WAZIUP Online Course

Developing IoT Solutions with WAZIUP

D-GW-4: Gateway Web Admin Interface (LowCostLoRaGw github version)

Prof. Congduc Pham
http://www.univ-pau.fr/~cpham
Université de Pau, France
ON-LINE ARDUINO SENSORS AND DIY LORA TUTORIAL

Forewords

This online tutorial on Arduino, Sensors, and LoRa technologies has been developed by University of Pau, France, in the WAZIUP project funded by the European Union in the H2020 research program. The main objective of this tutorial is to provide comprehensive and guided training materials to be used in training, hackathons, bootcamps, entrepreneur’s days, etc. The tutorial is on LoRa networks and IoT. This tutorial is first start with basic of Arduino and sensor programming to understand that the foundation of so-called Internet-of-Things (IoT) concepts. Then in a second step, we will introduce LoRa radios to show how to build low-cost, long-range and energy-efficient IoT devices.

WAZIUP Online Course

http://diy.waziup.io
This tutorial presents the web admin interface which is an add-on to the low-cost gateway framework.

Refer to D-GW-1 to understand the gateway configuration and architecture.

Note that the SD card image has everything needed, including the web admin interface installed, so you may skip the installation procedure if you flashed our SD card image.

Let’s get started...
Gateway web admin interface (1)

- To install the web admin interface, check if you have the `gw_web_admin` folder in your `lora_gateway` folder.
- If you don't, then update to the latest version.
- Then, go into `gw_web_admin` and run the `install.sh` script:
  - `cd gw_web_admin`
  - `sudo ./install.sh`
Gateway web admin interface (2)

- **URL:** [http://192.168.200.1/admin](http://192.168.200.1/admin) (with WiFi connection)
- **Login:** admin
- **Password:** loragateway

![Gateway web admin interface](image)

<table>
<thead>
<tr>
<th>Gateway configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
</tr>
<tr>
<td><strong>Spreading Factor</strong></td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
</tr>
<tr>
<td><strong>PA BOOST</strong></td>
</tr>
</tbody>
</table>

- **Mode** = 11 to indicate LoRaWAN mode
- For single-channel gateways, the default LoRaWAN mode means SF13BW125 and sync word 3x34. In this mode you can change the Spreading Factor SF.
- Change frequency for a single-channel gateway if needed. Leave frequency as 1 to use default values (for LoRaWAN mode: 868MHz for BAND68, 862.5MHz for BAND69 and 433.75MHz for BAND95).
- PA BOOST is required for some radio modules such as RN969, RN959W, RN199, RN199W, RN199LoRa1276. After changing the PA_BOOST settings, run Gateway Update/Basic config to recompile the low-level gateway program.
Gateway main page

Gateway main page (configuration page)

- Check Internet connectivity & get github version
- Display a simple packet logger
- Reboot the gateway. Need to reboot after any update
- Shutdown the gateway
Main gateway configuration (1)

- **radio configuration section**

  - **Pre-defined LoRa mode.** Mode 11 indicates LoRaWAN mode. Use **Configure for LoRaWAN**
  - Changing the Spreading Factor is only relevant in LoRaWAN mode
  - Set to a customized frequency band, e.g. 433.3MHz

  - **Edit PA_BOOST setting.** You must use **Gateway update/Basic config** to recompile

  - Indicate a single-channel or SX1301 concentrator hardware configuration
  - Last status from low-level radio layer, normally every 10mins
  - Last radio packet reception time
Main gateway configuration (2)

Gateway configuration section

- Set gateway ID (should normally be pre-configured)
  Default id is 0000XXXXXXXXXXXX with the 6 bytes of the MAC address of the gateway network interface (e.g. B827EBD4F300)

- The MD5 hash of the gateway's ID

- Enables local decryption at gateway. Decryption keys must be defined

- Easy configuration button to for LoRaWAN settings. Select which LoRaWAN network server to activate

- Indicate raw format to handle customized packet format. Required for LoRaWAN mode

- Set the downlink timer in seconds -1 means no downlink support

- Set the periodic status timer in seconds, 0 means no periodic tasks

- After changing gateway parameters, you need to reboot for changes to take effect.

