Sideband Situation Tracker

v0.02α

Michael Faragher

November 6, 2023

These suggestions have not been reviewed for use in medical, life-saving, or life-sustaining applications and use of unrated equipment or procedural errors in life-threatening situations could result in personal injury or death. This document is designed as a starting point for selection of equipment and guiding the production of a finalized doctrine.

Consult with your risk management and legal departments prior to finalizing your planned infrastructure.

This document was written in the United States and may assume FCC standards; it does not provide legal advice for any nation *including the United States.* The radio operator is responsible for legal operations in their situation and jurisdiction.

Design rules and guidance are not warranted to be correct or applicable to a specific purpose. Responsibility for final design and safety is the responsibility of the designer.

Except where specifically noted, no information has been reviewed by a licensed subject matter expert.

Localization note: Commas (,) are used as thousand separators and periods (.) are used for decimal places. Example: 1,234.56

Document targets RNS manual 0.5.5β and may not align with chapter/section numbers from other versions.

Contents

List of Figures

List of Tables

1 Forward

Real-time position and status tracking has been the dream of leaders since there were people to lead. One of the most terrifying sensations is to send people under your command into a disaster, then needing to simply wait and worry. The ability to keep track of a situation possibly spanning miles across can take rooms full of dedicated personnel, collating reports and documenting every word, or it can take a handful of electronics.

There is nothing that takes the place of a skilled, motivated professional, but the proper equipment can allow fewer people to do more work with less risk of human error. Reticulum allows a distributed mesh network to operate in environments without stable communications infrastructure, and as of Version β 0.7.0, Sideband comes equipped with automated telemetry and real-time mapping.

At the time of writing, a long term telemetry storage system specific to Sideband doesn't exist, however in the interim a compatible LXMF endpoint can record the datastream directly.

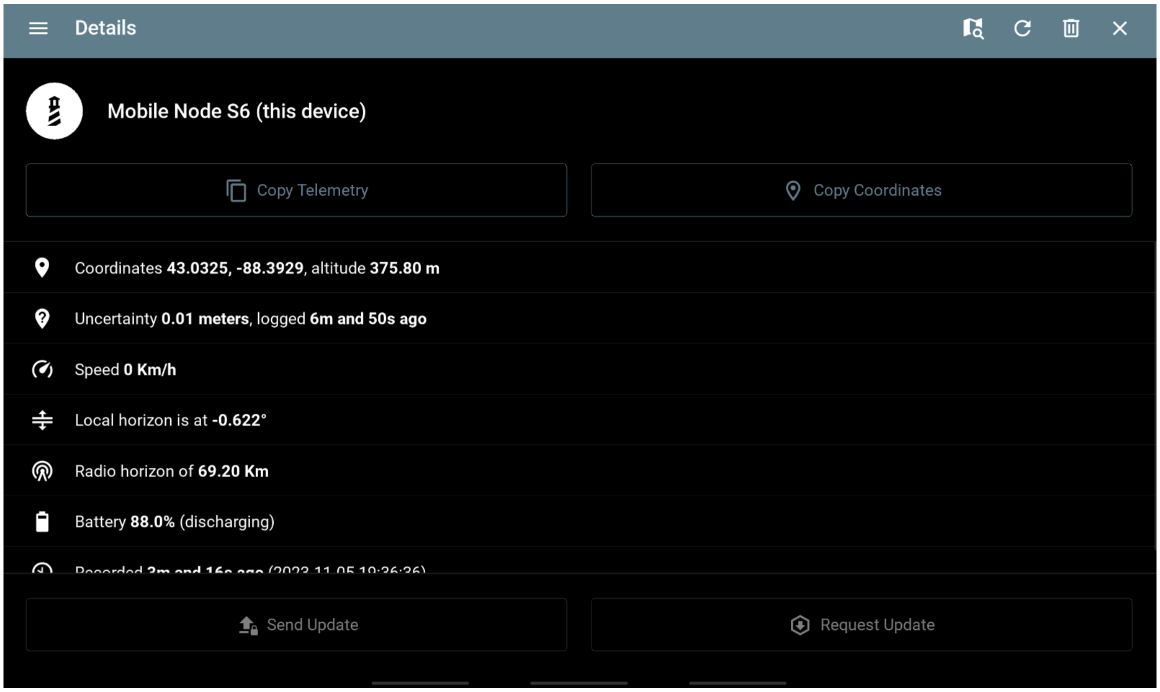
1.1 Alternate Uses

There is no reason to restrict Sideband Telemetry to special operations. A solar powered node with temperature and barometric sensors can be used as an automated weather station as well as a telemetry collector and relay node. Appearing on a map and providing GPS location data is very helpful, but for power savings, a stationary node could use a hard-wired location to leave the GPS receiver powered down.

1.2 License

This document is released under the MIT license as presented in the Reticulum GitHub repository (https://github.com/markqvist/Reticulum/blob/master/LICENSE)

1.3 Example Output



Mobile Node S6 (this device)

