Legend

[$] = A Paid Feature (requires unlock code)

Download & Install

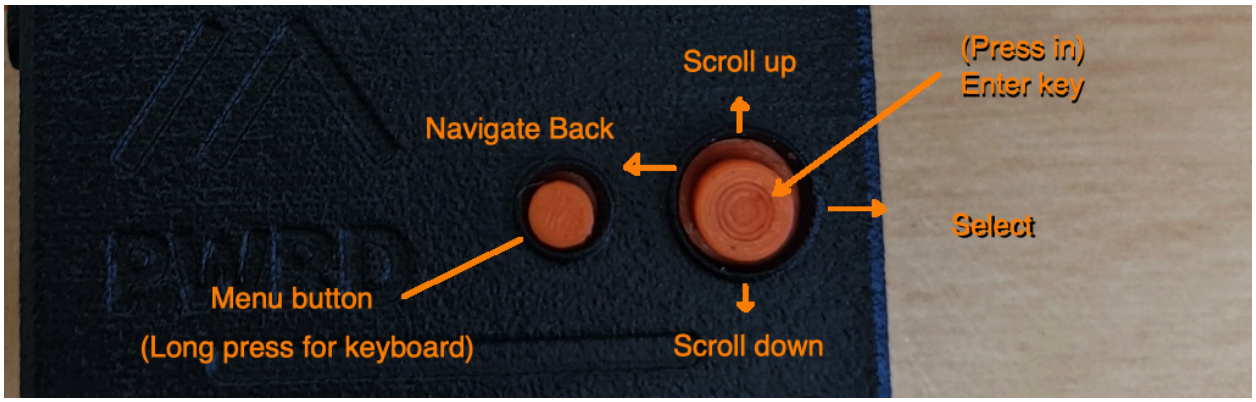
To install (also called *flashing*) just go to the MeshCore webflasher:
https://flasher.meshcore.io/seeed-studio-wio-tracker-l1-pro/

And connect your device via USB cable.

NOTE: You may need to first do the ‘Erase Flash’ step, especially if the device had some other firmware on it.

UI

The UI v10.+ for the L1 Pro uses the button + joystick for input:



Lists

A lot of screens involve vertically arranged lists like the Discover screen:

You can select an item using the joystick up/down, then joystick right to select. The small *arrow* icons at the left-hand side indicate if more content is further down/up.

TIP: you can press and hold the joystick up or down to automatically keep scrolling.

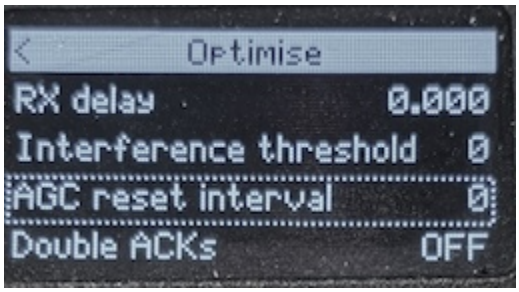
Menus

To open context menus, short press the left button:

You can select a menu item by scrolling up/down with the joystick, then pressing joystick right (or in), in. To close/cancel the context menu, just press joystick left (or press menu button again).

Input Fields

Many screens have a number of input fields, vertically arranged:



You can move the current selection up/down with the joystick.

Texboxes

Text or number textboxes, you press joystick right to open the on-screen keyboard:

Press the menu button to cycle through the different keyboard modes (lower, upper, symbols). Long-press the menu button to exit the on-screen keyboard, or select the ‘tick’.

TIP: You can press and hold the joystick left or right to keep moving in that direction. Also, the letter/symbol selection will wrap around.

Checkboxes/Multi-select boxes

These can be ON/OFF values, or anything where selecting one of a list of items. When the field is selected, to toggle through the possible values just press **joystick right**. (can be repeated)

Saving

To save changes, or submit information on these screens, it usually involves pressing the **ENTER** key. (ie. press joystick in)

Navigate Back

Just press the **joystick left** to navigate back to previous screen.

