

# MeshTastic@SichFreun

## Sicherheitsfreunde Meshtastic Workshop

byteborg

2024-09-13

1 Motivation

2 Hardware

3 Software

4 Benutzen

# Motivation

- (Private) Kommunikation untereinander, unabhängig von Netzinfrastruktur
- Erfahrung mit digitalem Datenfunk sammeln
- Nerdiges Basteln
- Weil's geht

# Plattformen/Module

## Plattformen

- ESP32
- nrf52840
- RasPi 2040

## Radios

- Semtech SX1262/SX127x/SX1280
- HopeRF RFM950W

Als Radiochip will man eher den SX1262 haben, der ist empfindlicher und hat mehr Leistung die anderen.

# Auswahlkriterien für die Hardware

- Preis/Lieferbarkeit
- Innen-/Außenmontage?
- Antennenkonnektivität? (onboard IPEX, SMA für externe Antennen)
- Autarkie (GPS? Akku?)

# Verfügbare Bandpläne

Wir sind in Europa, also sind zwei Bandpläne für uns relevant:

Band	ERP max.	Duty Cycle	Auslastung
EU_433 (ISM)	10dBm (10mW)	100%	dicht
EU_868 (SRD)	27dBm (500mW)	10%	mittel/leicht

869,4-869,65MHz sind für Breitbandanwendungen aus dem Band herausgeschnitten.

869,525MHz ist Frequency Slot 1 bei Meshtastic und darf mit 500mW bei 10%iger Auslastung des Bandes senden. Das ist das Band, was wir wollen.

# Auswahlmatrix für die Hardware

Device	Billig	GPS	Akku	SMA	Display	Architektur
HELTEC LoRa32 v3	++	-	-/(+)	(+)	OLED	ESP32
LILYGO T-Beam	○	+	18650	(+)	OLED	ESP32
LILYGO T-Echo	-	++	++	IPEX	e-Ink	nrf52840
LILYGO T-LoRa 2.1	++	-	-/(+)	+	OLED	ESP32
RAK Starter Kit	-	-/(+)	-/(+)	IPEX	(OLED)	nrf52840

# Installation

- Antenne montieren (*Betrieb mit schlecht oder nicht montierter Antenne killt den Transceiver!!!*)
- USB-Verbindung mit Rechner herstellen
- <https://flash.meshtastic.org> aufrufen
- Gerät auswählen
- Letzte Stable-Version (Beta) auswählen
- Flash!
- Baudrate bei ESP32-Devices: 921600
- Bei Erstinstallation: Full Erase
- Go...



# Software/App

F-Droid



Google Play Store



Apple AppStore



Python

```
pip install -U meshtastic
```

Die Apps dienen zur Gerätekonfiguration und dienen als Oberfläche für Messaging, Nodeliste und Statusanzeige.

Die Python CLI kann das auch, eignet sich aber eher für Backup und Restore der Konfiguration, sowie zum Aufspielen der Konfiguration auf mehreren Geräten. Messaging auf der Kommandozeile ist recht mühselig.

# Initiale Konfiguration

- Zuerst in der App BT Pairing durchführen
- Region: EU\_868
- Long Name auf etwas eindeutiges setzen
- Rechts oben "Radio Configuration → User" aufmachen
- Short Name prüfen und ggf. anpassen
- Alle anderen Dinge auf Defaults lassen

# Channels konfigurieren

- Der erste Kanal ist standardmäßig "LongFast" mit PSK "AQ==" und PRIMARY
- Der primäre Kanal überträgt per Default Standortdaten (das scheint sich aber gerade in neueren Firmwareversionen zu ändern)
- Private Kanäle sind verschlüsselt
- Channel Name und PSK bilden zusammen den Schlüssel (das ist wichtig, wenn man Kanäle mit anderen teilt, denn der Name darf nicht geändert werden – sonst geht's einfach nicht)
- Eine gute Idee ist, den privaten Kanal als ersten zu definieren und LongFast als zweiten, dann kann wenig schiefgehen
- Der LoRa Channel (Radio Configuration → LoRa → Frequency Slot) ist für EU\_868 1

# Benachbarte Nodes finden

- Um andere Nodes im Umfeld zu erkennen, sollte der Node etliche Stunden, manchmal auch Tage, an einer möglichst hohen Position laufen
- In Radio Configuration → Device ist unter Nodeinfo broadcast ein Intervall von 10800 Sekunden (3h) angegeben; so lange dauert es, bis die Nodes jeweils ein Lebenszeichen senden, was manchmal empfangen wird, aber auch verloren gehen kann; deshalb dauert es manchmal lange, bis sich Nodes gefunden haben
- Die Ausbreitung im 35cm-Band ist Line-of-Sight; das bedeutet, dass eine möglichst hohe Position der Antenne mit freier Sicht zu benachbarten Nodes die größtmögliche Chance auf Kommunikation hat

# Messaging

- Channels: Lassen sich wie ein Gruppenchat benutzen
- Direct Messages: In der Nodeliste auf den Short Name tippen und halten, Direct Message senden
- Der Status ist erstmal eine leere Wolke, das bedeutet, dass die Message gesendet wird
- Entweder materialisiert sich ein User-Symbol mit einem Haken; das heißt, der adressierte Node wurde direkt erreicht,
- Oder eine Wolke mit einem Haken; das bedeutet, dass ein oder mehrere Nodes dazwischen die Message weiterleiten (hier gibt es keine Bestätigung des Empfangs),
- Oder eine durchgestrichene Wolke; das bedeutet, die Aussendung schlug fehl
- Die Aussendungen benötigen durch das Scheduling und die geringe Bandbreite etwas Zeit, also Geduld ;)

# Danke

Viel Spaß am Gerät!  
@byteborg@chaos.social  
karsten@rohrbach.de

# Links

- Meshtastic Docs
- Artikel Allgemeinzuteilung auf mikrocontroller.net
- Thread zu Sperrtopfantenzen (Rundstrahler z.B. aufs Dach) für 35cm-Band