Coordinates **43.0325, -88.3929**, altitude **375.80 m**

Uncertainty **0.01 meters**, logged **6m and 50s ago**

Speed **0 Km/h**

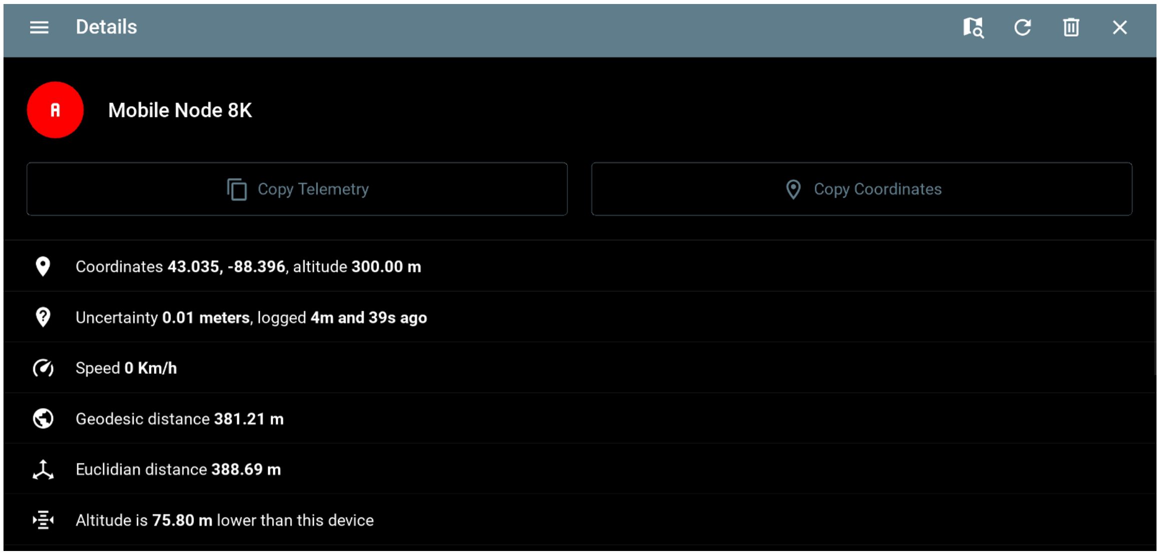
Local horizon is at **-0.622°**

Radio horizon of **69.20 Km**

Battery **88.0%** (discharging)

Recorded **3m and 16s ago** (2023-11-05 19:36:36)

Figure 1.1: Station S6: Collector



Mobile Node 8K

Coordinates **43.035, -88.396**, altitude **300.00 m**

Uncertainty **0.01 meters**, logged **4m and 39s ago**

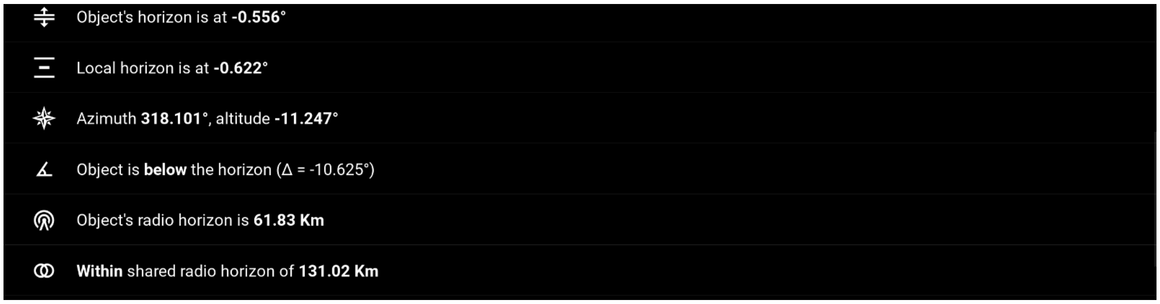
Speed **0 Km/h**

Geodesic distance **381.21 m**

Euclidian distance **388.69 m**

Altitude is **75.80 m** lower than this device

Figure 1.2: Station 8k: Mobile



Object's horizon is at **-0.556°**

Local horizon is at **-0.622°**

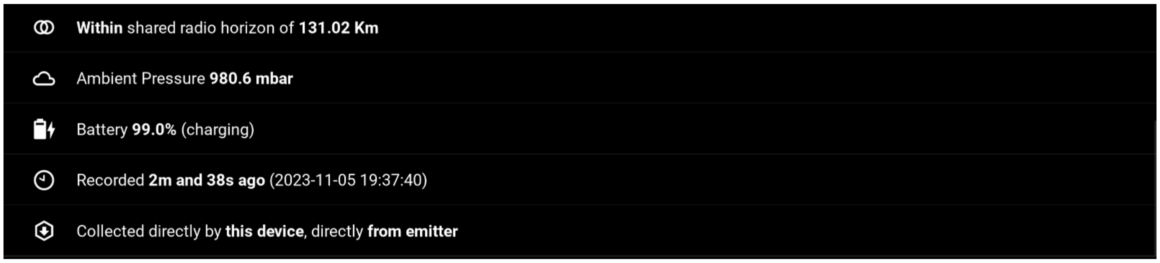
Azimuth **318.101°**, altitude **-11.247°**

Object is **below** the horizon (Δ = -10.625°)

Object's radio horizon is **61.83 Km**

Within shared radio horizon of **131.02 Km**

Figure 1.3: Station 8k: Mobile, cont.



Within shared radio horizon of **131.02 Km**

Ambient Pressure **980.6 mbar**

Battery **99.0%** (charging)

Recorded **2m and 38s ago** (2023-11-05 19:37:40)

Collected directly by **this device**, directly **from emitter**

Figure 1.4: Station 8k: Mobile, cont.

This page intentionally left blank.

2 Network Architecture

Sideband is an LXMF messenger built on the Reticulum Network Stack. The addition of telemetry and a situation map has vastly expanded its utility, but at its core it remains an LXMF system. The Lightweight Extensible Message Format is designed with Reticulum in mind and passes encrypted messages between two devices, either human to human or machine to machine. Unlike pure Reticulum packets, these are designed with a return address to allow two-way communication. The use of propagation nodes to store messages for offline recipients allows for a failure tolerant communication network.

The finer points of Reticulum network configuration is beyond the scope of this document and it is assumed that a network has been defined and the network administrator understands basic network functionality such as announces.

An understanding of collectors is required for minimum telemetry function, and due to the critical nature of propagation nodes, they will also be reviewed below. A propagation node is not required for basic function, but provides significant resilience.

2.1 Collectors

A collector is a repository for telemetry. Individual stations can send telemetry to a collector, either on demand or on a schedule, and authorized stations can request telemetry from a collector. Depending on configuration, a collector can send a single, current report on its own status or all known telemetry. This allows for local collectors to store data and display a local situation map, but also remain separate from larger networks.

Example 1

Five individuals with “enable collector” set to *off* enter their team leader’s LXMF address in their telemetry menu, and their team leader has the section leader’s address in their address field, along with both “enable collector” and “sync all known telemetry to connector” to *on*. The team members can only see themselves, but the team leader can see all of the team members and themselves. The section leader can see all of the members and the leader. If the team members request telemetry, they will see the entire team and the leader, but not the section leader.

Enabling “auto sync to/from” collector will automate this process, and update the situation map and stored telemetry on a set schedule.

Example 2

A situation display has the collector and "autosync to" disabled, but "autosync from" enabled, and is linked to the section leader from Example 1. This display does not provide telemetry to any other unit, but can see all the attached nodes. However, this requires that the section leader has "allow requests from all trusted" set to *on*.