Screen On/Off

When screen is off, just press any button to turn screen on.
Screen will turn off after an interval of inactivity. (configurable in Display settings)

Network Profiles

The Ripple firmware supports multiple profiles, so you can switch to different networks, where each one is *sandboxed*, ie. has separate user identity (key-pair), contacts, preferences, etc.

The start-up wizard will walk you through setting up the primary network profile, by asking to select a radio preset from a list (or you can select **custom** and provide custom radio params).

Once you have set up the primary profile, you can modify the radio params, or set up new profiles by opening the Home screen's context menu, then select the **Networks** menu.

Home Screen

This shows all your contacts, group channels, and Discover arranged in a tree, for each network profile you have.

Titlebar

The titlebar shows current profile user name, clock, and toggles between battery and GPS satellite count.

Context Menu

Press the menu button to open the context menu. Note, this has **system/device** menus only. Ie. settings that are typically *global* and not tied to the current Network Profile!

First Time Setup (!)

The first time you setup your device, you should do the following:

- Set the device **Timezone**. Open context menu from home screen, then select Timezone. Set the *minutes* offset from UTC.
- In rare cases, some times the device **GPS Config** needs to be set. The default is usually fine, but some devices may have a different GPS installed, which need a custom baud rate setting. (if you open the GPS Info screen, check that there is a spinning bar on the titlebar. If so, then the GPS data is being received OK)

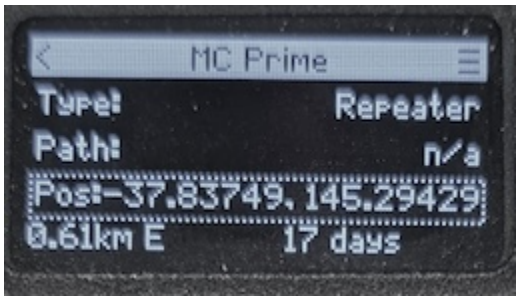
For first time a Network Profile is created, you need to do the following:

- Set your **Identity**. Open the profile menu (is typically named ‘MeshCore’ on the home List), then select Identity. Change the name from ‘NONAME’ to some display name (others will see this). Then press ENTER key to save.
- Select the **Permissions** menu, if you want to change the default telemetry permission. (ie. if your contacts are allowed to pull telemetry from your device)

Discover Contacts

A contact can be any of the node types: Chat device, Repeater, Room Server, or Sensor. These are all added to your device via an *advert* packet (transmitted over the radio). These are passively collected and shown in the **Discover** screen. (from Home, select Discover item)

To add a discovered node to your home screen (ie. favourites), select it from the list to show the node details screen:



Then select the **Add to Contacts** menu item. If this node is already in your contacts, the menu will instead be **Remove from Contacts**.

Sharing Your Identity

If you want to send your device details via an *advert* packet, just go into the **Discover** screen, then select the **Send ID Local** menu item. This sends a zero-hop advert of your device to devices around you.

If you want to broadcast your device to the *whole mesh*, select the **Send ID Broadcast** menu item.

Sharing Nodes With Others

If you have a node in the Discover list (not necessarily added to favourites/home), you can share that with a nearby device by selecting the node, then in the node details screen select the **Share…** menu. This will just re-transmit its advert packet verbatim, but just zero-hop (ie. just to nearby devices)

Discover Nearby Devices

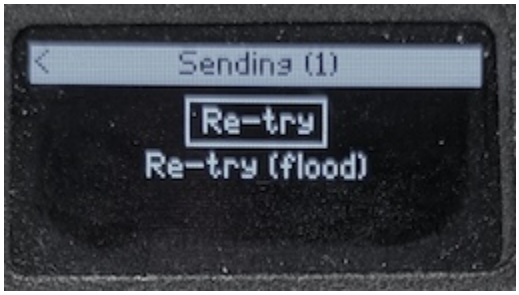
If you select the **Discover** > **Scan Local…** menu, a zero-hop request is sent to nearby devices. This is typically for repeater discovery, but can potentially be other node types. If other nodes

are within reach, and are configured to respond (some don't), then you will see items appear in the list. (will also show the SNR of response)

Conversations

For each chat contact there is a conversation screen, which keeps your message history:

