LoRa + Meshtastic: Encrypted messaging from your phone without the internet

by Mike Dank + Iffy Books
2022

The Meshastic project, founded in early 2020, uses inexpensive LoRa radios to create an off-grid mesh network for communication. If you've ever been hiking or camping in the wilderness away from cell towers, or at locations like music festivals where infrastructure is often congested from a high volume of use, you may understand the need for a platform that does not rely on traditional communication services.

Meshtastic is completely off-grid, and doesn't rely on any existing networks or infrastructure. It does so using LoRa (short for **Lo**ng **Ra**nge) radios that are advertised as being able to transmit data at a typical range of 10km (~6 miles) in areas with a clear line of sight, and some have reported communicating over longer distances. In a city environment with many obstructions, your range is more likely to be 1–3 blocks.

LoRa implements chirp spread spectrum (CSS) modulation, meaning that it is robust to channel noise and resistant to multi-path fading, resulting in low interference.

It is important to note that LoRa is not designed for high-speed data transmission, and the hardware is only capable of transmitting between 250 bits/s and 27 kbits/s. At this speed, LoRa becomes ideal for text communication via realtime chat as well as location beaconing, though it has also been adopted for use in IoT and sensor networks.

Meshtastic uses LoRa technology to provide a communication platform ideal for small groups of people who wish to have private conversations. This can be ideal for a temporary setup where there is no traditional infrastructure to use, or a permanent setup with fixed and mobile nodes operating in a particular neighborhood.

BUILDING A MESH

Each node in a Meshastic network is composed of a LoRa radio device, typically paired via Bluetooth to a mobile phone. Once paired, the host device can run the Meshtastic application to send and receive messages on the network.

Each node in the Meshtastic network additionally acts as a relay for other nodes. For example, if Alice and Bob want to send messages to one another, but are physically too far apart to make a connection, their data can automatically be routed through a third user Carlos who is physically between and in range of both Alice and Bob. This means that even the most distant nodes on the network have the ability to communicate with all other nodes, even if they are not nearby.
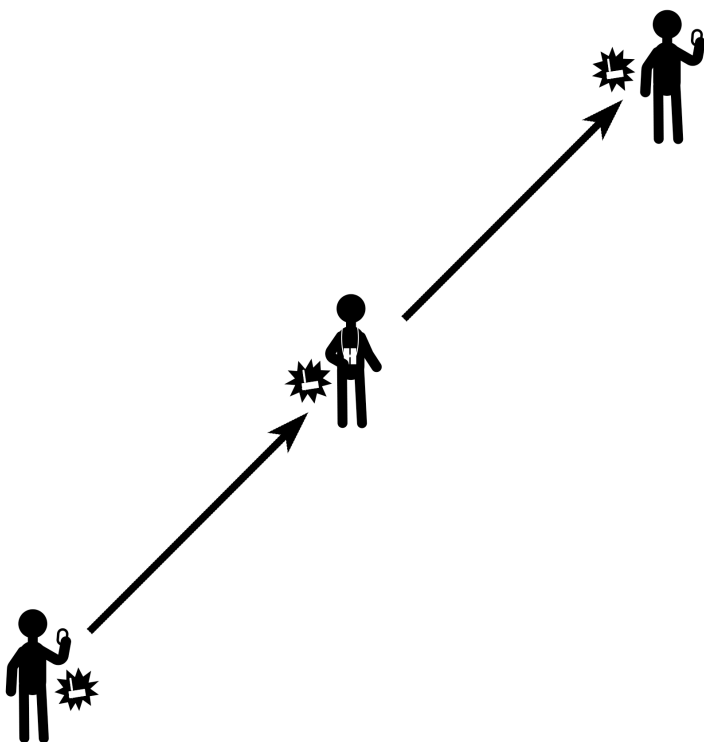
Nodes can also be set up as standalone repeaters that simply route traffic through the network without being connected to a host device. This allows nodes to be operated in an isolated or otherwise fixed position, supplying connection to the greater network for others nearby. This can be an ideal configuration for solar-powered nodes that are elevated for line-of-sight connection, requiring little to no maintenance from the operator.

PRIVACY

By default, a new Meshtastic node is configured to use a general chat channel that everyone has access to. On the channel tab, you can create a new channel by typing in a name and optionally change the bandwidth. With this option

you can choose to have your messages sent faster, but over a lower distance or vice versa. I prefer to keep the option set to allow for the longest distance and slowest speed. A private address for the new channel you created can be sent to others via a link or by scanning a QR code on the screen. Anyone who doesn't have the private address cannot join the channel or decrypt the messages within it.