Example 3

An unsecured weather station has "allow requests from anyone" set to *on*. It will provide its telemetry to any requester on the network. It is good for public information but should never house personally identifying information or other sensitive data. It is effectively broadcasting in the clear to anything on the Reticulum network.

2.2 Propagation Nodes

A propagation node is a fundamental piece of Reticulum. It stores LXMF messages for offline recipients. While not technically necessary, it allows asynchronous communication. Telemetry can be sent through a listed and trusted propagation node or it can be used as a fallback if direct delivery fails.

Example

Team members are in range of their vehicle, which contains a propagation node. When they try to send telemetry to the section leader, there is no network connection (the station is down, out of range, or similar issues). If they have "try propagation node on direct delivery failure" set to *on* then they will send the message to the propagation node, which will store it until the section leader is back online. These messages are stored encrypted and the content is unavailable to the node; it only knows the recipient.

2.3 Suggested Architecture

Based on the NIMS/ICS concept of span of control, the preferred architecture is a collector at every level, feeding a collector above it. With 3-7 team members per leader, the information presented grows at a reasonable rate. A team leader, in charge of approximately five people, sees their team and can make low level decisions quickly without information overload. The next level, with around 5 direct reports and 25 total members, can still understand the situation. Another level up could manage over 125 individual people, but the map would be less for individual direction and more for seeing patterns in the response.

As the scope increases, time sensitivity decreases. A five minute reporting period at the individual level may be important, but a 15 - 30 minute delay at the organizational level is likely fast enough, and an authorized party at any level can reach down and request updated telemetry from any collector on the network.

The greater the size of the network, the more helpful the ability to query any collector on the network. Allowing requests from any trusted source requires trusting peers manually, but can greatly increase the ability to zoom in on any unit. For both security and bandwidth purposes, the larger the network the more useful IFAC can be.

Co-locating collectors and propagation nodes in vehicles or static locations is a logical decision, but the role of the vehicle or location must be considered. If a collector, propagation node, and map display are all co-located, it can cut down on the individual number of electronic devices in the field, but unless the station is actually manned, there's little reason to have a map display, and a strong network may not need propagation nodes.

Each response is unique, but having a number of options pre-planned allows for a more rapid and better trained response.

This page intentionally left blank.

3 Configuration

Configuration of individual devices is straightforward once the network architecture is established. This chapter is designed to be accessible to non-technical users, but it requires a well designed network. Combined with the quick reference guides, the end user should be up and running in a short time.

The following is the sideband menu, accessible from the top left corner of the app. Of interest are the "telemetry," "preferences," and "hardware."

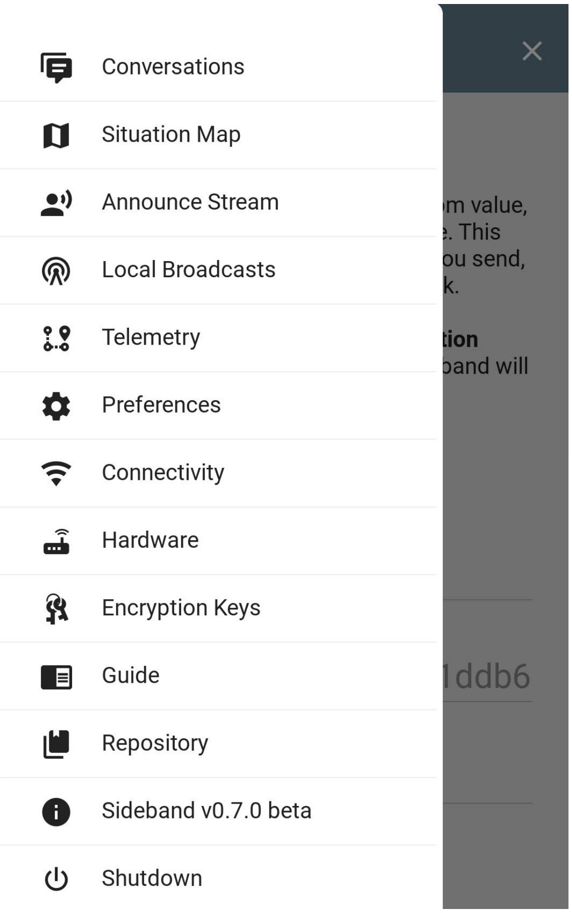
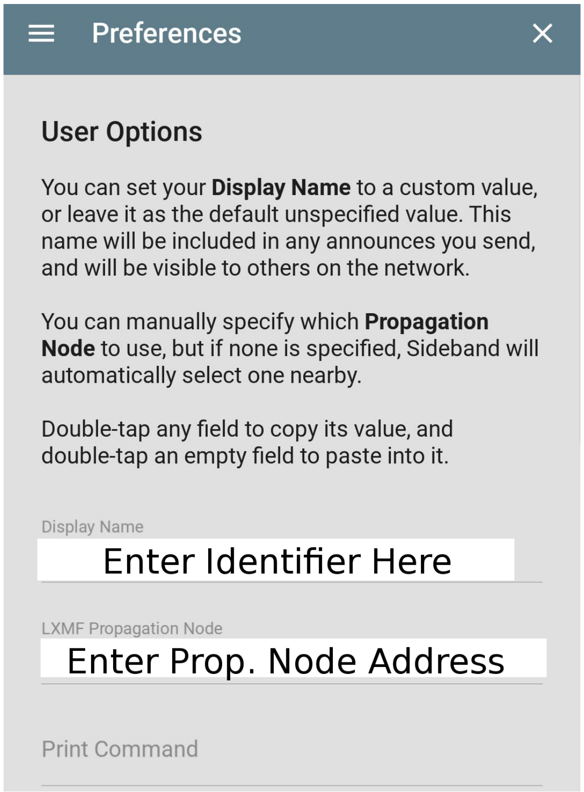


Figure 3.1: Sideband Menu

3.1 Preferences

The preferences menu contains a number of general preferences, but a number need to be set correctly for proper telemetry. Others may be set for personal preference or as directed by network administrators.



User Options

You can set your **Display Name** to a custom value, or leave it as the default unspecified value. This name will be included in any announces you send, and will be visible to others on the network.

You can manually specify which **Propagation Node** to use, but if none is specified, Sideband will automatically select one nearby.

Double-tap any field to copy its value, and double-tap an empty field to paste into it.