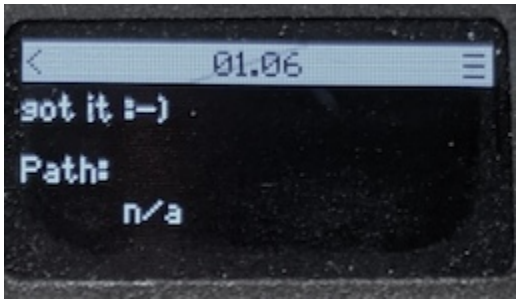
The dotted rectangle shows current selection. The bottom area is a textbox for input. **Long press** the **menu button** to compose your messages in the on-screen keyboard. When back at the conversation screen, press **ENTER to send**. While waiting for the acknowledgment from the other device, you will see the **Sending** screen. If this times out, you can re-try with another *direct path* attempt, or you can revert to *flood mode* attempt (in case the path has changed):



NOTE: at present only 4 attempts are allowed.

TIP: pressing joystick **right** when input textbox is selected will show a list of **Canned Messages** to select from.

TIP: For long incoming messages, just scroll up into the message history, and the messages are automatically scrolled horizontally.
Press joystick **right** to the show the Message Details screen:



Here you can get more info, like the timestamp (in titlebar), and also the *path* the message took to get to your device (can be *n/a* if unknown). There are also extra menu items like **Add Region…** if a special "[region: …]" encoding is present in the message.

Automatic Telemetry [$]

When you navigate into the conversation screen and you have a *direct path* to that node, a telemetry request is automatically sent, and if a response is received, the *WiFi* icon is shown on the top-left of the titlebar, so you can quickly see if they are online and reachable.

Also, if they have allowed GPS telemetry permission, their location is recorded and you will see a direction/distance estimation (from your location) rendered in titlebar.

Full Telemetry

If you select the **Get Telemetry…** menu item, a request is sent, and if a response is received, the *full* telemetry details are shown as a text message.

Group Channels

You can configure up to 6 group channels, from the network profile menu. The **Public** one is auto-enabled for you (on slot #1), and is configured with a widely known Pre-Shared Key. So, even though all group channel messages are symmetrically encrypted, consider all Public channel activity to be *insecure*. There is also no way (at present) to authenticate *senders* in the group channels, so beware. It is just an easy way to interact with others out there.

You can, however, setup your own custom group channels, with a key that only you and your friends know. This is much more secure, but note that there is still no *sender* authentication.

Channel Setup

From the network profile menu, select one of the Channel menus, then select **Enable** from the context menu:

Just give it a name, then enter a key (either in Hex or Base64). If you want a new, random key created for you, just select from the context menu **New 128-bit key**. You then share this key with others in your group.

If you start the channel name with a '#' character, the channel key is generated automatically. These are *hashtag channels*, and are an easy way to setup alternatives to the **public** channel, where they have some specific *topic*. These are still *public* channels, and thus insecure, as they will be using a well-known key.

Group Chats

From the home screen, you should then see your private channel listed (under Discover). Just select to go into the group chat screen. One difference with group messages is there are **no ACKs** sent by recipients, and there is *no guarantee that anyone will receive* your message! There is a *confirmations* feature, though, to help indicate if your message did, indeed, get *out there*. If a repeater forwards your message, and your device hears this re-transmission, then a counter will be displayed in a box:

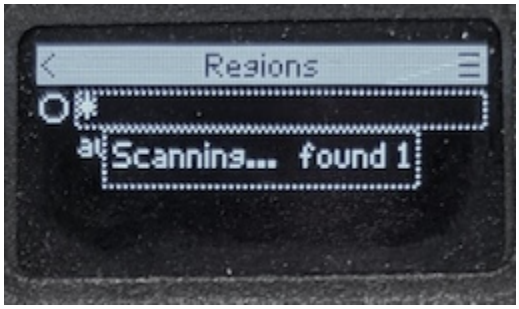
If you select your message (with the confirmations counter) and navigate to the message details screen, the list will show a "Heard By" list (instead of Path, for incoming messages). ie. it shows a list of repeaters which re-transmitted your message.

