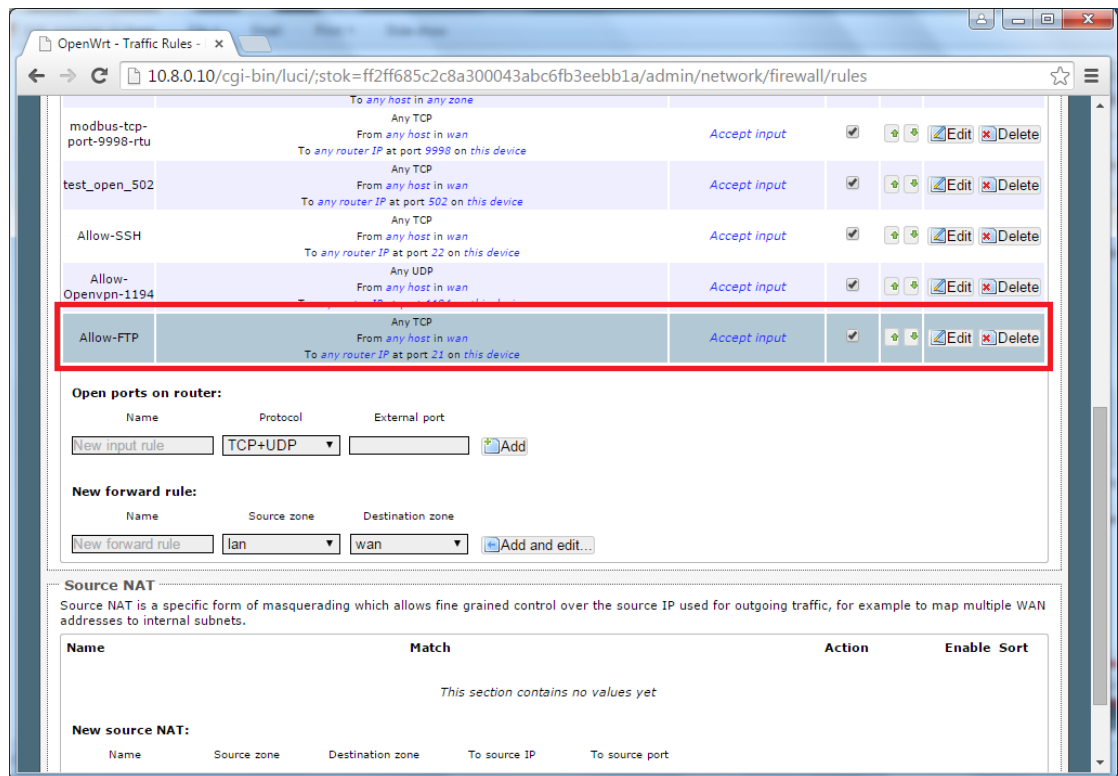
Name	Source zone	Destination zone	To source IP	To source port	Add and edit...
New SNAT rule	lan	wan	-- Please choose	Do not rewrite	Add and edit...

[Reset](#) [Save](#) [Save & Apply](#)

Powered by LuCI Master (git-15.146.54948-a497fba)

**** DO NOT FORGET TO SAVE AND APPLY ****

6) Check to see the updated rules.

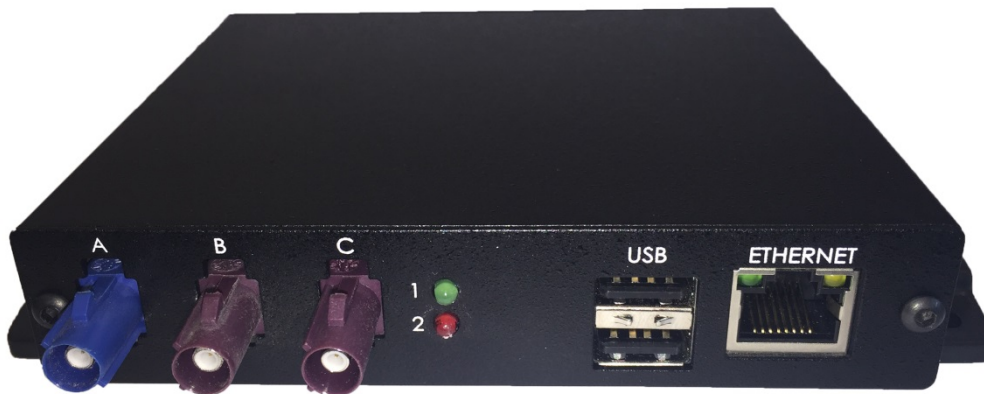


11. Appendix E Leds

There are two leds in use in the OpenVPN EZmoto.
Both of them are on the back side of the EZmoto.

Led 2(red led) indicates registration to a network:
Blinking 0.5s on, 0.5s off, searching for a network
Blinking 3s off 0.3s on registered to a network.

Led 1(green led) indicates OpenVPN state:
Led off – not connected to OpenVPN
Led blinking – trying to connect to OpenVPN.
Led constant on – connected to OpenVPN.



12. Misc

- The Bridging can traverse over Nat in the internal Cellular Company's network, assuming the Slave is at the private IP range side of the Nat.
- The Bridging can traverse over two different cellular companies, depends on whether the Slaves can reach the Master. This is most likely to happen if the cellular companies' WAN aims to the Internet and the Master have a public IP address. Although the communication speed may be influenced by their connectivity.

13. Product Variations

1. Pure OpenVPN
2. Cellular Modbus to RTU
3. OpenVPN modbus