Display Name
Enter Identifier Here

LXMF Propagation Node
Enter Prop. Node Address

Print Command

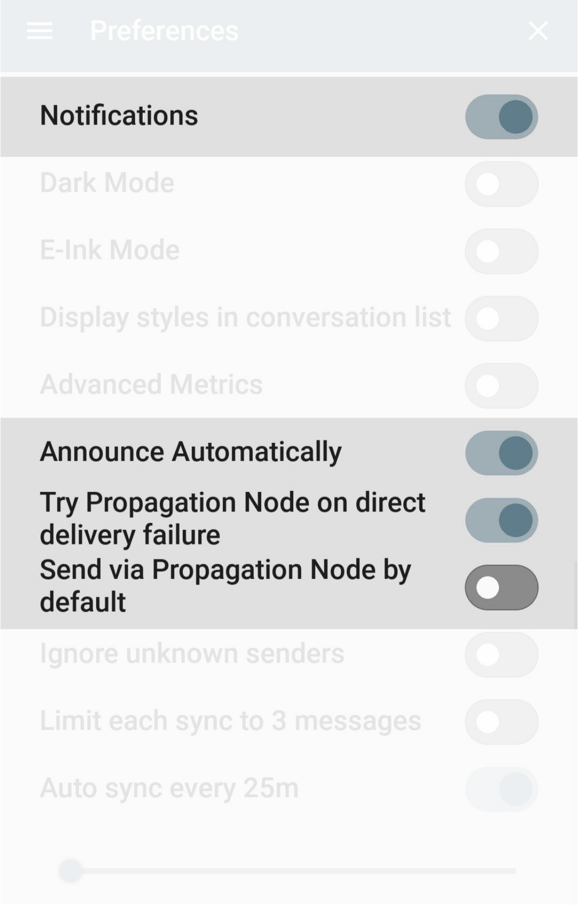
Figure 3.2: Display name and propagation node Entry

Sideband will generate an identity[1] automatically, and unless otherwise instructed, it does not need to be changed. However, it's useful to change the display name and if a specific propagation node is required, it can also be entered here.

The display name is a friendly name for the user, and can be set as desired. It can be used for individual names, such as "Jane Smith" but it can also be used for designations like "Rescue - 3," "Red - 6," or an elaborate designation such as "OPS - IV - A - 1" for somehing like Operations, Division IV, Team A, Member 1, but it's more important to remain readable and consistent. This is the primary way a user will be known in messenger, and should be clear but readable.

The primary identification on the situation map is the icon, and will be discussed later.

[1] An identity is what generates addresses and contains cryptographic keys; it is a fundamental part of Reticulum and beyond the scope of this document



Notifications

Dark Mode

E-Ink Mode

Display styles in conversation list

Advanced Metrics

Announce Automatically

Try Propagation Node on direct delivery failure

Send via Propagation Node by default

Ignore unknown senders

Limit each sync to 3 messages

Auto sync every 25m

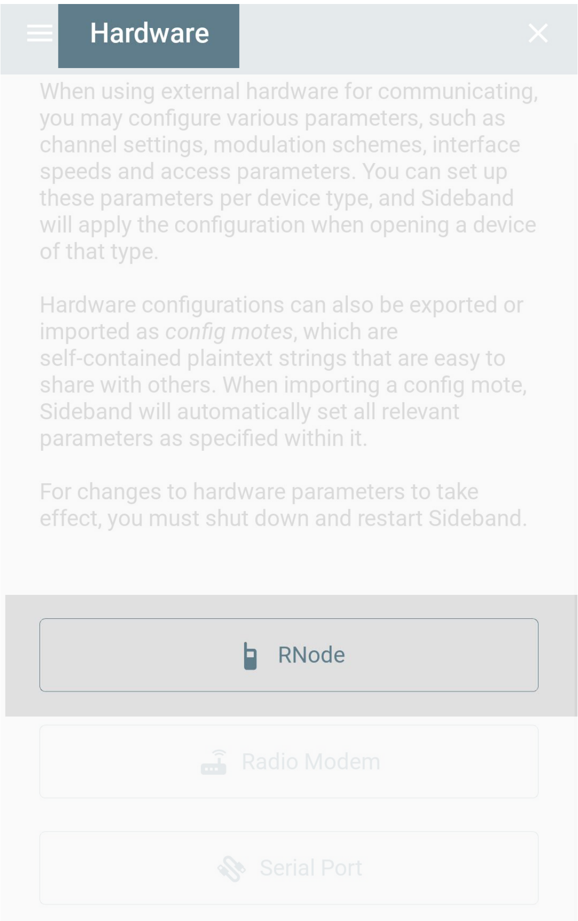
Figure 3.3: Useful Preferences

Keeping the notifications on is important for communications, but since propagation node messages are synced relatively slowly, only directly delivered messages can be counted on for quick notifications.

Automatic announces are situational. While it can be useful if the network topography changes frequently or if there are new users joining, it does require some bandwidth and Sideband can always query the network for paths and cryptographic keys so long as the destination has announced to the network at least once.

If there are propagation nodes on the network, it's advisable to try to send failed messages over the propagation network, but sending them by default is not advisable in most situations unless destinations are expected to be unavailable by default.

3.2 Hardware



When using external hardware for communicating, you may configure various parameters, such as channel settings, modulation schemes, interface speeds and access parameters. You can set up these parameters per device type, and Sideband will apply the configuration when opening a device of that type.

Hardware configurations can also be exported or imported as *config motes*, which are self-contained plaintext strings that are easy to share with others. When importing a config mote, Sideband will automatically set all relevant parameters as specified within it.