- Configured for LoRaWAN
  - TTIN cloud
  - ChirpStack cloud

- Gateway ID 0000B827EBEFCA46
- Gateway ID MD5 hashed 620d6c3e7916e30445086e2d3e46af1d
- IP address 192.168.2.3
- MAC address eth0: b8:27:eb:fe:ca:a6
- GPS coordinates Latitude : 43.314109
  Longitude : -0.363887
- wappkey not editable
- raw format false
- aes_lorawan for local decrypt
- aes for local decrypt
- loc for local decrypt
- downlink 0
- status 600
Main gateway configuration (3a)

- Configuring for LoRaWAN mode
  - LoRaWAN mode enables reception from LoRaWAN devices and LoRaWAN downlink support including Over-The-Air-Activation (OTAA)
  - Select a LoRaWAN cloud
    - TheThingNetwork (TTN)
    - Local or remote open-source ChirpStack
  - Use the **Configure for LoRaWAN** button to automatically change all relevant parameters for LoRaWAN mode

![Gateway configuration interface](image-url)
Main gateway configuration (3b)

- Limited LoRaWAN support with single-channel gateway
  - Only 1 frequency and 1 Spreading Factor, e.g. datarate
  - When building DIY LoRaWAN devices with LMIC for instance, you can easily make the datarate of device and gateway to be similar
  - For OTAA, join-request must use the same datarate than data uplink

- Full LoRaWAN with multi-channel gateway
  - With an SX1301-based concentrator shield, you can have full LoRaWAN
  - and still benefit from the versatility of our open gateway architecture to push to any cloud platforms as well as local edge processing capabilities
Main gateway configuration (4)

Network Server configuration section (open-source ChirpStack)

- Show whether ChirpStack is installed or not
- Enable/Disable message upload to the ChirpStack Network Server
  - 127.0.0.1 indicates a local ChirpStack Network Server
  - Note that you can also use a remote ChirpStack Network Server by indicating its IP address

If ChirpStack is installed, it can be started (and enabled at boot)

Open the local ChirpStack web page

- For more information about the ChirpStack open-source LoRaWAN network server, see https://www.chirpstack.io/overview/
- For more information on using ChirpStack with our framework, see https://github.com/CongducPham/LowCostLoRaGw/blob/master/gw_full_latest/scripts/chirpstack/README.md
- You can use the (local) ChirpStack Network Server to register gateways, create devices, handle LoRaWAN downlink, …
## ChirpStack example page (1)

### Local ChirpStack Applications page

![ChirpStack Application Page](image)

<table>
<thead>
<tr>
<th>Last seen</th>
<th>Device name</th>
<th>Device EUI</th>
<th>Link margin</th>
<th>Battery</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 days ago</td>
<td>danang_software_park</td>
<td>170ac0d7d681c5a5</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>a day ago</td>
<td>pau_testing_device</td>
<td>4f93fe6025b77c2</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>12 days ago</td>
<td>pau_testing_c1aa_device</td>
<td>0086a90c8d4a862</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

**Rows per page**: 10  
**1-3 of 3**
ChirpStack example page (2)

Local ChirpStack Device/Data page

![ChirpStack example page](image-url)
Main gateway configuration (5)

- Gateway email alerting section

- Enter your mail address for sending emails
- The SMTP mail server to send emails
- A list of email recipient addresses to receive alert notifications
- Your email account password, what is displayed is the MD5 hash version
Main gateway configuration (6)

Gateway SMS alerting section (needs cellular)

- The SIM card pin code
- A list of mobile phone numbers to receive alert notifications
Main gateway configuration (7)

Generating **non-LoRaWAN** downlink messages

- The string to send. Can be specific commands for the device if it has been programmed/configured accordingly.

Submit will generate in the downlink folder a `downlink-post.txt` file with the following entry for instance:

```json
{"status":"send_request","dst":2,"data":"hello from gateway"}
```

More info on [https://github.com/CongducPham/LowCostLoRaGw/blob/master/gw_full_latest/README-downlink.md](https://github.com/CongducPham/LowCostLoRaGw/blob/master/gw_full_latest/README-downlink.md)
Main gateway configuration (8)

Gateway log files section

1. Select this tab

(2) Click to start the generation of a copy of the log files

Then, this is the link to the entire post-processing.log file

And this is the link to an extract containing the last 500 lines of post-processing.log file
Get gateway log files

- The option is a convenient way for an end-user to obtain the log file that can be sent (via mail for instance) to an experienced user for analysis or debug purposes.
- The entire *post-processing.log* file can be obtained, or only the last 500 lines.
- A simple packet logger page is more suitable to check in real time whether packets are received or not, see next slide.
Simple packet logger

- Real-time packet logger

Display the packet logger

Show in real-time the last 20 packet receptions

LoRaWAN OTAA Packet from newly joined device: 0x2601298D

Non-LoRaWAN From src=6
LoRaWAN ABP From 0x26011721
LoRaWAN OTAA join-request
LoRaWAN ABP From 0x26041F24

Gateway Web Admin

Gateway Configuration
Gateway Update
System

Gateway Web Admin

Gateway Web Admin
Gateway update

- The gateway will be updated to the latest version
- Internet access for the gateway is necessary
- The update procedure can easily be done with the web admin interface, connect to the gateway WiFi first

The update steps are

1. Full Update
2. Basic Config
3. Update Web Interface
Gateway update page

Gateway update section

Install a new gateway by removing the existing *lora_gateway* folder, all existing configuration files will be overwritten.