Channel Message Scope

You can now set a region *Scope* on various group chat channels, to limit how far messages you send will flood to.

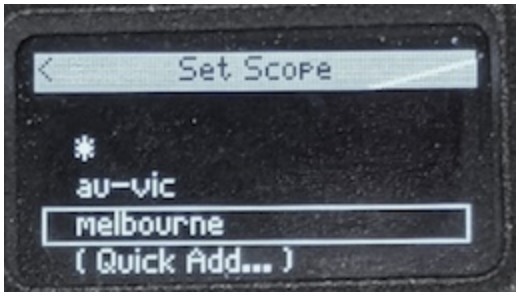
What you will need to do first is define the region names into a new **Regions** screen (from the network profile menu):

You can do this manually with the **Add New** menu, but a cool new feature of the repeater v1.12.0 firmware is support for new request types, and one is to auto-discover regions in your area! To use this, you select the **Scan Local** menu:



This uses the new Discover request, and any repeaters within reach respond with a list of regions which they are configured to allow. These are then collated, and if any are *not* in your device's list, then you are prompted if you wish to add:

Once you have regions defined, when you go into any of the group channel chat screens, you can use the new **Set Scope** menu, to select which region you want to limit *messages you send.* (you can still *receive* messages from anywhere in the mesh)



The scope preference is saved per group channel, and you can change it at any time.

Rooms

There is a node type called a *Room Server*, which is a very simple bulletin board system, where you can post messages and others can read them at a later time. Is a very useful store-and-forward system, for leaving messages for others who may be offline. When you select a Room from home screen, you will initially be prompted to enter either the *admin* or *guest* password:

The same out-path rules apply, as with other contacts. So, if you are in a new location, you may need to select the **Path** menu, then select **Reset Path**. After tapping Connect (or press ENTER), and login is successful, the screen then changes to the usual conversation UI. (see above)

The room server will then typically be attempting to push unsynced messages to your device. This is quite a slow process, so be patient.

Posting a message is simply a matter of typing and pressing ENTER, like with a contact. If the room server successfully receives and queues the message, it sends an ACK like a client would, and your post will scroll up into the conversation list.

NOTE: at present the room server only holds the last 32 posts, so your device will only receive up to the last 32 missed messages.

[$]*:* if you are the admin of the room server, and you entered the *admin* password here, you will also be able to enter a second, reserved, area via the **Admin CLI** menu item. The CLI screen is

then entered, where you can instead type CLI commands, like '`ver`' or '`set` ... ', etc. The command messages are slightly different in that the server does *not* send ACKs, instead sending a reply message. If no reply comes back, then you just have to re-try sending the command. It's a fairly basic, but powerful feature for doing remote admin on your node.

Repeater Admin - [$]

You can login to your repeaters remotely. They also support *guest* and *admin* passwords, where guests can only get telemetry or request the current stats via the **Get Stats** menu item. The CLI commands are (mostly) the same as for room servers. See the CLI Reference Document here.

Similar to client contacts, when you navigate into repeater screen (or room server, actually) the same automatic telemetry request is sent. This is really handy and convenient way to quickly check if the repeater is healthy/online, and to get the current battery voltage, which is then displayed in the titlebar.

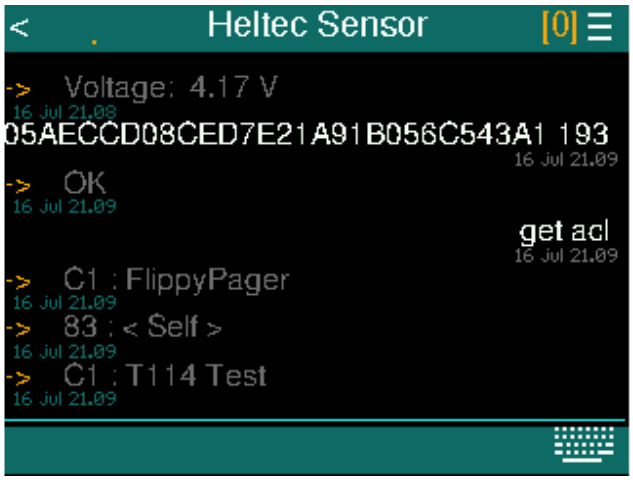
Some CLI commands are now intercepted and a binary request/response is used instead, with the result converted to a nice human-readable format. These include: `setperm`, `neighbors`, `get`, `get acl`