If you want, Meshtastic can share your current GPS coordinates with everyone else on the channel you're using. Sharing your location can be helpful if you're in a remote area or navigating a large crowd. If you're using Meshtastic from home, we recommend turning off GPS sharing so you don't dox yourself.

SUPPLIES

Setting up a Meshtastic node is relatively inexpensive, assuming you already have a host device you can use to interact with the radio. I recommend getting materials for two nodes so you can adequately test an end-to-end connection.

Currently, there are Meshtastic applications for both Android and iOS, though the iOS application is in beta. Alternatively, there is a Meshtastic-python library you can use to interface with a LoRa radio via PC, but you will likely need some prior Python language experience to make full use of it. Further, there is a serial interface and web interfaces to access Methtastic from a browser, though the latter may currently be unstable. There is no current turnkey application for PC use.

When you purchase your board, make sure to purchase one that operates in a frequency you are allowed to

transmit on in the country you are operating in. As I am in the United States, I purchased a 915MHz model that uses an unlicensed band here which is safe to use.
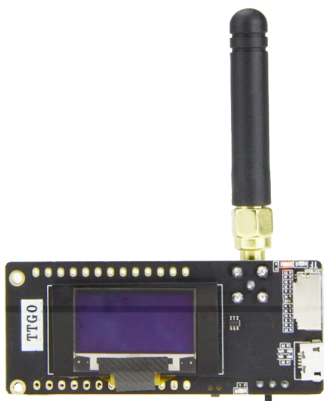
LILYGO LORA32 SETUP

1. Screw the included antenna onto the SMA connector on the back of the board. If you turn on your device without an antenna attached, you can potentially damage the board.

2. Connect a microUSB cable into the board and plug the other end into a power source. You can use a USB power bank, a phone charger, or a USB port on your computer. You'll see the Meshtastic logo on the LCD screen, followed by a screen that looks like this:
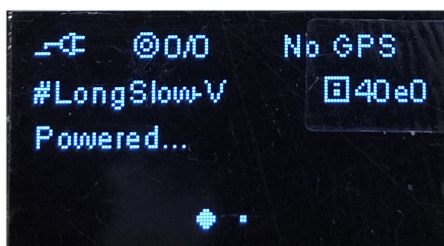
At the top right of the screen you'll see a 4-digit ID code for your device. In this case the device's ID is **40e0**.

HELTEC LORA32 SETUP

1. Connect the included antenna onto the IPEX-1 connector on the back of the board. You can snap it on with your fingernail, or

2. Connect a microUSB cable into the board and plug the other end into a power source. You can use a USB power bank, a phone charger, or a USB port on your computer. You'll see the Meshtastic logo on the LCD screen, followed by a screen that looks like this:
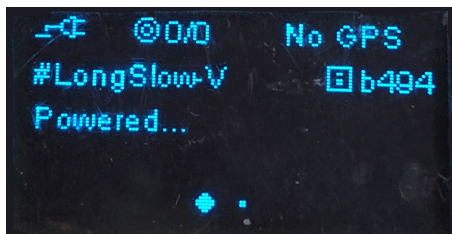
At the top right of the screen you'll see a 4-digit ID code for your device. In this case the device's ID is **b494**.

LILYGO T-BEAM SETUP

The T-Beam package includes an OLED screen that must be soldered in place (with included header pins) if you would like to utilize the display. The screen is not a requirement for the board to function, though it is nice to have for Bluetooth pairing as well as troubleshooting and diagnostics. If you choose not to use the display, you will have to open a console session with the board (via USB) to find the pairing key in the boot log. Information for doing this is available from github.com/meshtastic/Meshtastic-device.

The T-Beam has a built-in battery holder on the back to accommodate a common 18650 battery. Even name-brand 18650s are relatively inexpensive and should provide great battery life, meaning you can go days without needing to recharge. The T-Beam has a micoUSB jack which functions as a way to charge the battery, or power the board directly in the absence of one.

Upon receiving my T-Beams, I went ahead and soldered the headers in place, and soldered the OLED directly to the headers on the board. At a minimum, there are only four pins requiring connection to the board, so this is a quick task, though you can go ahead and solder the full set of headers in place if you'd like to increase stability. Further, if you have female-to-female dupont jumpers, you could solder separate headers to the board and the screen and then connect them together via jumper wires. This makes the screen detachable so you can run the node without it in the future (likely saving some battery life).