If you install a new gateway with our SD card image, you can use this option.

Can download and install a file in the *lora_gateway* folder. A link to a file should be provided, e.g. a Dropbox link.

Update with latest version on github, all your configuration files will be kept. This is the recommended option.

Compile and configure the gateway (to set the gateway id & the WiFi access point SSID). This is also required if you install a new gateway using the provided SD card image. It is recommended to run *Basic config* right after *Full update* or *New installation*.

Update the web admin interface after an update of the distribution to install the last version of the web admin interface.

It is recommended to run *Update web admin* right after *Full update* or *New installation*.

Then reload the page.
Software version number

Gateway Update

- New installation
- Full update
- Basic config
- Download and install a file
- Update web admin interface

Run Basic config after any update and reboot for new version to be applied.

- Install latest version of gateway. erasing all existing configuration file.
  Custom SSID will be preserved. May take minutes, wait for finish notification.

Git version: 476. Installed version: 476. Date of current distribution is 2020-01-07 15:50:37.937685972 +0100

- The software version number on github and the installed version number are displayed
- Click on Test Internet to obtain the latest software version number on github

Online. Got github version number. 2019-12-02T13:44:29 [online] Test Internet pkt logger Reboot Shutdown
Download & install a file

- The option is a convenient way to install a configuration file.

- For instance, a customized `radio.makefile` file can be edited by an experienced user, then put on Dropbox and the link provided to an end-user (mail, SMS,...)

- When providing a link to a `.zip` file, the archive content will be installed.

- After installation, the end-user can use "Basic config" to recompile the gateway program and then reboot.
Gateway cloud pages

- Gateway cloud configuration section

Provides a quick and easy way to configure selected clouds.

If the server is unavailable/unreachable, you can see it immediately.

The last upload with a given cloud is indicated.

The cloud configuration page is very basic. It is expected that if you want to have more advanced cloud management, you have to use `ssh` to connect to the gateway and configure it by editing the `clouds.json` file.
Gateway WAZIUP cloud

- Configuring WAZIUP cloud

The WAZIUP cloud tab is only available when key_WAZIUP.py is found.

WAZIUP cloud uses FIWARE platform with the possibility to define domains. The domain will be defined as project_name+'-'+organization_name+service_tree, e.g. waziup-UPPA-TESTS if:
- project_name is waziup,
- organization_name is UPPA,
- service_tree is -TESTS
service_tree can be empty otherwise it must begin with a '-'.

The device id will be organization_name+service_tree+"_Sensor"+device_addr. For instance, for sensor 2 hosted by UPPA: UPPA-TESTS_Sensor2.

Username and password of the WAZIUP account. If username is "guest" then all data will be public.
Gateway system configuration (1)

- Gateway WiFi access point

Set the gateway's access point SSID (should normally be pre-configured, see Update section)

Also allow to define/change the WiFi access point password

Default SSID is
WAZIUP_PI_GW_XXXXXXXXXXXX
with the 6 bytes of the gateway network interface (e.g. B827EB84C456)

If you indicate a customized SSID, it will be preserved when the gateway is updated.

If you want to get back to the default SSID, just copy/paste from here
Gateway system configuration (2)

- Configure as WiFi client

Configure the gateway as WiFi client to connect to an existing WiFi network. Changes will take effect after reboot.

Warning: if a valid WiFi network is not configured you will not be able to connect through the gateway's access point anymore. If that happens, use wired Ethernet to switch back to access point mode.
Gateway system configuration (3)

Configure as WiFi Access Point

Configure the gateway as Access Point

Changes will take effect after reboot

Switch to AP mode immediately, you may loose connection with the gateway

Warning: Internet connectivity should then be provided by wired Ethernet or 2G/3G.
Warning: If using the "now" mode, you may lose current connection. Connect to gateway’s access point WiFi.
Gateway system configuration (4)

- Configure cellular for Internet access

System

Configure cellular settings

- Cellular is through a USB dongle
- Cellular is through the Loranga board
- LoRa+cellular
- Select 2G or 3G version

Gateway is acting as WiFi Access Point

<table>
<thead>
<tr>
<th>Dongle on boot</th>
<th>false</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loranga on boot</td>
<td>false</td>
</tr>
<tr>
<td>Loranga 3G/2G</td>
<td>2G</td>
</tr>
</tbody>
</table>
Run the RaspAP module

- Run the RaspAP web module from https://github.com/billz/raspap-webgui

Default login is **admin** and default password is **secret**
Gateway system configuration (6)

- RaspAP can configure some networking functions. It can be useful for dynamically select WiFi networks.

- However, it is recommended to use our web admin interface to control WiFi client <-> Access Mode feature.
Configure auth for web admin interface

Change both the login and password to access the web admin interface. Default login is admin and default password is loragateway.