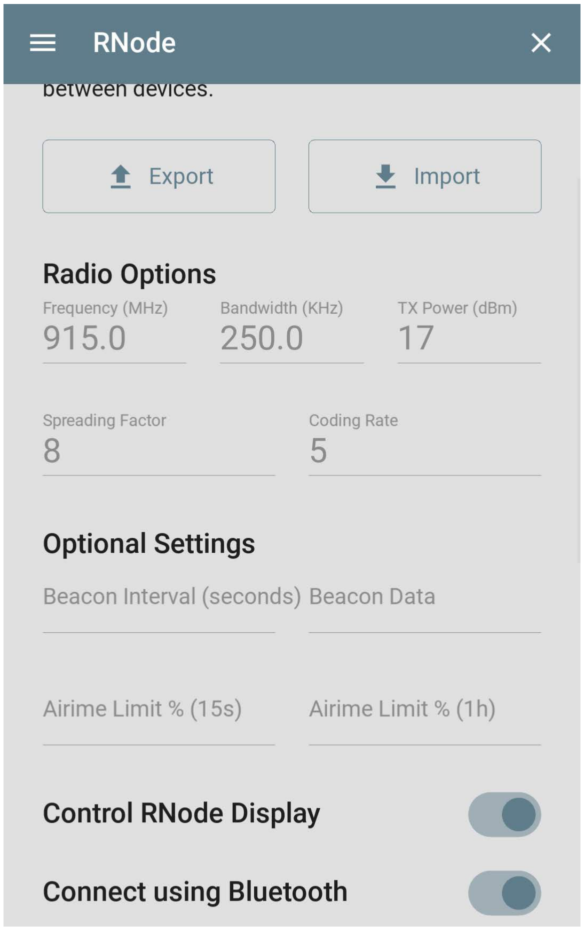
For changes to hardware parameters to take effect, you must shut down and restart Sideband.

Figure 3.4: RNode configuration Option

For the purposes of this document, it's assumed that the only additional hardware is an RNode; the configuration of other hardware interfaces is beyond the scope of this document.

The first step is to access the RNode specific section of the hardware menu using the button shown in Figure 3.4

This example configuration may not be legal in all jurisdictions. Please check your local laws while selecting these parameters.



between devices.

Radio Options

Frequency (MHz) 915.0

Bandwidth (KHz) 250.0

TX Power (dBm) 17

Spreading Factor 8

Coding Rate 5

Optional Settings

Beacon Interval (seconds)

Beacon Data

Airime Limit % (15s)

Airime Limit % (1h)

Control RNode Display

Connect using Bluetooth

Figure 3.5: RNode Configuration

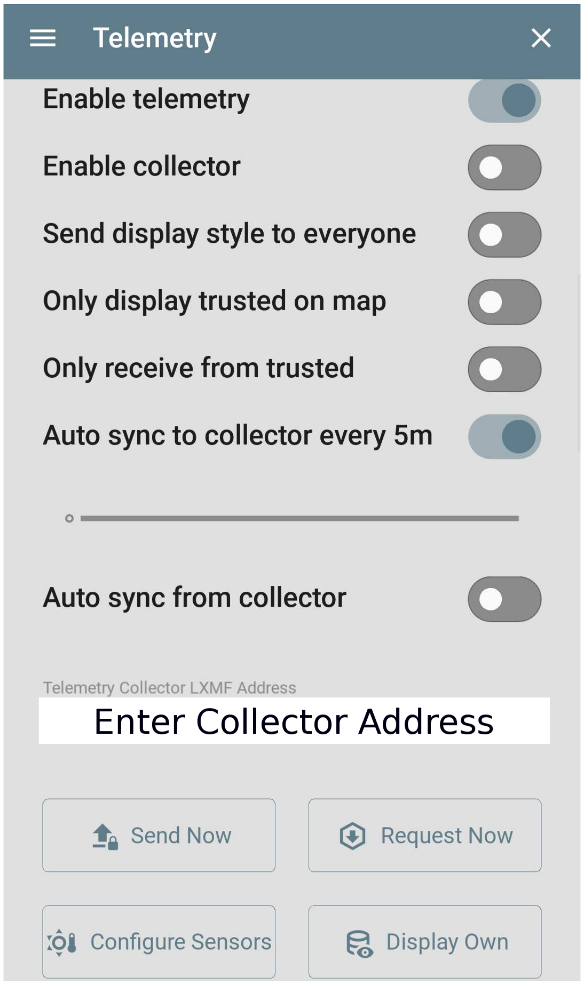
RNode configurations are covered in more detail in the main Reticulum manual, but the basic configuration is straightforward. The frequency, bandwidth, and spreading factor must be identical to the network, but transmission power and coding rate can vary. Contact your network administrator for the proper configuration, or the base Reticulum documentation to generate a new configuration.

As noted in the hardware menu, the frequency is measured in Megahertz and the bandwidth in Kilohertz. This means a frequency of 915,200,000 Hz is equivalent to an entry of 915.2 on this page, and 125,000 Hz is equivalent to 125. The use of consistent nomenclature should be used across all signage and quick reference, but it's important to understand how to operate with documents using differing nomenclature.

Beacon settings are designed for compliance with traditional RF regulations, and are not typically needed with an RNode.

Airtime limits are for duty cycle compliance in jurisdictions which require them. Set according to the local regulations and the guidance from your network administrator.

3.3 Telemetry



Telemetry

Enable telemetry ☑

Enable collector ☐

Send display style to everyone ☐

Only display trusted on map ☐

Only receive from trusted ☐

Auto sync to collector every 5m ☑

Auto sync from collector ☐

Telemetry Collector LXMF Address

Enter Collector Address

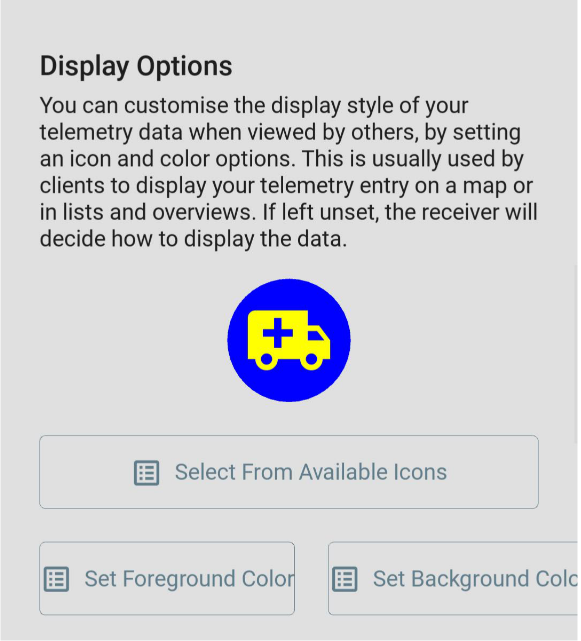
Figure 3.6: Telemetry Configuration

By enabling local telemetry collection with “enable telemetry”, all selected sensors (see below) will be available to be sent or requested. This doesn’t provide much functionality by itself, but can be combined with the previously mentioned trust-based requests, but the primary use is through collectors.