After this, the included antenna can be screwed in and the 18650 battery can be inserted into the board. There is no on/off switch so if the battery is retaining any charge the board will power up. At this point, you can plug the microUSB cable into the board and connect the other end to a power adapter or PC in order to charge up the battery.
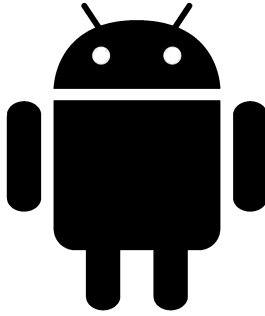
ANDROID QUICK START

Go to the Google Play Store or the Amazon Appstore and search for "Meshtastic." Install the app.

Or download the .apk from GitHub and sideload it: https://github.com/meshtastic/Meshtastic-Android/ *or* https://iffybooks.net/link/5a11

Open the Meshtastic app and tap the **plus sign** (+) in the bottom right corner. You'll be prompted to share your location to connect via Bluetooth (for some reason). Tap the plus sign again and your phone will start scanning for LoRa devices.
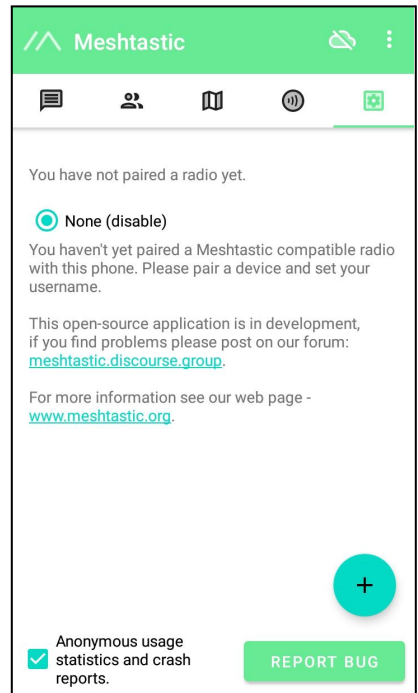
Find your device using its four-character ID. Tap the radio button next to it to start pairing.
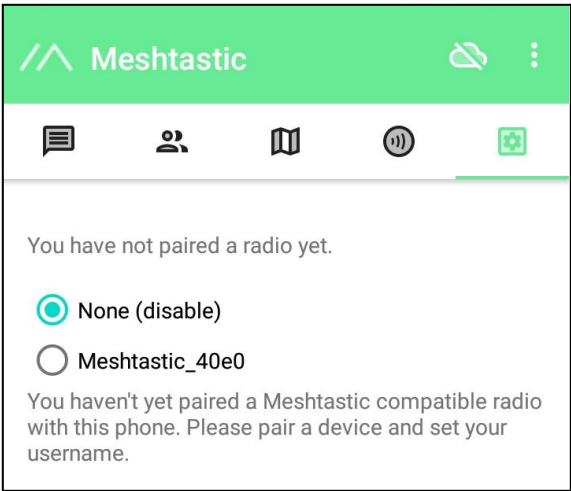
Type the six-digit number from your LoRa device's screen and tap **OK**.
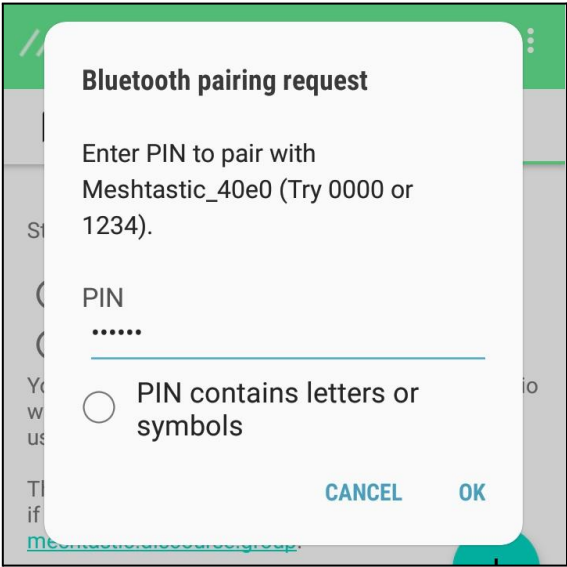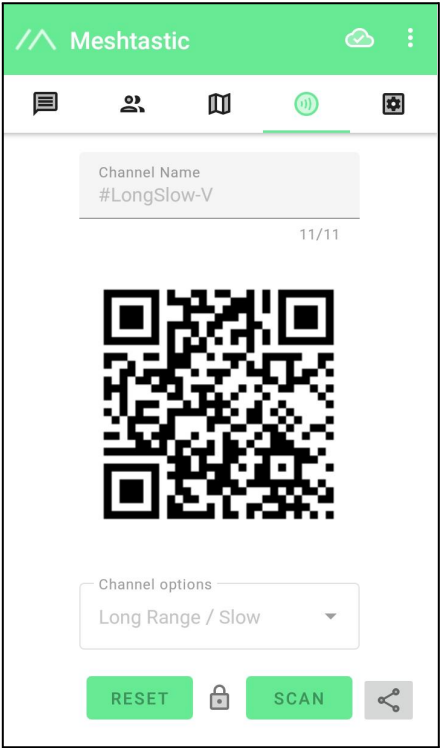
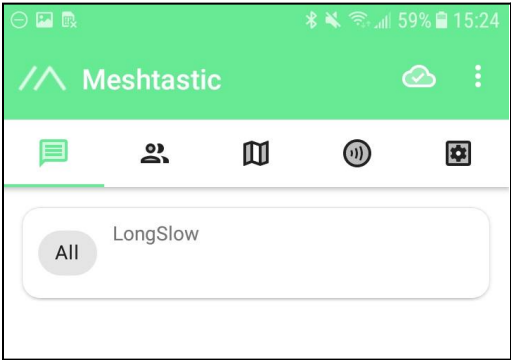Select your region and set a name for your node.
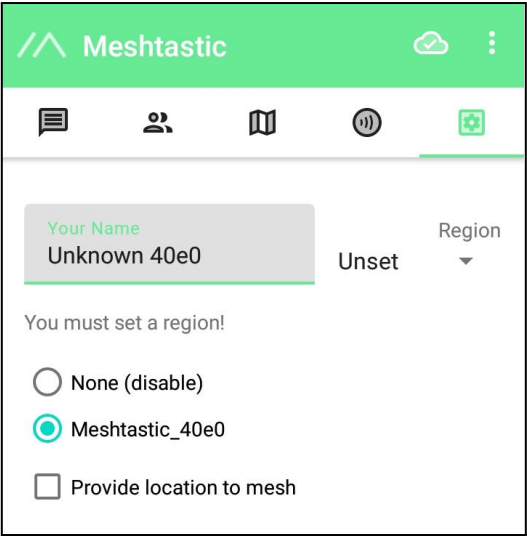
To set a new private key, tap the circular navigation icon at the top of the screen.