The canned message selection is customised for the command-line UI. When the textbox is blank, and you open the canned message list, you get to select from common CLI commands:

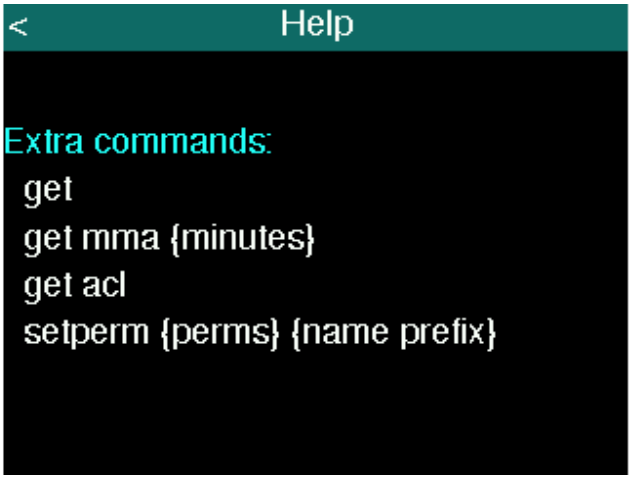
If the textbox has, say, '`get`' and you open canned messages again, you then get options listed that are parameters to the '`get`' command:

Sensor Admin - [$]

Sensor nodes have a firmware similar to repeater and room server, but specialised for using various sensor hardware attached (like temperature sensor, for instance). Sensor nodes are not intended to be *public*, however, and instead use a persisted *ACL* (Access Control List). Initially, this list is empty and the admin must perform a Login using the pre-configured admin password (like with a repeater). After selecting the sensor and navigating into the sensor screen, you initially need to select the **Admin Sign Up** menu, and enter admin password. If successful you are then shown a command-line interface:



Sensor nodes support the common CLI Commands, but also have extra, sensor-specific commands, which you can get quick info on with the **Help** menu:



The `get` command, simply sends telemetry request. (the response is parsed, and sensor values displayed as a text reply).

The `get mma` command is for min-max-average queries, for the last *x* minutes.

The `get acl` command is for showing who currently has access to this node. The list returned will have {permission-bits} : {name}

The `setperm` command is for adding/updating/removing an entry from the ACL. {perms} is either the numeric permission bits, or for convenience can be letters: **a** (for Admin), **w** (for Write), **l** (want Low pri alerts), **h** (want High pri alerts)

Permission-bits are:

- lower 2 bits: role (1: read_only, 2: write, 3: admin)
- middle 4 bits: unused
- Bit 6: wants Low pri alerts
- Bit 7: wants High pri alerts

To remove a node from ACL, use `setperm 0 {name prefix}`

When a sensor node detects some alert condition, it will send alert messages to *all* devices in its ACL which have the needed Alert permission (Lo or Hi). Low priority alerts will only make 1 send attempt per node, but High priority alerts will wait for an ACK from each node, and re-try. Alerts are also rendered in a special orange so they stand out.

Custom Paths

Each of the conversation/detail screens (for clients, repeaters, rooms, or sensors) should have a **Path...** menu. Here you can modify the current *out-path* for this node:

In the *custom path* textbox you can enter a comma-separated path hash list for completely custom path to use (you need to know the hex-encoded path hashes). To save having to re-type you can scroll down to the **Save** button and assign a name for this path, eg. 'Via roof'. Once saved, you can then re-use them at later times, or for other contacts.

The other quick actions you can do are:

- Flood (reset) - this resets the out-path, forcing next sends to be done flood-mode
- Direct (zero hop) - sets the out-path to direct, ie. expects node to be in immediate area

Other items in the list will be the various *named paths* which you have saved, starting with a ">". Select these to re-use a named path.