Turning on “enable collector” will turn that Sideband instance into a collector, allowing uploading and downloading from the collector. This is the core of a telemetry tracking system, and functions as both storage and asynchronous distribution node.

Incoming telemetry can be filtered by using the “only receive from trusted” option, and the time between automated syncs can be set on this page.

A remote collector can be designated on this page using its LXMF address. The easiest and most error-resistant way to fill this field is by finding the collector in either the conversation or announce tabs (which is required for trusting it) and then simply copying the address and pasting it in this field.



Display Options

You can customise the display style of your telemetry data when viewed by others, by setting an icon and color options. This is usually used by clients to display your telemetry entry on a map or in lists and overviews. If left unset, the receiver will decide how to display the data.

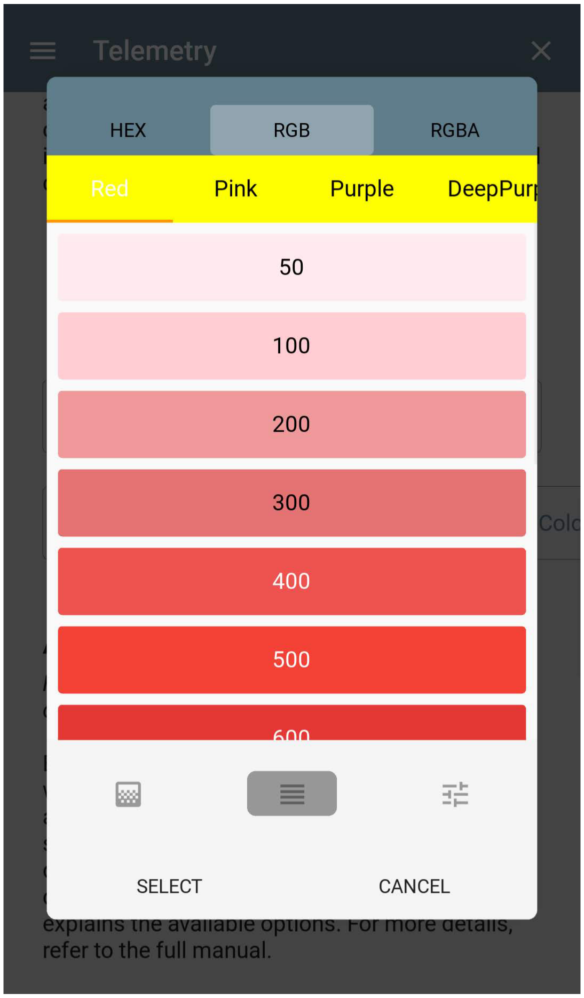
Figure 3.7: Display icon Configuration

The icon set in these options is the primary way the station is known on the situation map; its selection is critically important for readability. In smaller operations, with teams such as “Red” or “Blue” then it would be possible to use the color of the team as a background with letters for the specific team member, while in larger operations it may be more helpful to split colors by function, such as Fire Department red, Police Department Blue, etc. or by the ICS T-Card colors. Whatever the scheme, it needs to be clear, consistent, and well published.

High contrast is important in color choices. Modern highway signage is an excellent example, but the basic rules date back to classical heraldry. The simplest guideline is to never place a color on a color or a metal on a metal. There are some logical contradictions, as a bright green may create poor contrast with white or yellow, but generally speaking the old rules still apply. One exception is the use of purple. A large percentage of the population has a variant of colorblindness that makes blue and purple appear identical, and for that reason, purple should be avoided. Multiple variations of colors or shades should also be avoided. The basic metal/color chart is provided in Table 3.1.

Metal	Color
Gold / Yellow	Red
Silver / White	Green
	Blue
	Black

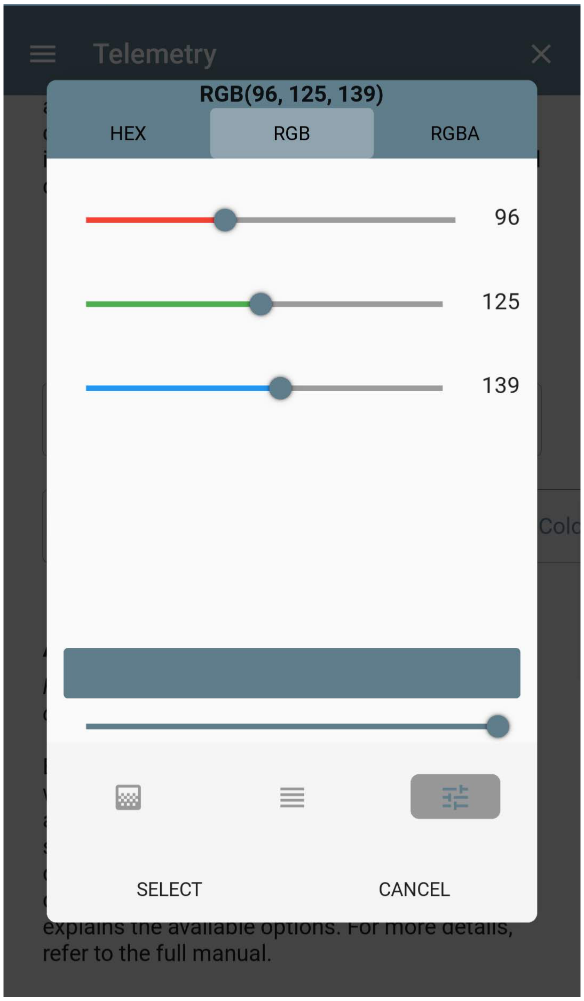
Table 3.1: Heraldic color types



explains the available options. For more details, refer to the full manual.

Figure 3.8: Nominal color Selection

Nominal color selection can be used to select a color by name and intensity. It can be chosen by using the middle icon just above the select and cancel buttons.