Tap **Scan** to join a channel by scanning QR code. Or tap **Reset** to create a new private key.

Tap the message icon on the left side to get to the chat interface.

iOS QUICK START

The Meshtastic iOS app is currently in beta (as of August 2022), so you'll need to use TestFlight to install the app. Search for "TestFlight" in the App Store and install it.

Next, go to this URL to install Meshtastic: https://testflight.apple.com/join/c8nNl8q1

Once the Meshtastic app is installed, you'll need to downgrade to version 1.2.53. (The most recent version of the app only works with firmware version 1.3 and above, which is unstable as of August 2022.)
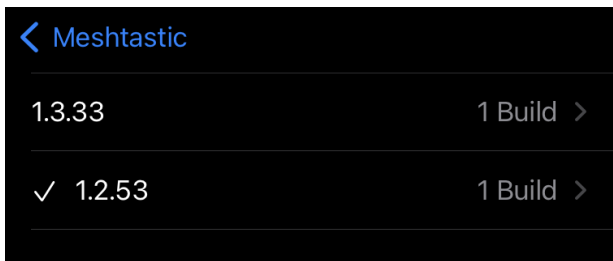
Open TestFlight. Long tap the Meshtastic icon and you'll see a window like the one below. Tap **more** in the bottom right corner.
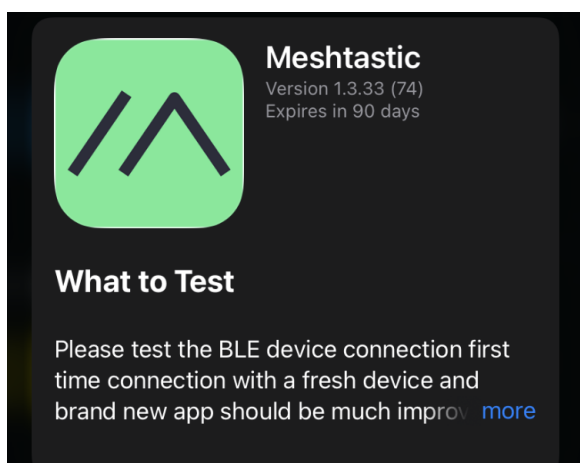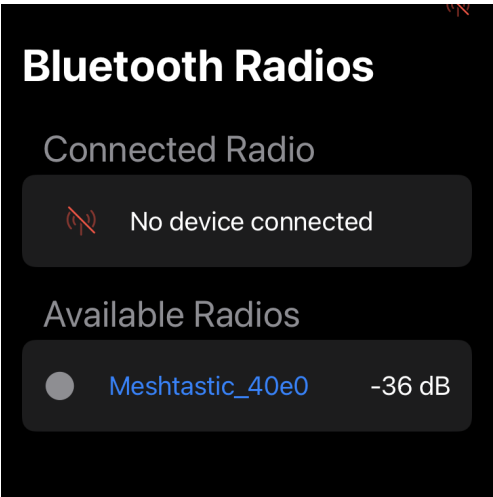
Now tap **Previous Builds**.
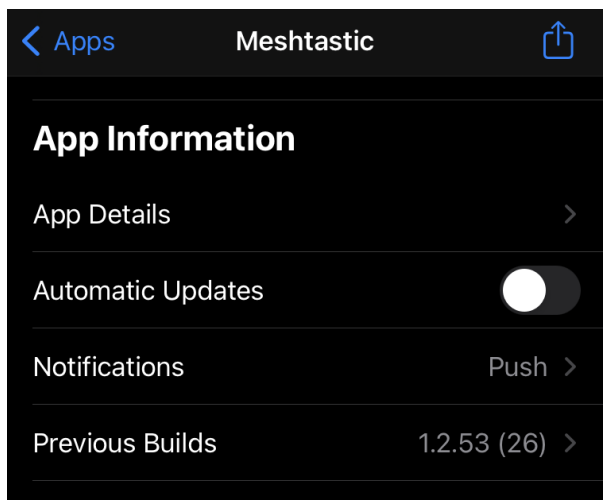
Tap **1.2.53** to install the older version. (It's already installed in the screen capture below.)

Make sure Bluetooth is enabled on your device, and open the Meshtastic app. You should see a list of Meshtastic nodes within Bluetooth range.
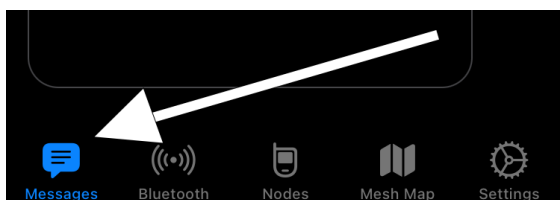

Find your device using its four-character ID and tap on it. Type the six-digit number from your device's screen and tap **Pair**.
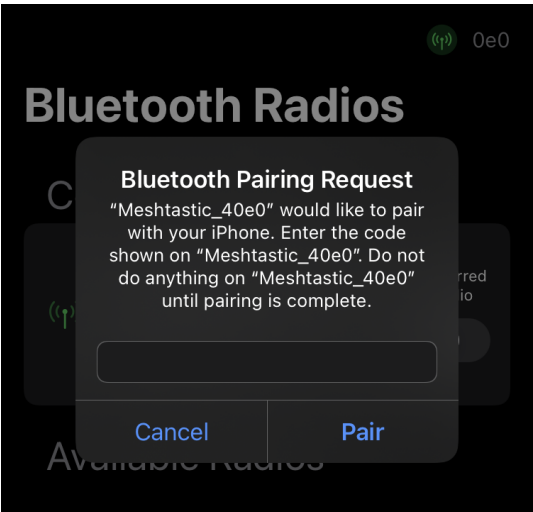
Your LoRa device will appear in the list of connected radios. If you're planning to make this your primary device, tap the "Preferred Radio" toggle switch.
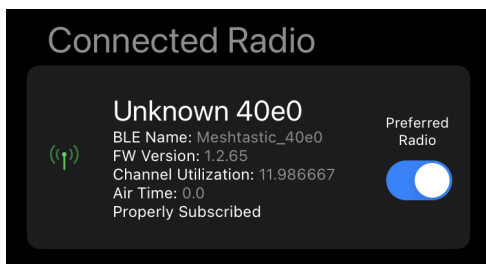
Tap the "Messages" icon in the bottom left corner to get to the chat interface.

As of August 2022, the Meshtastic iOS app doesn't support switching to a private encryption key from within the app. In the next section you'll learn to use the command line to set your own private key.
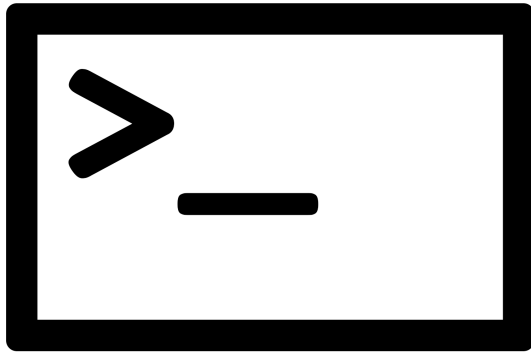
COMMAND-LINE SETUP

Whether you're using Android or iOS, using the command-line makes it possible to set your device preferences using a config file on your computer. This is especially useful if you're setting up two or more devices with the same settings.

First, go to the following URL and install the USB-to-serial drivers you'll need to communicate with your device. The links below include instructions for macOS, Windows, and Linux.

https://meshtastic.org/docs/getting-started/flashing-firmware/#install-usb-to-serial-drivers

or https://iffybooks.net/link/5a9u

If you're using a Heltec LoRa32 device, you'll need to install some files using the Arduino Board Manager:

https://heltec-automation-docs.readthedocs.io/en/latest/esp32/quick_start.html

or https://iffybooks.net/link/e95b

Before you use the Meshtastic command-line program, you'll need **Python 3** and the **pip** package manager. To check whether you have them, first open a terminal window. (If you're using macOS, open the Terminal app. In Windows you can use PowerShell.)

Type the following command and press enter:

```
python3 -m pip -V
```

If Python 3 and pip are installed, you'll see a version number for both. If you get an error message, you'll need to install them.

Install Python 3 on macOS:

https://docs.python-guide.org/starting/install3/osx

or https://iffybooks.net/link/bba2

Install Python 3 on Windows:

https://realpython.com/installing-python/#how-to-install-python-on-windows

or https://iffybooks.net/link/4f5e

Next, run the following two commands to install the Meshtastic command-line program:

```
python3 -m pip install --upgrade pytap2

python3 -m pip install --upgrade meshtastic
```

If you're using macOS, you may need to add **sudo** before each command. You'll be prompted to enter your password.

You can read more about the Meshtastic command-line tool here:
https://meshtastic.org/docs/software/python/python-installation
*or* https://iffybooks.net/a27e

FLASH YOUR LORA DEVICE

If your LoRa device already has the Meshtastic firmware installed, you can skip this section for now.

Follow the instructions at the following URL to install the Meshtastic Flasher app:

https://meshtastic.org/docs/getting-started/flashing-firmware/meshtastic-flasher

*or* https://iffybooks.net/link/1d37

Open the Meshtastic Flasher app. First click **Get Versions** to check for new versions of the Meshtastic firmware. Then connect your LoRa device to your computer with a microUSB cable and click **Detect Device**.
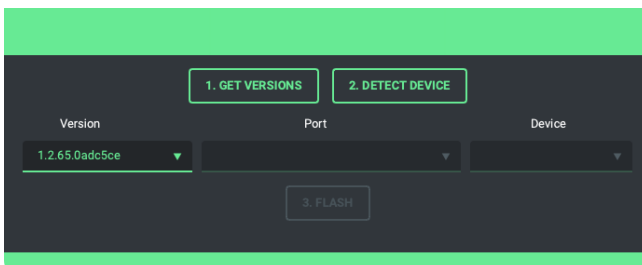
You'll see a popup window that says, "Does the device currently have Meshtastic version 1.2 or greater?" If Meshtastic is already installed on your device, click **Yes**.
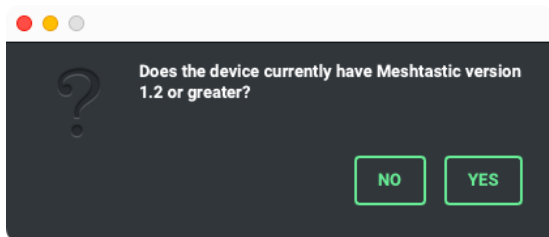
Click **Flash** to flash the Meshtastic firmware to your device. It may take a minute or two to finish.
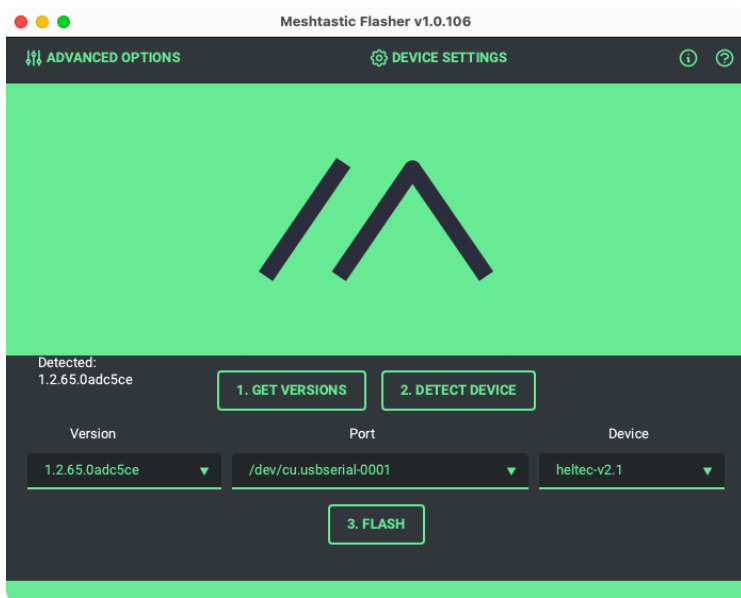
When flashing is complete, click **OK** to close the window.

CONFIGURE YOUR LORA DEVICE FROM THE COMMAND LINE

If you're using iOS, you'll need to use the Meshtastic command-line program to set the private key on your device. Even if you're using Android, you may find it helpful to store your channel URL (private key) and other device settings in a configuration file so you can keep track of them.

Here's an example config file to get you started, using the channel URL for the Iffy Books public chat channel:

```
owner: Iffy Test Unit
owner_short: ITU
channel_url:
https://www.meshtastic.org/d/#CiQYAyIgvc0rL4ZyTGFD
0qE7s2ptf9Mm6QQxXeedO2fpmBZ1xb0
user_prefs:
  region: US
  screen_on_secs: 60
  wait_bluetooth_secs: 120
  phone_timeout_secs: 1800
  position_broadcast_secs: 120
  mesh_sds_timeout_secs: 4294967295
  ls_secs: 300
  is_always_powered: 'true'
```

You can find the file above at the following URL:

https://gist.github.com/iffybooks/166f866d95f50c77473a 7afbea4f6e22

or https://iffybooks.net/link/98d7

Save your config options to a plaintext file called **config.yml**. Then use the Meshtastic CLI app to update the preferences on your LoRa device:

```
meshtastic --configure config.yml
```

You can read about Meshtastic device settings at the following URL:

https://meshtastic.org/docs/settings

CREATE A NEW PRIVATE KEY

You can start a new encrypted chat channel or join an existing one. To start a new private channel, run the command below to choose a random AES-256 key and display a shareable URL containing the key:

meshtastic --ch-set psk random --ch-index 0 --info

To see your channel URL (which contains the complete key), run the following command. Since the URL itself contains the private key in plaintext, you'll want to keep it secret.

meshtastic --info

To join an existing chat group, you can include the private key URL in your configuration file before updating the preferences. Or run a command like this one, using your shared URL:

```
meshtastic --seturl
https://www.meshtastic.org/d/#CiQYAyIgvc0rL4Zy
TGFD0qE7s2ptf9Mm6QQxXeedO2fpmBZ1xb0
```

Join the Iffy Books Public Meshtastic Channel!

If you're using Android, open the Meshtastic app and scan this QR code to join the channel:

If you're using iOS, go to the section of this zine titled "Configure your LoRa device from the command line."

Here's the complete channel URL, which should all be one line:

https://www.meshtastic.org/d/#CiQYAyIgvc0rL4ZyTGFD0qE7s2ptf9Mm6QQxXeedO2fpmBZ1xb0

Or find it here:

https://iffybooks.net/link/a361

Go to the "All" chat and say hi!