RGB(96, 125, 139)

96

125

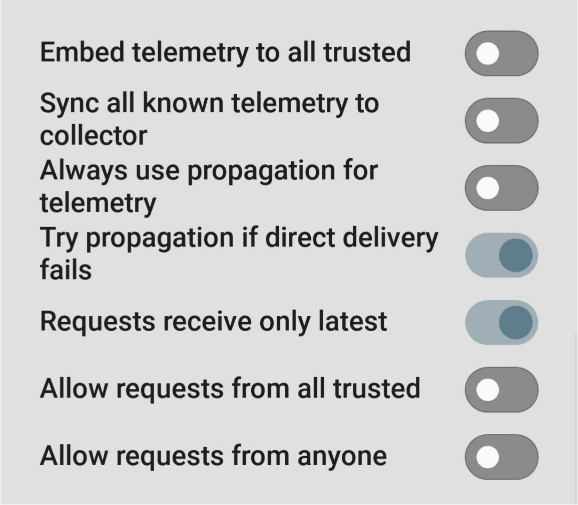
139

explains the available options. For more details, refer to the full manual.

Figure 3.9: RGB Color Selection

RGB color selection can be used via the rightmost button, and is effective for choosing pure colors (red/green/blue/white/black) and yellow (red+green). Please do not use teal or purple, this will cause confusion in approximately 8% of the genetically male population and one half percent of the genetically female population. This is an avoidable risk; colors for quick reference must be at high contrast to each other.

The symbol in the icon is also important, and has a wide number of options. Sideband has access to a tremendous number of graphics, from the Latin letters A - Z and a police station to the symbol for Aurebesh (the typeset from Star Wars) and the Guy Fawkes mask. Any icon available in the Material Design Icon set (https://pictogrammers.com/library/mdi/) can be used, and pre-planning will prevent unnecessary delays; the set is sizable.



Embed telemetry to all trusted ○

Sync all known telemetry to collector ○

Always use propagation for telemetry ○

Try propagation if direct delivery fails ●

Requests receive only latest ●

Allow requests from all trusted ○

Allow requests from anyone ○

Figure 3.10: Advanced telemetry Configuration

Sideband can embed telemetry to all trusted sources, making every LXMF message a telemetry report. This may be useful in cases where someone is marking locations or times of events, or for automated systems to send information on a trigger.

By default a station only reports its own telemetry, but by selecting “sync all known telemetry” it will send all collected telemetry, including its own, whenever it syncs to another collector. This is useful for local repositories meant to upload to a larger organizational storage system.

For stations that only require an instantaneous telemetry reading, such as a pure positional indicator, opting to send only the current reading, not complete telemetry, can cut down on unnecessary traffic and save bandwidth.

Finally, a station can allow its telemetry to be requested by either all trusted users, or by any user on the network.

> Unless the station is meant to be public and the information accessible to anyone connected to the network, *do not* set “allow requests from anyone” to *on*

4 Authorized Requests

Only authorized systems can upload or request telemetry, but there are many ways to authorize a specific address.[1]

- Unless specifically instructed to only accept telemetry from trusted nodes, it will accept telemetry from any source
- By default, a non-collector will not send telemetry and refuse all requests
- Selecting "send telemetry" in a conversation will send any new telemetry with any message
- Selecting "embed telemetry to all trusted" will send new telemetry with any message to a trusted address
- Selecting "allow requests" in a conversation will allow telemetry requests, ping, echo, and signal report commands
- Selecting "allow requests from all trusted" will enable the above functionality for all trusted addresses
- Selecting "allow requests from anyone" is an emergency option that will allow the above functionality for all addresses. This is an unsafe condition and will change the UI color to remind the user it is enabled

  These rules all flow from the same concept: that telemetry must be manually enabled and collection is always an opt-in affair. Accepting telemetry from all stations is convenient, but if there is a question of DOS or poisoning, then either the network can be secured with IFAC or by only accepting telemetry from trusted sources.

  Creating a source that can properly distribute information requires some configuration, but these rules allow the collector to allow requests from specific addresses or classes of addresses. It is even possible to trust another collector that will act as a distribution center to other addresses, simply by sending telemetry to the other connector with the authorized addresses properly configured.

[1] This section based on correspondence with Mark Qvist, used with permission

This page intentionally left blank.

5 Reference Sheets

The following sheets are used for quick reference purposes and are intended to be printed, filled out by hand, and posted in staging areas. To facilitate the use of QR codes and printed collector addresses, the desaturated area is 4x6 inches to facilitate the use of thermal printed labels.

A label generation program is planned but not available at time of writing.

Filled examples should not be used as their information is region specific, and the example address is live, but is not connected to a telemetry collector.

For further guidance on interface modes and network configuration, see the Reticulum manual or primer.

The Team Leader and Team Member reference sheets should be plain, and Team Leaders can certainly be used for vehicles or base stations, but the Map Station is designed not to provide telemetry to a central hub, but to get data from an authoritative collector for local display.

Team Leader

RNode Configuration

FREQUENCY

BW

SF

CR

TX Pwr

Your Collector

NAME

QR

ADDRESS

- ☐ Auto Announce
- ☑ Try Propagation
- ☐ Default Propagation
- ☐ Ignore Unknown
- ☐ Limit Sync

- ☑ Telemetry
- ☑ Collector
- ☑ Auto Sync To
- ☐ Auto Sync From

Sync Time:

- ☑ All Known
- ☐ All Prop
- ☑ Try Prop
- ☐ Latest
- ☐ Anyone

Display Options

ICON

FORE COLOR

BACK COLOR

Team Member

RNode Configuration

FREQUENCY

BW

SF

CR

TX Pwr

Your Collector

NAME

QR

ADDRESS

□ Auto Announce
☑ Try Propagation
□ Default Propagation
□ Ignore Unknown
□ Limit Sync

☑ Telemetry
□ Collector
☑ Auto Sync To
□ Auto Sync From
Sync Time:

□ All Known
□ All Prop
☑ Try Prop
□ Latest
□ Anyone

Display Options

ICON

FORE COLOR

BACK COLOR

Map Station

RNode Configuration

FREQUENCY

BW

SF

CR

TX Pwr

Your Collector

NAME

QR

ADDRESS

□ Auto Announce
☑ Try Propagation
□ Default Propagation
□ Ignore Unknown
□ Limit Sync

□ Telemetry
□ Collector
□ Auto Sync To
☑ Auto Sync From
Sync Time:

☑ All Known
□ All Prop
☑ Try Prop
□ Latest
□ Anyone

Display Options

ICON

FORE COLOR

BACK COLOR

Team Member - EXAMPLE

RNode Configuration

FREQUENCY

915.200

BW

250

SF

8

CR

5

TX Pwr

17

Your Collector

NAME

BtB Node Delta

ADDRESS

96c3106007a1b9ea489a8356400bffb5

QR

□ Auto Announce
☑ Try Propagation
□ Default Propagation
□ Ignore Unknown
□ Limit Sync

☑ Telemetry
□ Collector
☑ Auto Sync To
□ Auto Sync From
Sync Time:

□ All Known
□ All Prop
☑ Try Prop
□ Latest
□ Anyone

Display Options

ICON

account-hard-hat

FORE COLOR

Yellow (255,255,0)

BACK COLOR

Blue (0,0,255)

This page intentionally left blank.

6 FAQ / Issues

Can all nodes see everyone on the situation map?
My map only shows me.

The situation map displays all telemetry known by the local machine. A collector will know all information sent to or requested by it, but any node can request the data from their collector, then display that information.

How can I prevent nodes from poisoning my data?

Enable "Only receive from trusted" in order to only accept data from trusted nodes. Nodes must be manually trusted in order for this to work.

How do I prevent people from seeing my telemetry?

Listed collectors can receive and request data, but so long as "Allow requests from all trusted" is off, other nodes should not be able to collect your telemetry? *There is almost no reason to "Allow requests from anyone" except for public infrastructure like weather stations. Do not upload telemetry to these machines.*

Are you collecting my telemetry?
Is my data secure?
Do you comply with EU regulations?

All data is sent encrypted between stations. It is not collected by any party other than the listed collector and their attached nodes. A properly configured network will not distribute data to unauthorized nodes. If security is critical, enable IFAC and only provide the passphrase to trusted nodes. Compliance with security best practices and legal requirements are the duty of the system operators of the collectors.

Why can't I enable some sensors?
Why are some of my sensors returning bad information?

Sideband can only send data from sensors that exist on the hardware and are accessible. Check your hardware specifications and permissions.

I don't want people knowing my position!

Telemetry should only be sent to trusted sources. However, you can disable your location reporting or even provide a fixed position in the sensor settings.

What is the range of transmission?

Sideband uses the LXMF protocol on top of the Reticulum Network Stack. Telemetry will be carried across any configured interface across any available network. This makes the range indefinite, especially when using Internet or cellular uplinks. Since a propagation node can store messages for later transmission, the node itself can be moved and transmitted several days later, making range in both distance and time indefinite. See individual interfaces, such as the RNode, for ranges for a given transmission system.

Why are some pages marked "intentionally left blank?"

After printing hundreds of documents and tens of thousands of pages using a cheap laser printer, the author has learned the pain of "Is this page supposed to be blank?" This document follows the convention of starting chapters on odd numbered pages both for tradition and to assist in printing by chapter for reference binders/folders.

7 Iconography Reference

Icon	Name	Suggested Uses
((•))	access-point	Radio/network access point, repeater
👤	account	User
👷	account-hard-hat	Construction, engineering
🔍	account-search	Investigations
✈	airplane	Fixed-wing aircraft
🛫	airport	Airfield
⚠	alert	Warning, danger, distress
A	alpha-a	(Typical, A-Z) Alpha unit designation
🚑	ambulance	EMS vehicle/team
🗃	archive	Sorage, supply
🏍	atv	All-terrain vehicle
🪪	badge-account-outline	Officials
🧪	beaker	Lab, test facility
🛏	bed	Rest area, lodgings
🚲	bicycle	Bicycle
☣	biohazard	Biohazard, biohazard response team
💣	bomb	Explosive hazard, EOD
📡	broadcast	Radio/network access point, repeater
💡	bulkhead-light	Lighting unit/vehicle
📢	bullhorn-outline	Loudspeaker/announcement unit/vehicle
🚌	bus	Bus, mass person transport
🔥	campfire	Camp, unimproved rest area
🚗	car	Automobile, vehicle
🚘	car-connected	Vehicle with radio node/repeater
🛢	database	Information storage
🖥	desktop-classic	Computation, administration, office, clerical
🤿	diving-scuba	Rescue divers, underwater operations
🛩	drone	Unmanned Aerial Vehicles
🚚	dump-truck	Dump truck, earthmovers

Table 7.1: Selected Icons

Icon	Name	Suggested Uses
🔌	ev-plug-tesla	EV charging point
🚜	excavator	Excavator, earthmoving equip., excavation site
⛴	ferry	Ferry, large ship
🚒	fire-truck	Fire truck, firefighting
⚡	flash	Power, electrical hazard
🍔	food	Food, canteen, provisions
⛽	fuel	Fuel
🚗	golf-cart	Golf card, light battery powered vehicle
🪦	grave-stone	Mortician, body storage, recovery team
🍖	grill	Field kitchen, unimproved meal site
🛠	hammer-wrench	Maintenance, engineering
🧼	hand-water	Hygiene, sanitation
🚁	helicopter	Rotary wing aircraft
🚶	hiking	User, searcher
🏇	horse-human	Mounted personnel
🛶	kayaking	Light boat transport
🧰	medical-bag	EMS, medical
0	numeric-0	(Typical, 0-9) Numeric unit designation
🧻	paper-roll-outline	Hygiene, toilets, waste
🪂	parachute	Airdropped personnel or supplies
⛨	police-badge	Law enforcement
🏢	police-station	Law enforcement HQ/staging point
☢	radioactive	Radiological hazard, CBRNE Response
📱	radio-handheld	Radio operator
📡	radio-tower	Radio access point/repeater
VI	roman-numeral-6	(Typical, 1 - 10) Branch/division designation
🏃	run	Person, courier, runner

Table 7.2: Selected Icons, cont.

Icon	Name	Suggested Uses
📡	satellite-uplink	Satellite uplink
🛰	satellite-variant	Satellite uplink
🎓	school	Training facility/unit, shool
💺	seat-passenger	Rest area
🛡	security	Security
🛁	shower	Hygiene, decontamination
⛷	ski-cross-country	Ski transport
🚛	tanker-truck	Tanker truck, fuel/water
🌡	thermometer	Weather station
🗼	tower-fire	Fire/observation tower
🚚	tow-truck	Tow truck, recovery vehicle
🚚	truck	Truck
📶	wifi	WiFi/radio access point

Table 7.3: Selected Icons, cont.